5 Deploying and securing servers ................................................................. 135
Predeployment configuration .................................................................... 135
Configuring image installs ........................................................................ 136
  Configuring imaging jobs ....................................................................... 136
  Configuring Windows Sysprep jobs ....................................................... 136
Configuring scripted installs ................................................................. 137
  Configuring scripted install jobs ......................................................... 137
  Configuring SAN-attached scripted install jobs ................................... 137
  Configuring Boot from SAN scripted install jobs ............................... 138
Using the Rapid Deployment Pack ......................................................... 138
  Connecting the server blades ............................................................... 139
Creating a reference server and image .................................................... 141
Deploying a captured image to other similar servers ............................. 143
Reconfiguring the new servers .............................................................. 144
Maintaining server blades with rip-and-replace ..................................... 146
Performing a Boot from SAN installation .............................................. 147
Vulnerability scanning and deploying patches and fixes ....................... 148
  The Vulnerability and Patch Management Pack interface ................. 151
  Provided scan definitions .................................................................... 152
  Scanning for vulnerabilities .................................................................. 152
  Viewing vulnerability scan results ...................................................... 153
  Deleting vulnerability scan results ....................................................... 154
  Deploying patches and fixes ............................................................... 155
  Validating installed patches ............................................................... 160
  Deploying the VPM Patch Agent ......................................................... 161
  Removing patches ............................................................................. 162
  Vulnerability and Patch Management Pack events ........................... 164
6 Virtualization and consolidation of servers .......................................... 165
Virtual Machine Management Pack ...................................................... 165
  Virtual machine host .......................................................................... 166
  Virtual machine guest ........................................................................ 167
  Task execution process ....................................................................... 169
  Using the Virtual Machine Management Pack tools and controls .... 170
  Configuring the polling frequency for virtual machine status checks 183
  Event handling .................................................................................. 184
  Setting up prefailure event handling .................................................. 184
  Failed host recovery ........................................................................... 186
  Setting up the recovery feature ......................................................... 186
  Creating a CriticalVmHost collection .................................................. 186
  Launching SCVMM ............................................................................. 189
  Launching VirtualCenter .................................................................... 190
  VirtualCenter information ................................................................... 191
  Configuring Virtual Machine Management Pack on a Microsoft Cluster Server ........................................ 192
  Multisystem aware tools available ..................................................... 193
  Performance information .................................................................... 193
  Virtual Machine Management Pack infrastructure ......................... 197
7 Reporting .............................................................................................. 198
Reporting in HP SIM ............................................................................. 198
  Generating reports in HP SIM ............................................................ 198
  Software inventory details ................................................................... 199
  Printing reports in HP SIM ................................................................. 199
Installation fails with “Product RMS not installed: Service RMS error. The specified service does not exist as an
installed service (0x424)” message ................................................................. 235
Vulnerability and Patch Management Pack installation fails ......................................................... 236
Cannot modify VPM acquisition settings to acquire updates from a local repository ................. 236
Required open ports ........................................................................................................ 236
Modifying firewall configuration settings .............................................................................. 237
Configuring a DNS server ...................................................................................................... 237
All target systems do not have the same administrator credentials ........................................ 238
Multiple VPM servers ......................................................................................................... 238
Administrator credentials have been changed ........................................................................ 238
Changing the IIS IWAM user name and password ............................................................... 239
The IIS Certificate has expired and the Vulnerability and Patch Management Pack connection must be reconfigured
to use an HTTP connection ................................................................................................. 239
Radias uses installation account instead of local account ........................................................ 241
Uninstalling Vulnerability and Patch Management Pack ....................................................... 241
Reinstalling Vulnerability and Patch Management Pack ........................................................ 242
Vulnerability scans ............................................................................................................... 242
Patches and configuration fixes ............................................................................................. 245
HP SIM integration .............................................................................................................. 248

9 Technical support ............................................................................................................... 249
HP Installation and Startup Service for HP BladeSystem infrastructure .................................. 250
Where to go for additional help ............................................................................................ 250
HP contact information ........................................................................................................ 252

Appendix A Performance Management Pack reference matrix ............................................. 253
Static analysis ....................................................................................................................... 253
ATA disk array .................................................................................................................... 254
ATA Disk Array Status ....................................................................................................... 254
ATA Disk Array Inventory ................................................................................................. 254
ATA disk .................................................................................................................................. 254
ATA Disk Status .................................................................................................................. 254
ATA Disk Inventory ............................................................................................................. 255
Drive array ............................................................................................................................ 255
Drive Array Status .............................................................................................................. 255
Drive Array Inventory ........................................................................................................ 255
External storage enclosure .................................................................................................... 256
External Storage Enclosure Status ....................................................................................... 256
External Storage Enclosure Inventory .................................................................................... 256
Fibre Channel host bus adapter .............................................................................................. 256
Fibre Channel Host Bus Adapter Status .................................................................................. 256
Fibre Channel Host Bus Adapter Inventory ............................................................................ 257
Host buses ............................................................................................................................ 257
Host Buses Status ............................................................................................................... 257
Host Buses Inventory .......................................................................................................... 257
IDE channel .......................................................................................................................... 257
IDE Channel Status ............................................................................................................. 257
IDE Channel Inventory ....................................................................................................... 257
IDE controller ....................................................................................................................... 258
IDE Controller Status ......................................................................................................... 258
IDE Controller Inventory .................................................................................................... 258
Logical drive .......................................................................................................................... 258
Logical Drive Status ............................................................................................................ 258
Logical Drive Inventory ....................................................................................................... 259
Memory .................................................................................................................................. 259
<table>
<thead>
<tr>
<th>Storage components</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Drives</td>
<td>272</td>
</tr>
<tr>
<td>Smart Array SCSI drive</td>
<td>270</td>
</tr>
<tr>
<td>Server metrics</td>
<td>269</td>
</tr>
<tr>
<td>SCSI drive</td>
<td>268</td>
</tr>
<tr>
<td>Server status</td>
<td>269</td>
</tr>
<tr>
<td>Smart Array controller</td>
<td>269</td>
</tr>
<tr>
<td>Smart Array SCSI drive Status</td>
<td>270</td>
</tr>
<tr>
<td>SATA Drives</td>
<td>271</td>
</tr>
<tr>
<td>SAS Drives</td>
<td>272</td>
</tr>
<tr>
<td>Storage components</td>
<td>273</td>
</tr>
</tbody>
</table>
Contents

Storage Status .................................................................................................................. 273
Storage Inventory ........................................................................................................... 273

Appendix B Vulnerability and Patch Management Pack additional information .......... 274
  Infrastructure .................................................................................................................. 274
  Shared server configuration ........................................................................................... 275
  Vulnerability and Patch Management Pack hardware requirements ......................... 277
  Vulnerability and Patch Management Pack software requirements ............................ 278
  VPM Acquisition Utility (optional) ............................................................................... 279
    Target systems ............................................................................................................ 279
    Provided scans .......................................................................................................... 280
  Updating VPM credentials using the Change VPM Credentials Utility ......................... 281
  Backing up and restoring the Vulnerability and Patch Management Pack .................... 281
    Component backup ..................................................................................................... 281
    Component restoration .............................................................................................. 282
  Vulnerability and Patch Management Pack events ...................................................... 282
    Scan events ................................................................................................................ 283
    Patch and fix events ................................................................................................. 284
    Acquisition events ..................................................................................................... 285
    Miscellaneous events ............................................................................................... 286

Appendix C Installing additional operating systems to be deployed by Rapid Deployment Pack .... 288

Index ............................................................................................................................... 290
1 Introduction

This chapter provides an overview of HP Insight Control Management suites provided on the Insight Control Management DVD, and describes the features, benefits, and functionality delivered with these integrated software solutions.

Overview

To help you create the best-run server infrastructures, HP develops Insight Control Management suites that build on HP hardware intelligence combined with powerful HP Systems Insight Manager (HP SIM) and Essentials software.

Insight Control Management suites are designed to address the most difficult issues encountering IT infrastructures, such as cost, time, energy, and change. With flexible software that unifies the management of hardware resources and scales to businesses of all sizes, Insight Control Management helps IT staff gain:

- Total control—Take complete control of the server infrastructure and maintain system availability.
- Maximum flexibility—Be responsive to the needs of your business and increase IT staff efficiency.
- Tangible savings—Make the most of your investments in server assets, staff, and facilities to save time and costs.

The Insight Control Management DVD uses an integrated installer to deploy, configure, integrate, and update Insight Control Management suites and individual management products quickly and accurately. This wizard-based installer enables you to predefined installation and configuration preferences for HP management software, including access credentials, performance settings, and discovery parameters. Then, you can install all components as a single integrated process that requires no media swapping and minimal intervention. You can also install Insight Control Management suites from a component list.

Insight Control Management suites

The Insight Management DVD can be used to deploy and license the following Insight Control Management suites. See Table 1 for a list of components delivered and licensed with each suite. You can install one or more suites during installation.

- Insight Control Environment (ICE)
- Insight Control Environment for BladeSystem (ICE-BL)
- Insight Control Data Center Edition (ICDC)
- iLO Power Management Pack (iPMP)
- iLO Power Management Pack for BladeSystem (iPMP-BL)
Insight Control Environment (ProLiant ML/DL servers)

Insight Control Environment is an integrated software package that delivers comprehensive foundation management for ProLiant DL and ML servers.

Key features

- Unified system monitoring and control, built on HP SIM 5.1
- Rapid server and operating system deployment
- Advanced server power management, including power capping
- Industry-leading remote control and administration delivered through HP Integrated Lights-Out management
- Proactive performance management and bottleneck analysis
- Consolidated vulnerability scanning and patching for Microsoft® Windows® and Linux

Insight Control Environment for BladeSystem

Insight Control Environment for BladeSystem is an integrated software suite that simplifies the provisioning and management of HP BladeSystem infrastructures.

Key features

- Unified system monitoring and control, built on HP SIM 5.1
- Graphical blade infrastructure discovery and administration
- Rapid server and operating system deployment
- Advanced power management for BladeSystem servers and enclosure resources, including power capping
- Industry-leading remote control and administration delivered through embedded BladeSystem functionality and HP Integrated Lights-Out management
- Proactive performance management and bottleneck analysis
- Consolidated vulnerability scanning and patching for Windows and Linux servers
- United management of physical and virtual infrastructure for VMware or Microsoft Virtual Server Environments

Insight Control Data Center Edition

Insight Control Data Center Edition is an integrated software suite that simplifies the provisioning and management of HP BladeSystem infrastructures. Insight Control Data Center Edition can be purchased with select HP BladeSystem c-Class enclosures.

Key features

- Unified system monitoring and control, built on HP SIM 5.1
- Graphical blade infrastructure discovery and administration
- Rapid server and operating system deployment
- Proactive performance management and bottleneck analysis
- Consolidated vulnerability scanning and patching for Windows and Linux servers
iLO Power Management Pack (ProLiant ML/DL servers)

HP iLO Power Management Pack is an energy-efficient management suite that provides core management services, full remote control, and advanced power management for ProLiant DL and ML servers through HP SIM.

Key features

- Unified system monitoring and control built on HP SIM 5.1
- Advanced server power management, including power capping
- Industry-leading remote control and administration

iLO Power Management Pack for BladeSystem

HP iLO Power Management Pack for BladeSystem is an energy-efficient management suite that provides full remote control and advanced power management for BladeSystem infrastructures.

Key features

- Unified system monitoring and control built on HP SIM 5.1
- Advanced power management for BladeSystem servers and enclosure resources, including power capping
- Graphical blade infrastructure discovery and administration
- Industry-leading remote control and administration delivered through embedded BladeSystem functionality and HP Integrated Lights-Out management

Key benefits

Insight Control Management suites:

- Build on proven HP SIM and Essentials software
- Simplify infrastructure lifecycle management
- Unify resource management through a single console
- Enable rapid and consistent server deployment using predefined scripts or system images
- Control remote or headless systems securely at any time, independent of the operating system state
- Optimize server performance and configuration to exacting requirements with real-time monitoring
- Reduce power consumption costs without sacrificing performance

For complete information and licensing options for HP Insight Control Management suites, see http://www.hp.com/go/insightcontrol.
Management suite licensing

For management suite licensing information, see the license keys provided with the Insight Control Management DVD or delivered separately. The Insight Control Management licensing menu in HP SIM is needed to create and assign the Insight Control Environment, Insight Control Environment for BladeSystem, and Insight Control Data Center Edition license keys. The integrated installer must be run to install the licensing menu for these suites. At least one system supported by the suite must be discovered before the corresponding suite license menu appears. To apply license keys, see the “Installing, licensing, and configuring Insight Control Management software” chapter in this guide.

If you are using Integrity servers running HP-UX, then you do not need to purchase licenses, but can still take advantage of Insight Control Management ease of installation and configuration of HP SIM and Extensions for HP SIM on Microsoft Windows. If you are using Integrity servers running Windows or Linux, you can purchase licenses for the Rapid Deployment Pack for operating system deployment while taking advantage of Insight Control Management integrated installation.

Platform support

Insight Control Management is supported on a defined set of HP hardware, HP storage, software, and third-party operating platforms. For a full list of supported platforms and components, see the HP Insight Control Management Support Matrix.

Insight Control Management suite summary

Table 1 lists the components delivered and licensed with Insight Control Management that you can install using the Insight Control Management Integrated Installer. A bullet signifies that the component is part of the suite.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Licensed with ICE</th>
<th>Licensed with ICE-BL</th>
<th>Licensed with ICDC</th>
<th>Licensed with iPMP</th>
<th>Licensed with iPMP-BL</th>
<th>For more information, see chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insight Control</td>
<td>A wizard-based installer used by Insight Control Management suites to simplify the installation, configuration, and integration of HP SIM and Essentials software.</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>2</td>
</tr>
<tr>
<td>Management Integrated Installer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
<td>Licensed with ICE</td>
<td>Licensed with ICE-BL</td>
<td>Licensed with ICDC</td>
<td>Licensed with iPMP</td>
<td>Licensed with iPMP-BL</td>
<td>For more information, see chapter</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-----------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>HP Systems Insight Manager (HP SIM)</td>
<td>The central management server (CMS) that provides unified foundation management services for HP servers, storage, and network resources from a single console. HP SIM delivers centralized fault, configuration, inventory, performance management, warranty details, automated service call initiation and troubleshooting information. HP SIM is built according to industry standards to manage HP and non-HP infrastructure resources.</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>2, 8</td>
</tr>
<tr>
<td>HP Hotfix Update Kit for HP Systems Insight Manager 5.1</td>
<td>This kit installs improvements and bug fixes for HP Systems Insight Manager 5.1 or 5.1 with SP1. For detailed information, see the release notes.</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Extensions for HP SIM on Microsoft Windows</td>
<td>A software package that adds menus to HP SIM that access server management tools for HP-UX and Linux. The server management tools run on HP-UX and Linux managed systems, and include OpenView GlancePlus and HP-UX tools such as Ignite-UX, Software Distributor-UX, HP-UX configuration tools, and HP-UX Workload Manager. You license HP-UX and Linux server management tools separately (for example, as part of an HP-UX 11i operating environment).</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>3</td>
</tr>
<tr>
<td>HP BladeSystem Integrated Manager</td>
<td>Graphical user interface (GUI) used to discover, monitor, and administer HP BladeSystem enclosures and managed components, including servers (ProLiant and Integrity), storage, power, and cooling. This component is installed with HP SIM.</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>3</td>
</tr>
</tbody>
</table>
Table 1  HP components delivered and licensed with Insight Control Management suites

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Licensed with ICE</th>
<th>Licensed with ICE-BL</th>
<th>Licensed with ICDC</th>
<th>Licensed with iPMP</th>
<th>Licensed with iPMP-BL</th>
<th>For more information, see chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Insight Power Manager (IPM)</td>
<td>Power management application that extends HP SIM with power consumption and thermal output monitoring to optimize data center power and cooling. Includes power regulation policies for groups of HP ProLiant servers. This component is installed with HP SIM.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Integrated Lights-Out 2 Advanced</td>
<td>Integrated management processor for shared remote consoles that delivers remote control performance and ease of use suitable for routine and emergency server administration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Integrated Lights-Out 2 Select</td>
<td>Integrated management processor for ProLiant servers that deliver remote control performance and ease of use suitable for routine and emergency server administration in selected environments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>HP Service Essentials Remote Support Pack</td>
<td>Remote support tool that provides remote monitoring to supplement local monitoring of HP SIM. It also provides real-time hardware event monitoring and secure event submission to HP Support to help identify and prevent potentially critical problems on HP ProLiant servers, Linux-based Integrity servers, and their associated internal devices.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>HP Rapid Deployment Pack (RDP)</td>
<td>Tool that configures and deploys multiple servers quickly and predictably in an unattended fashion using scripts and system images. Includes predefined scripts to configure HP server hardware and deploy operating systems for Windows and Linux platforms.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>
### Table 1 HP components delivered and licensed with Insight Control Management suites

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Licensed with ICE</th>
<th>Licensed with ICE-BL</th>
<th>Licensed with ICDC</th>
<th>Licensed with iPMP</th>
<th>Licensed with iPMP-BL</th>
<th>For more information, see chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Insight Control Management Services</td>
<td>Management services that facilitate component integration and update. These services simplify assignment of Insight Control licenses to servers managed by HP SIM and identification of software updates.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>HP Insight Control Environment Advisor</td>
<td>Tool that automatically verifies the target platform for compliance with installation prerequisites. The advisor runs a series of tests on the server and identifies issues that might affect the Insight Control Management suite installation or operation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>HP Performance Management Pack (PMP)</td>
<td>Performance and monitoring tool that enables HP SIM to proactively detect, analyze, and report performance bottlenecks on HP ProLiant and Integrity servers, Modular Storage Array storage, and VMware and Microsoft Virtual Server virtual machines, ensuring server workloads run at peak performance levels.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>HP Vulnerability and Patch Management Pack (VPM)</td>
<td>Vulnerability and patch tool that integrates comprehensive vulnerability assessment and advanced patch management into HP SIM, to identify and resolve security vulnerabilities quickly and reliably in Microsoft Windows and Linux environments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>HP Virtual Machine Management Pack (VMM)</td>
<td>Virtual machine management tool that provides unified virtual machine management of physical and virtual server resources within HP SIM. Supports VMware™ and Microsoft virtual machine environments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2, 6</td>
</tr>
</tbody>
</table>

HP Server Migration Pack – Universal Edition Licensed and installed separately

HP Virtual Connect Enterprise Manager Licensed and installed separately

**NOTE:** You can install all components as part of an Insight Control Management suite installation, but you license the components separately.
Table 2 lists the HP component provided on the Insight Control Management DVD that can be installed and licensed separately.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Open Service Event</td>
<td>Event management software application that performs real-time SNMP service event filtering, analysis, event notification and reporting for supported systems (ProLiant and Integrity servers) running Insight Management Agents. When used with HP Service Essentials Remote Support Pack, OSEM can automatically send service event notifications to HP call centers when a system problem is detected.</td>
</tr>
<tr>
<td>Manager (OSEM)</td>
<td></td>
</tr>
</tbody>
</table>

Identifying and using suite icons

This user guide describes the processes and functions associated with Insight Control Management suites supported by the Insight Control Management DVD. Some processes and functions, such as installation, are common to all suites. Other processes and functions might apply to only some suites. The following icons appear at the beginning of each section to highlight content that applies to a specific Insight Control Management suite.

The blue ICE icon represents HP Insight Control Environment.

ICE

The light green ICE-BL icon represents HP Insight Control Environment for BladeSystem.

ICE-BL

The red ICDC icon represents HP Insight Control Data Center Edition.

ICDC

The dark green iPMP icon represents HP iLO Power Management Pack.

iPMP

The orange iPMP-BL icon represents HP iLO Power Management Pack for BladeSystem.

iPMP-BL

NOTE: No icons are applied when the content applies to all suites.
2 Installing, licensing, and configuring Insight Control Management software

This chapter provides procedures to successfully install Insight Control Management software.

Understanding the Insight Control Management software installation process

Software can be installed from the DVD using the integrated installer on the Install tab or individual component installers on the Products tab. The integrated installer can be configured to install suites and individual components.

Supported suites

The Insight Control Management integrated installer supports these suites:
- HP Insight Control Environment
- HP Insight Control Environment for BladeSystem
- HP Insight Control Data Center Edition
- HP iLO Power Management Pack
- HP iLO Power Management Pack for BladeSystem

Integrated installer components

The following components can be installed with the Insight Control Management integrated installer.
- HP SIM, including the following components:
  - OpenSSH
- HP System Management Homepage
- HP Version Control Repository Manager and HP Version Control Agent
- Windows Management instrumentation (WMI) Mapper
- HP BladeSystem Integrated Manager
- HP Insight Power Manager
- HP Service Essentials Remote Support Pack
- Extensions for HP SIM on Microsoft Windows
- HP Rapid Deployment Pack
- HP Performance Management Pack
- HP Vulnerability and Patch Management Pack
- HP Virtual Machine Management Pack
For a list of components included with each suite, see Table 1 in this guide.

**NOTE:** Virtual Machine Management Pack and Server Migration Pack were previously installed as Virtualization Management Software. Server Migration Pack has moved to the HP Server Migration Pack - Universal Edition Application and Boot CD. Server Migration Pack 2.2 or earlier will be uninstalled when Virtualization Management Software is upgraded to Virtual Machine Management Pack 3.0.

### Upgrading with Insight Control Management Integrated Installer components

Table 3 lists the Insight Control Management Integrated Installer component version numbers and their upgrades for this release. All installed components are automatically upgraded.

**Table 3** Insight Control Management component upgrades

<table>
<thead>
<tr>
<th>Component</th>
<th>From version</th>
<th>To version</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP SIM</td>
<td>5.0, 5.1 and 5.1 SP1</td>
<td>5.1 SP1 with hotfixes</td>
</tr>
<tr>
<td>HP BladeSystem Integrated Manager</td>
<td>2.1, 2.2, 2.3, 2.4, and 3.0</td>
<td>3.1</td>
</tr>
<tr>
<td>Extensions for HP SIM on Microsoft Windows</td>
<td>–</td>
<td>1.0</td>
</tr>
<tr>
<td>HP Rapid Deployment Pack (if installed on local server)</td>
<td>3.00, 3.10, 3.50, and 3.60</td>
<td>3.70</td>
</tr>
<tr>
<td>HP Insight Control Management Services</td>
<td>1.0, 1.0.2, 1.10, 1.11, and 2.00</td>
<td>2.10</td>
</tr>
<tr>
<td>HP Insight Control Environment Advisor</td>
<td>1.00</td>
<td>2.10</td>
</tr>
<tr>
<td>HP Insight Power Manager</td>
<td>1.0, 1.10, and 1.20</td>
<td>1.30</td>
</tr>
<tr>
<td>HP Performance Management Pack</td>
<td>4.0, 4.1, 4.1.1, 4.2, 4.3, 4.4, and 4.5</td>
<td>4.6</td>
</tr>
<tr>
<td>HP Vulnerability and Patch Management Pack</td>
<td>2.0, 2.0.1, 2.0.2, 2.0.3, and 2.1</td>
<td>2.1.1</td>
</tr>
<tr>
<td>HP Virtual Machine Management Pack</td>
<td>2.0, 2.0.1, 2.0.2, 2.1, 2.1.01, and 2.2</td>
<td>3.0</td>
</tr>
</tbody>
</table>

**NOTE:** Virtual Machine Management Pack and Server Migration Pack were previously installed as part of HP Virtualization Management Software. Server Migration Pack has moved to the HP Server Migration Pack - Universal Edition Application and Boot CD.

### Uninstalling Insight Control Management

If you must uninstall Insight Control Management, click **Start>Programs>Insight Control Management>Uninstall Insight Control Management**. When prompted to confirm the removal, click **Yes**. Only those components that were installed by Insight Control Management are uninstalled. Previously installed components are not uninstalled. A status window enables you to monitor the progress of components that are uninstalled.

You can also uninstall individual components separately using the Add/Remove Programs tool in Windows.
Insight Control Management integrated installation requirements

This section describes the installation requirements and provides preliminary information for Insight Control Management installation. The server on which the Insight Control Management suite is installed must meet the hardware and software requirements listed in the following tables. It is important to have this preliminary information available before beginning the installation process to reduce the time for installation.

Insight Control Management hardware installation requirements

Table 4 lists the hardware installation requirements for Insight Control Management.

### Table 4  Insight Control Management hardware installation requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>HP ProLiant BladeSystem c-Class or p-Class server blades, or HP ProLiant 300 and 500 series ML or DL servers</td>
</tr>
<tr>
<td>Memory</td>
<td>At least 2 GB RAM (4 GB RAM recommended)</td>
</tr>
<tr>
<td>Processor</td>
<td>At least 1.6 GHz (2 GHz or faster recommended)</td>
</tr>
<tr>
<td>Disk space</td>
<td>At least 5 GB for Insight Control Management software; however, more disk space is required for operating systems, logs, and patch databases (but if HP SIM and Rapid Deployment Pack are installed, only 2 GB are required)</td>
</tr>
<tr>
<td>File structure</td>
<td>New Technology File System (NTFS)</td>
</tr>
<tr>
<td>DVD drive</td>
<td>Local or mapped DVD drive required</td>
</tr>
</tbody>
</table>
## Insight Control Management software installation requirements

Table 5 lists the software installation requirements for Insight Control Management.

### Table 5  Insight Control Management software installation requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows Server™ 2003, Standard Edition SP1 or SP2 (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003™, Enterprise Edition SP1 or SP2 (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2, Standard Edition (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2, Enterprise Edition (32-bit only)</td>
</tr>
<tr>
<td>Services</td>
<td>Microsoft Internet Information Services (IIS) 6.0 installed and running with FTP service</td>
</tr>
<tr>
<td></td>
<td>ASP.NET 1.1, with .NET 1.1 Framework*</td>
</tr>
<tr>
<td></td>
<td>ASP.NET 2.0**</td>
</tr>
<tr>
<td></td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>TCP/IP with DNS installed so system names can be resolved to IP addresses</td>
</tr>
<tr>
<td></td>
<td>FTP service running on IIS (for Linux or VMware deployment)</td>
</tr>
<tr>
<td>Database</td>
<td>MSDE 2000 SP 3a (bundled with HPSIM) or one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2000 Standard Edition, SP3 or SP4 (for Standard Server operating system)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2000 Standard Edition, SP3 or 4 (for Standard Server operating system)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2000 Enterprise Edition with Service Pack 3 or 4 (for Advanced Server operating system)</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2005 running on Windows Server 2003</td>
</tr>
<tr>
<td>Applications</td>
<td>Microsoft Internet Explorer 6.0 SP1 or 7.0</td>
</tr>
<tr>
<td></td>
<td>Adobe® Acrobat® Reader</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 1.5.0.12 (not supported by all components)</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 2.0.0.4 (not supported by all components)</td>
</tr>
</tbody>
</table>

* ASP.NET 1.1 is not installed in Microsoft Internet Information Services (IIS) by default. For installation information, see the “ASP.NET 1.1 installation error” section in this guide.

** Rapid Deployment Pack requires .NET 2.0 Framework.

*** If SQL Server is not present, then Microsoft Data Engine (MSDE) 2000 SP3a is installed automatically.

**NOTE:** The CMS supports Windows 2000 and 2003 International Server – French, German, Italian, Spanish, and Japanese (latest service pack available for each language).
Insight Control Management configuration parameters

Before beginning the Insight Control Management integrated installation process, record the configuration parameters or configure the settings as listed in the following tables. Record the information in the Parameter column. The integrated installer uses this information to implement and configure HP SIM and the ProLiant Essentials products.

Configuration parameters vary depending on the components selected for installation and whether the selected component must be installed or upgraded.

You can install either by management suite or by customized component list. You can install one or more suites. You can select or clear components from the default selection list.

If you are installing Rapid Deployment Pack, then have your operating system media and Windows keys available so that you can use them during installation.

Before beginning installation, use the Insight Control Environment Advisor located on the DVD to verify that all prerequisites are met. The Insight Control Environment Advisor is a tool that verifies the target platform for compliance with installation prerequisites. To access this tool during installation, follow the link on the Warning screen of the Insight Control Management installer. The advisor runs a series of tests on the server and identifies issues that might affect the Insight Control Management suite installation or operation.

Table 6 Root installation directory and existing Rapid Deployment Pack configuration parameters

<table>
<thead>
<tr>
<th>Install/Reuse/ Upgrade</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install/Upgrade</td>
<td>List of suites and components to install</td>
<td>Select suites and components to install</td>
<td>You can install by suite or individual product. You can select more than one suite or component.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Installation directory</td>
<td>Any valid directory on the installation system (default is C:\Program Files\HP)</td>
<td>The directory where you want to install Insight Control Management components. Preinstalled components are upgraded in their current location. The installation directory cannot be changed for upgrades.</td>
<td></td>
</tr>
<tr>
<td>Install (local Rapid Deployment Pack)</td>
<td>Rapid Deployment Pack deployment network interface (used for PXE)</td>
<td>Select a detected NIC from the menu</td>
<td>The NIC that deploys images on the associated network. Deployment targets must be on the same network.</td>
<td></td>
</tr>
<tr>
<td>Reuse (remote Rapid Deployment Pack)</td>
<td>Existing deployment server host name or IP address</td>
<td>IP address ###.###.###.###, where ### ranges from 0 to 255, or a fully qualified host name</td>
<td>The host name or IP address of the existing Rapid Deployment Pack installation. This installation must be version 3.00 or later.</td>
<td></td>
</tr>
<tr>
<td>Reuse (remote Rapid Deployment Pack)</td>
<td>Existing Rapid Deployment Pack username</td>
<td>A valid, existing Rapid Deployment Pack username</td>
<td>The administrator username for the existing Rapid Deployment Pack installation</td>
<td></td>
</tr>
</tbody>
</table>
## Table 6  Root installation directory and existing Rapid Deployment Pack configuration parameters

<table>
<thead>
<tr>
<th>Install/Reuse/Upgrade</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reuse (remote Rapid Deployment Pack)</td>
<td>Existing Rapid Deployment Pack password</td>
<td>A valid, existing Rapid Deployment Pack password</td>
<td>The administrator password for the existing Rapid Deployment Pack installation.</td>
<td></td>
</tr>
<tr>
<td>Upgrade (local Rapid Deployment Pack)</td>
<td>Existing Rapid Deployment Pack username</td>
<td>A valid, existing Rapid Deployment Pack username</td>
<td>The administrator username for the existing Rapid Deployment Pack installation.</td>
<td></td>
</tr>
<tr>
<td>Upgrade (local Rapid Deployment Pack)</td>
<td>Existing Rapid Deployment Pack password</td>
<td>A valid, existing Rapid Deployment Pack password</td>
<td>The administrator password for the existing Rapid Deployment Pack installation.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Passwords must be alphanumeric characters or [ ], ( ), !, @, -, _, $, *, comma, period, and space. Do not use a space as the last character in the account password.
<table>
<thead>
<tr>
<th>Install/Reuse/ Upgrade</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Installing username</td>
<td></td>
<td>A valid, existing username with administrative privileges. When HP SIM is</td>
<td>The username for the administrator performing the installation. This administrator has full control of the HP SIM installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>being reused or upgraded, the username field is automatically populated with</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the username in use by HP SIM and cannot be changed.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Installing password</td>
<td></td>
<td>A valid password for the username</td>
<td>The password for the HP SIM administrator performing the installation.</td>
</tr>
<tr>
<td>Install</td>
<td>Domain</td>
<td></td>
<td>Domain account with administrator privileges in the local server or domain</td>
<td>When the server is part of a Windows domain, a domain account with administrative privileges in the local server can be used. In this case,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>name currently in use by HP SIM.</td>
<td>use the domain for the account provided in the username.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>When HP SIM is being reused or upgraded, the domain is automatically selected with the domain name in use by HP SIM and cannot be changed.</td>
</tr>
<tr>
<td>Reuse/Upgrade</td>
<td>Existing HP SIM</td>
<td>A valid HP SIM password</td>
<td>The password for the administrator account for the existing HP SIM installation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>password</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Passwords must be alphanumeric characters or [ ], ( ), !, @, -, _, $, *, comma, period, or space. Do not use a space as the last character in the account password.

**NOTE:** If HP SIM is already installed, then the Insight Control Management Integrated Installer reads the service and database credentials from the previous HP SIM installation. You must upgrade using these same credentials.
### Table 8  Database configuration parameters

<table>
<thead>
<tr>
<th>Install/Reuse</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Database type (MSDE or SQL Server)</td>
<td>Install MSDE or use existing SQL or MSDE database</td>
<td>The installer installs MSDE locally or uses an existing SQL or MSDE database.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Database username</td>
<td>A valid user with database administrator privileges (required to create databases)</td>
<td>The username for database access (Windows authentication). User must have administrative privileges to the database and CMS.</td>
<td></td>
</tr>
<tr>
<td>Install/Reuse</td>
<td>Database password</td>
<td>Valid password for database administrative user</td>
<td>The password for database access (Windows authentication). User must have administrative privileges to the database and CMS.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Database domain</td>
<td>Windows domain</td>
<td>The Windows domain for the database server</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Database hostname</td>
<td>Valid hostname</td>
<td>The host name or IP address of the database server</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Database instance name</td>
<td>Valid database instance. Leave blank to use the default instance</td>
<td>The existing database instance name (optional)</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Database port</td>
<td>Range: 65535; default: 1433</td>
<td>The database port to be used for the components</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Passwords must be alphanumeric characters or [ ], ( ), !, @, ., _, $, *, comma, period, or space. Do not use a space as the last character in the account password.

**NOTE:** If HP SIM is already installed, the Insight Control Management Integrated Installer reads the service and database credentials from the previous HP SIM installation. You must upgrade using these same credentials.
### Table 9  Automatic login after reboot

<table>
<thead>
<tr>
<th>Install/Reuse</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install/Upgrade</td>
<td>Enable automatic logon</td>
<td>Yes or No</td>
<td>A reboot might be required after installing or upgrading HP SIM or RDP. To enable an automatic login to continue the installation after the reboot, provide credentials for a one-time login.</td>
<td></td>
</tr>
<tr>
<td>Install/Upgrade</td>
<td>Logon password</td>
<td>Valid password for the current installation user.</td>
<td>The password for the current user that will be used to logon after the reboot.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** Passwords must be alphanumeric characters or [ , ] , (, ), !, @, -, _, $, *, comma, period, and space. Do not use a space as the last character in the account password.

### Table 10  Extensions for HP SIM on Microsoft Windows and configuration parameters

<table>
<thead>
<tr>
<th>Install</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Extensions for HP SIM on Microsoft Windows</td>
<td>Ignite-UX and Software Distributor (HP-UX)</td>
<td>Yes or No</td>
<td>Installs menu items for Ignite-UX and Software Distributor (HP-UX) product.</td>
<td></td>
</tr>
<tr>
<td>Install Extensions for HP SIM on Microsoft Windows</td>
<td>Ignite and Software Distributor server IP address or hostname</td>
<td>IP address is ###.###.###.###, where ### ranges from 0 to 255, or the name of a valid, fully-qualified host HP-UX server where Ignite server and depots to be used by Software Distributor server are installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install Extensions for HP SIM on Microsoft Windows</td>
<td>Configure secure shell (SSH) access</td>
<td>Yes or No</td>
<td>You must have secure shell access between HP SIM and the Ignite server for the Ignite integration to work. This option enables you to set up security for this access. You can also configure secure shell access from HP SIM later.</td>
<td></td>
</tr>
<tr>
<td>Install Extensions for HP SIM on Microsoft Windows</td>
<td>SSH username</td>
<td>Valid HP-UX user in Ignite Server</td>
<td>This is the user that is configured for SSH access.</td>
<td></td>
</tr>
</tbody>
</table>
Table 10 Extensions for HP SIM on Microsoft Windows and configuration parameters

<table>
<thead>
<tr>
<th>Install Item</th>
<th>Parameter</th>
<th>Possible value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH password</td>
<td>Valid HP-UX password on Ignite Server</td>
<td>This is the password that is used to configure SSH access.</td>
</tr>
<tr>
<td>Authentication—Choose host-based or each user</td>
<td>Checkbox to indicate the level of SSH access to set up</td>
<td>Host-based enables HP SIM to connect to Ignite and SD server on the remote server on behalf of all users authorized to use those tools by the HP SIM authorization mechanism. The user must have root access for this option. If you choose Each user, only the user you configure will have access to run any tools from HP SIM to the Ignite or SD server. To add other users from the HP SIM GUI, select Configure&gt;Configure or Repair Agents.</td>
</tr>
<tr>
<td>HP-UX Configuration</td>
<td>Yes or No</td>
<td>Installs menu items for HP-UX Configuration tools (kernel configuration, disks and file systems, peripherals and devices, and users and groups).</td>
</tr>
<tr>
<td>HP-UX Workload Manager</td>
<td>Yes or No</td>
<td>Installs menu items for HP-UX Workload Manager product. This product should be installed on the HP-UX managed node.</td>
</tr>
<tr>
<td>OpenView GlancePlus (Glance) for HP-UX and Linux</td>
<td>Yes or No</td>
<td>Installs menu items for OpenView GlancePlus product for HP-UX and Linux. This product should be installed on the HP-UX and Linux managed nodes.</td>
</tr>
</tbody>
</table>
Table 10  Extensions for HP SIM on Microsoft Windows and configuration parameters

<table>
<thead>
<tr>
<th>Install</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Username for</td>
<td>Username for</td>
<td>Valid HP-UX username on managed systems</td>
<td>This logon is used to invoke Glance on a managed system when Glance tools are launched.</td>
</tr>
<tr>
<td>Install</td>
<td>Glance logon to target systems</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 11  Proxy configuration parameters

<table>
<thead>
<tr>
<th>Install</th>
<th>Item</th>
<th>Parameters</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>I use an HTTP proxy server</td>
<td>Select the checkbox if your</td>
<td></td>
<td>If your environment requires a proxy to access the Internet, the installer configures your proxy settings for the Insight Control Software Update Utility and Vulnerability and Patch Management. You can configure this setting during or after installation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>environment requires a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>proxy server for Internet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Proxy host</td>
<td>IP address</td>
<td></td>
<td>The hostname for proxy server. (Insight Control Management Software Update and Vulnerability and Patch Management Pack must access the Internet for updates.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>###.###.###.###, where</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>### ranges from 0 to 255 or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>the name of a valid, fully-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>qualified host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Proxy port</td>
<td>Valid port number ranging</td>
<td></td>
<td>The port for proxy server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>from 0 to 65535</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>My proxy requires authentication</td>
<td>Yes or No</td>
<td></td>
<td>If the proxy requires authentication, select the checkbox. Only basic (not encrypted) authentication is supported.</td>
</tr>
<tr>
<td>Install</td>
<td>Proxy username</td>
<td>Valid proxy username</td>
<td></td>
<td>The username for proxy authentication</td>
</tr>
<tr>
<td>Install</td>
<td>Proxy password</td>
<td>Valid proxy password</td>
<td></td>
<td>The password for proxy authentication</td>
</tr>
</tbody>
</table>
## Table 12 Installing or upgrading Rapid Deployment Pack configuration parameters

<table>
<thead>
<tr>
<th>Install</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install/Upgrade</td>
<td>Rapid Deployment Pack</td>
<td>Operating systems to load into Rapid Deployment Pack (media must be supplied) optional but recommended</td>
<td>A list of operating systems can be selected. Physical media or a directory location must be provided</td>
<td>The operating systems to be deployed in the future. These operating systems can be Windows, Linux, or VMware ESX systems. Load these system images so that their location can be verified, license keys can be entered, and associated ProLiant Support Packs can be made ready for installation. Loading these system images ensures that deployment payload data is given to RDP target systems.</td>
</tr>
<tr>
<td>Install Rapid</td>
<td>Create IIS FTP virtual directory named DSLIB required if VMware or Linux is to be deployed</td>
<td>Yes or No</td>
<td>To perform VMware or Linux deployments, an FTP server must be available before beginning the installation process. To set up the FTP server, from the Windows start menu, select Control Panel&gt; Add/Remove Programs.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Windows Server 2000 product key (optional)</td>
<td>A valid Windows Server 2000 key</td>
<td>This key deploys Windows Server 2000. For more information, see your Microsoft licensing agreement.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Windows Server 2003 product key (optional)</td>
<td>A valid Windows Server 2003 key</td>
<td>This key deploys Windows Server 2003. For more information, see your Microsoft licensing agreement.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Windows Server 2003 x64 product key (optional)</td>
<td>A valid Windows Server 2003 key</td>
<td>This key deploys Windows Server 2003 x64. For more information, see your Microsoft licensing agreement.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Windows Server 2003 IA64 product key (optional)</td>
<td>A valid Windows Server 2003 key</td>
<td>This key deploys Windows Server 2003 ia64. For more information, see your Microsoft licensing agreement.</td>
<td></td>
</tr>
<tr>
<td>Install Rapid</td>
<td>SNMP setting for deployed targets</td>
<td>Up to 32 characters and including the following: uppercase and lowercase alphanumeric, hyphen, or underscore. Do not include spaces. Default: public.</td>
<td>The SNMP string that is used for managing deployed targets. This string is used on the community string of all deployed targets.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 13  Protocol, community string, and discovery configuration parameters

<table>
<thead>
<tr>
<th>Install/Upgrade</th>
<th>Item</th>
<th>Parameter</th>
<th>Possible value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install HP SIM</td>
<td>Global protocol settings (recommended)</td>
<td>Up to four username and password pairs used to remotely access the systems you are attempting to manage</td>
<td>The WBEM credentials enable authentication of WBEM to enable access to management information.</td>
<td></td>
</tr>
<tr>
<td>Install HP SIM</td>
<td>SNMP community string (recommended)</td>
<td>Up to 32 characters and including the following: uppercase and lowercase alphanumeric, hyphen, or underscore. Do not include spaces.</td>
<td>The SNMP community string enables authentication of SNMP messages. If you have SNMP systems and you do not enter read community strings that match these systems, HP SIM does not discover them.</td>
<td></td>
</tr>
<tr>
<td>Install HP SIM</td>
<td>HP SIM Discovery range (recommended)</td>
<td>###.###.###-###.###, where ### ranges from 0 to 255. Multiple ranges can be specified by separating them with white space (tabs, new lines, and spaces).</td>
<td>The range of IP addresses on which HP SIM attempts to discover devices. A large IP address range takes longer to discover than a targeted range. Starting a discovery process from the integrated installer initiates the population of the database. Scheduled discoveries can be set up during the HP SIM post-installation configuration process.</td>
<td></td>
</tr>
</tbody>
</table>
Installation times for Insight Control Management components

Table 14 lists the approximate installation times for the Insight Control Management components on a HP ProLiant BL35p server blade with 2 GB of RAM. Installation times using other servers and memory sizes might vary. An active virus scanner might slow down the installation time.

<table>
<thead>
<tr>
<th>Component</th>
<th>Installation time</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management Homepage</td>
<td>1 minute</td>
</tr>
<tr>
<td>WMI Mapper</td>
<td>1 minute</td>
</tr>
<tr>
<td>HP Systems Insight Manager</td>
<td>7 minutes</td>
</tr>
<tr>
<td>Version Control Repository</td>
<td>1 minute</td>
</tr>
<tr>
<td>Rapid Deployment Pack</td>
<td>28 minutes</td>
</tr>
<tr>
<td>Reboot for install or upgrade</td>
<td>4 minutes</td>
</tr>
<tr>
<td>HP Insight Power Manager</td>
<td>3 minutes</td>
</tr>
<tr>
<td>HP Service Essentials Remote Support Pack</td>
<td>3 minutes</td>
</tr>
<tr>
<td>Performance Management Pack</td>
<td>3 minutes</td>
</tr>
<tr>
<td>Extensions for HP SIM on Microsoft Windows</td>
<td>1 minute</td>
</tr>
<tr>
<td>HP BladeSystem Integrated Manager</td>
<td>2 minutes</td>
</tr>
<tr>
<td>Hotfix Update Kit for HP Systems Insight Manager 5.1</td>
<td>2 minutes</td>
</tr>
<tr>
<td>Insight Control Management Services</td>
<td>3 minutes</td>
</tr>
<tr>
<td>HP Rapid Deployment Pack SIM Integration Module</td>
<td>1 minute</td>
</tr>
<tr>
<td>Vulnerability and Patch Management Pack</td>
<td>7 minutes</td>
</tr>
<tr>
<td>Virtual Machine Management Pack</td>
<td>3 minutes</td>
</tr>
<tr>
<td>Insight Control Environment Advisor</td>
<td>2 minutes</td>
</tr>
<tr>
<td>Product configuration</td>
<td>4 minutes</td>
</tr>
<tr>
<td>Total installation time (including a delay to reboot)</td>
<td>76 minutes</td>
</tr>
</tbody>
</table>
Performing an Insight Control Management integrated installation

**IMPORTANT:** Be sure that either maintenance activities will not reboot the system during installation.

The Insight Control Management integrated installation is completed in a single process, with all Insight Control Management software components installed on a single management server. Variations to this installation process might occur under any of the following scenarios:

- If HP SIM 5.0 or higher is already installed, Insight Control Management and all its components are installed on the HP SIM Central Management Server (CMS). If necessary, HP SIM and all of its components are updated to the latest version.
- If the Rapid Deployment Pack 3.00, 3.10, 3.50, or 3.60 is installed on your HP SIM CMS, Insight Control Management upgrades Rapid Deployment Pack to version 3.70.
- If the Rapid Deployment Pack 3.70 is already installed in your environment, you can provide the Insight Control Management installer with information to incorporate your existing Rapid Deployment Pack installation. In this configuration, the Rapid Deployment Pack 3.70 can reside on the same server or on a different server from the HP SIM CMS.
- If neither HP SIM nor the Rapid Deployment Pack is present, both components are installed, along with the other Insight Control Management components, during the Insight Control Management integrated installation process.

**IMPORTANT:** Before performing the Insight Control Management integrated installation process, identify the preliminary information as listed in the “Insight Control Management configuration parameters” section in this guide. Having this information available before beginning the installation process reduces the time needed for installation.

**IMPORTANT:** Microsoft IIS 6.0 or later must be installed on the target CMS to successfully install and use the Vulnerability and Patch Management Pack. HP strongly recommends enabling HTTPS if HP SIM and VPM are installed on separate servers. For more information about configuring HTTPS service in IIS, see [http://support.microsoft.com/?kbid=324069](http://support.microsoft.com/?kbid=324069).

**NOTE:** Before beginning the installation process, identify all operating systems to be deployed.

You can install or upgrade an Insight Control Management suite either by management suite or by customized product list, selecting one or more suites or components for installation. Individual components may also be installed or upgraded using the integrated installer.

To install Insight Control Management:

1. Insert the Insight Control Management DVD into the DVD-ROM of the intended management server. The End User License Agreement appears. Read the agreement, and then to continue, click **Agree**.
2. The Welcome screen appears. To ensure that your environment meets the appropriate installation requirements, click **Run Insight Control Advisor**.

3. The Insight Control Environment Advisor page appears. The Insight Control Environment Advisor is a tool that verifies the target platform for compliance with installation prerequisites. Click **Run Now**.
4. The Insight Control Environment Advisor results screen identifies issues that could affect the installation of the Insight Control Management suite. The following example screen shows two items that could affect the installation of the Insight Control Management suite. For more information on those issues, click the corresponding hyperlinks, and then resolve the issues. To proceed, click Run Now.

![Insight Control Environment Advisor](image)

5. The Welcome screen reappears. Click Review Installation Checklist. A PDF of the Insight Control Management Installation Checklist appears. You must identify the configuration parameters or configure the settings as listed in the checklist. The integrated installer uses this information to implement and configure HP SIM and the ProLiant Essentials products.
6. Click **Run Integrated Installer.** The Welcome screen appears. Choose either of the following options:

- To install by management suite, select **management suite**, click **Next**, and then go to step 4.
- To install by customized product list, select **customized list**, click **Next**, and then go to step 5.

If you need help at any time during the installation process, click the ? icon.
7. When installing by management suite, the Select installation by management suite screen appears. Select the corresponding checkboxes of suites to install. This action automatically selects the appropriate components for installation. Previously installed components are automatically upgraded to the revisions provided. Components have expandable lists that enable you to see the list of components, as shown in the following figure. You can customize the default component selections in the next step.

NOTE: The ProLiant (Windows and Linux) targets checkbox is automatically selected when Insight Control Environment for BladeSystem is selected. This checkbox can be cleared if you are not managing ProLiant systems (that is, managing all Integrity blades).

8. When installing by customized product list or continuing with a management suite installation, the Select components for install or upgrade screen appears. Select the corresponding checkboxes of components to install, and then click Next. Components have expandable lists that enable you to see their descriptions. The installer detects components already installed and uses or upgrades those components if they are the correct version or can be upgraded. Checkboxes for required components and previously installed components cannot be cleared.
9. The Warning screen appears, listing the system prerequisites for installation. Your system must meet all these prerequisites. Prerequisites are based on selections from step 5. To use the Insight Control Environment Advisor to verify prerequisite status, click the run the Insight Control Environment Advisor hyperlink provided at the bottom of the screen.

**IMPORTANT:** The installation server IP address is assigned by Dynamic Host Configuration Protocol (DHCP). The IP address must not be changed.

10. Click Next. The installation directory screen appears.
11. Select the installation location by performing either of the following steps:
   - To use the default directory location, click **Next**.
   - To select a different directory, click **Browse**, or enter the path in the **Installation Directory** box. Click **Next**.

   If you previously installed Insight Control Management, then the installation directory remains the same and cannot be changed. If you have already installed a component outside of Insight Control Management, then the integrated installer upgrades that component in the original component location.
12. If you have selected Rapid Deployment Pack and it is not already installed, then you must choose to install the Rapid Deployment Pack on this server or use Rapid Deployment Pack on an existing remote server. Choose either of the following options:
   ○ To install on this server, select **Install Rapid Deployment Pack on this server**, and then select the deployment network interface to be used by Preboot eXecution Environment (PXE).
   ○ To use the Rapid Deployment Pack already installed on an existing remote server, select **Use existing remote Rapid Deployment Pack**, and then enter the credentials.

**IMPORTANT:** If you use an existing remote Rapid Deployment Pack server, then DHCP services must be running on your network to operate properly.

Click **Next**.

13. If the locally installed Rapid Deployment Pack must be upgraded, the **Use existing HP ProLiant Essentials Rapid Deployment Pack** screen appears. Enter the service credentials, and click **Next**.
14. From the Service account credentials screen, enter the credentials, and then click **Next**. All Insight Control Management components use these credentials. If HP SIM is already installed, then the Username and Domain box are automatically populated.

15. From the Database configuration screen, depending on whether the local database is detected, perform either of the following steps:
   - If a local database is detected, enter the credentials for the existing database, and then click **Next**.
   - If no local database server is detected, select the appropriate option to install MSDE, or enter the name of a remote database server:
     - To install Microsoft SQL Desktop Edition, select **Install and use MSDE**.
     - To use and existing SQL Server or MSDE, select **Use existing SQL/MSDE database**.

   Enter the password. To use an existing database, you must provide the server and database information. Entering Instance Name is optional. Click **Next**.
16. (Optional) From the Automatic logon configuration screen, to enable automatic logon after the installation reboot, select Enable Automatic Logon, and then provide logon credentials. These credentials are used only for the reboot initiated during the installation process.

The Automatic logon configuration screen appears only if HP SIM or Rapid Deployment Pack is installed or upgraded because the system requires a reboot during the installation process.

![Automatic logon configuration screen]

17. From the Extensions for HP SIM on Microsoft Windows configuration screen, select the desired tools, and then provide the required information. Click Next.

- If you select Ignite-UX and Software Distributor (HP-UX), then you must provide the Ignite and software distributor server IP address or host name. If you select Configure secure shell (SSH) access, you must provide the username and password.
- If you select OpenView GlancePlus for HP-UX and Linux, then you must provide the username for logon to target systems. The default is root.
18. If your network requires a proxy server to access the Internet, then enter the proxy settings in the boxes on the Proxy Configuration screen. VPM uses these settings to acquire patches, while Insight Control Management uses them to verify new component versions. If your network does not use a proxy or you do not intend to use this feature, then you can omit this step. Click **Next**.

19. (Optional) If you are installing Rapid Deployment Pack, from the Deployment operating systems screen, select all operating systems to deploy using Rapid Deployment Pack, and then click **Copy Files**. To quickly select or clear all options, select the **Check/uncheck all** checkbox. You are prompted to provide the media or location for each operating system. When you finish copying files, click **Next**.

**IMPORTANT:** If you omit step 15, to deploy a system, you must add these files later. For more information, see “Appendix C Installing additional operating systems to be deployed by Rapid Deployment Pack” in this guide.
20. If you are installing Rapid Deployment Pack, from the Deployment configuration options screen, then specify the configuration options for Rapid Deployment Pack, and then click Next.

**NOTE:** Obtain Windows operating system product keys from Microsoft.

21. (Optional) If you are installing HP SIM, from the Basic settings for HP Systems Insight Manager screen, enter the global protocol settings (the WBEM credentials) and the SNMP default read community string. These credentials enable access management targets. Click Next. HP recommends performing this step at this time, although you can provide these values later through HP SIM. You can also add additional global settings or individual system settings in HP SIM.
22. (Optional) If you are installing HP SIM, the Discovery settings for HP Systems Insight Manager screen appear. Enter at least one IP address range that includes the devices for network discovery to find. To enter multiple ranges, separate the ranges with white space (for example, tabs, new lines, or spaces). Click **Next**. HP recommends performing this step so that HP SIM discovers devices faster. This discovery is a one-time discovery. For more information about performing and scheduling discoveries, see the **HP Systems Insight Manager User Guide**.

![Discovery Settings Screen](image)

23. From the Installation summary screen, verify that the actions are correct, and then click **Install**. An estimated install time is provided based on the installation selections.

**IMPORTANT:** The system automatically reboots after the HP SIM and RDP components are installed or upgraded.

![Installation Summary Screen](image)
24. To access HP SIM after the installation completes, click the **Click here to access HP Systems Insight Manager** hyperlink. Use the credentials provided during installation to log in to HP SIM. When a user with full configuration rights logs in to HP SIM for the first time, the HP Systems Insight Manager Registration window appears. Register HP SIM now, or click **Register Later**. If you do not have Internet access, click **Register Later**.

A task is scheduled to check for Insight Control Management component updates once immediately after installation and then weekly thereafter. If updates are available, an event with component download information is logged in the HP SIM events list.

### Checking for software updates

The Insight Control Management Software Update utility connects to the HP website to verify for new releases of the components installed by Insight Control Management. If newer versions of installed components are available, the utility provides links to the downloads, component status, version numbers, and release dates. DVD update notifications are also provided for new DVDs. Access the links to download and manually install the updates.

A task is scheduled to check for Insight Control Management component updates weekly. If updates or new components are available, then an event with component download information is logged in the HP SIM events list.
To check for updates or modify the scheduled task, click **Tools>Insight Control Management> Software Updates**.

1. (Optional) If you use a proxy server, select the appropriate checkboxes, and then enter your configuration information. If the proxy server requires authentication, select the appropriate checkbox, and then enter your user credentials. Only basic (nonencrypted) authentication is supported. Click **Apply**. This information has to be entered only once.

2. To check for results, click **Check for Updates Now**. A list of available updates appears. To modify the scheduled task, click **Schedule**. The HP SIM task scheduler appears.
3. The results table includes the product name, installation status, version number, release date, and a link to download information. In the Download column, click on Installer or DVD to view new product information and access the download. A record of available updates is in the HP SIM events list in the left pane. To display the All Events page, click All Events. The right pane on the Check for HP Insight Control Component Updates screen shows the version number and includes a link to download information.

Performing post-installation configuration tasks

This section describes the procedures for performing post-installation configuration tasks for Insight Control Management suites.

**IMPORTANT:** The Getting Started screen appears after the Insight Control Management suites are installed. The information on this screen assists you in performing post-installation configuration tasks.

Post-installation configuration tasks include the following:

1. Checking for software updates (see the “Checking for software updates” section in this guide)
2. Performing HP SIM initial setup tasks
3. Configuring the HP Service Essentials Remote Support Software Pack
4. Performing additional Vulnerability and Patch Management Pack post-installation configuration tasks
5. Performing Insight Power Manager post-installation configuration tasks
6. Configuring domain accounts for Rapid Deployment Pack
7. Setting up virtual machine hosts for Virtual Machine Management Pack
Deploying the VMM Agent

You can deploy the VMM Agent manually or from HP SIM. This section includes instructions for various methods of deploying agents using manual deployment or from HP SIM.

NOTE: The communication between the agents during a copy or move is not encrypted. Agents use the certificate that shipped with the product instead of generating certificates.

Manual registration of virtual machine hosts

The following topics explain how to deploy agents manually.

Registering Windows virtual machine hosts

1. Log in to HP SIM on the HP SIM CMS, from an account with administrator privileges.
2. Locate the cms.cer file in the VMM installation lib directory on the CMS. The default path is C:\Program Files\HP\Virtual Machine Management Pack\lib.
3. Zip the file, and transfer it from CMS to the virtual machine host over a secure channel to the C:\Documents and Settings\Administrator folder. Unzip the file in this location.
4. Locate the importcert.bat file in the VMM installation bin directory from the default path: C:\Program Files\HP\Virtual Machine Management Pack\bin. Transfer the file to C:\Documents and Settings\Administrator folder on the virtual machine host.
5. After these files are transferred successfully, access the command prompt on the virtual machine host and run the importcert.bat file to import the CMS certificate into the VMM truststore.
6. On CMS, access the VMM installation bin directory using the default Path: C:\Program Files\HP\Virtual Machine Management Pack\bin, and then register the virtual machine host by executing the following command: vmcli -registerAgent <URI agent>

Registering VMware ESX hosts

1. Log in to HP SIM on the HP SIM CMS, from an account with administrator privileges.
2. Locate the cms.cer file in the VMM installation lib directory on the CMS. The default path is C:\Program Files\HP\Virtual Machine Management Pack\lib.
3. Zip the file and transfer it from CMS to the virtual machine host over a secure channel to the /root folder on the virtual machine host, and then unzip the file.
4. Locate the importcert.sh file in the VMM installation bin directory from the default path: C:\Program Files\HP\Virtual Machine Management Pack\bin. Transfer the file to the /root folder on the virtual machine host.
5. After these files are transferred successfully, access the command prompt on the virtual machine host and run the importcert.sh file to import the CMS certificate into the VMM truststore.
6. On CMS, access the VMM installation bin directory using the default Path: C:\Program Files\HP\Virtual Machine Management Pack\bin, and then register the virtual machine host by executing the following command: vmcli -registerAgent <URI agent>
Deployment of VMM Agent from HP SIM

The following topics explain various aspects of VMM Agent deployment with OpenSSH.

Installing OpenSSH on HP SIM CMS and Windows-based virtual machine hosts

OpenSSH provides secure communications between the virtual machine host and the CMS by encrypting online traffic to eliminate network-level attacks. You must install OpenSSH on Windows hosts and HP SIM CMS before you can deploy the VMM Agent from the CMS.

1. Be sure the system rebooted after an installation of HP SIM.
2. Log in to HP SIM from an account with administrator privileges.
3. Select Deploy>Deploy Drivers, Firmware and Agents>Install OpenSSH.
4. Click the HP SIM help icon, and follow the on-screen instructions to complete the installation.

Configuring OpenSSH

For VMware ESX Server 3.0 or later, the root login for OpenSSH is disabled by default. OpenSSH is required only if deploying through CMS.

To enable the root access for OpenSSH:

1. Edit the /etc/ssh/sshd_config file from VMware ESX Server, and change the parameter of PermitRootLogin to Yes.
2. Restart the OpenSSH service - /etc/init.d/sshd restart.

To configure OpenSSH:

1. Verify that OpenSSH is installed on the virtual machine host.
   a. In the HP SIM All System page, click the System Name entry for the virtual machine host to verify. The System Page appears.
   b. Expand the product description. The management protocols display the following:
      SSH: SSH-2.0-OpenSSH_xx.1p1, where xx is the version number.
      If OpenSSH is already installed, it must be configured on both Windows and Linux virtual machine hosts.

2. Configure OpenSSH using the mxagentconfig command. From the command prompt, enter:
   mxagentconfig –r -n <host IP address>
   mxagentconfig –a -n <hostname> -u <username> -p <password>

   For more information about the mxagentconfig command, go to the HP SIM online help, and search for keywords “Getting started using command line interface commands.”

Deploying the VMM Agent from the HP SIM menu

OpenSSH must be configured properly and running on both the HP SIM CMS and the selected target virtual machine hosts to deploy the VMM Agent.

1. Log in to HP SIM from an account with administrator privileges.
2. Select Deploy>Deploy Drivers, Firmware and Agents>Install VMM Agent from the HP SIM toolbar, and select Linux or Windows.
3. Select the target virtual machine hosts by selecting the appropriate systems.
4. Click Apply.
5. (Optional) To add targets, click **Add Targets**, or to remove targets, click **Remove Targets**. Click **Next**.
6. To deploy the VMM Agent immediately, click **Run Now**, or to deploy the VMM Agent to selected virtual machine hosts later, click **Schedule**.
7. View task results in the HP SIM task logs.

**Post-installation configuration tasks**

**Configuring VMware VirtualCenter**

To configure the VMware VirtualCenter, select **Options>Virtual Machine Management>Security>VMware® VirtualCenter Settings**.

This configuration is required for Live Move, which uses VMware VMotion™ Technology.

The Virtual Machine Management Pack supports VirtualCenter Version 1.x, 2.0.x, and 2.x. However, only one version of VirtualCenter can be registered at a time. Select the appropriate version of VirtualCenter.

![VirtualCenter Settings](image)

Previously saved values, such as user name, service URL, and version appear when you revisit this page. The password box is always blank when you revisit this page.

When you load the page, the connection is automatically tested with the stored values.

- The question mark icon (?) indicates that no credentials are present.
- The red X icon (❌) indicates that the connection is failing.
- The green check icon (✔) indicates that the connection is working.

The test connection repeats the check with the information given on the page (the password must be supplied). The text is changed accordingly.

To save the latest information, click **Save**.
Post-upgrade configuration task

Perform the following procedure.

Upgrading the VMM Agent

You must upgrade the VMM Agent to maintain all associated information in the database, including all HP SIM associations and scheduled task data.

You can upgrade the VMM Agent only after a Virtual Machine Management Pack upgrade. To upgrade the VMM Agent:

2. To deploy the agent immediately, click Run Now, or to deploy the agent later, click Schedule.

Performing HP SIM initial setup tasks

HP SIM initial setup tasks include the following:

1. Enabling system automatic discovery
2. Adding users to the Central Management Server
3. Configuring e-mail settings
4. Setting up managed systems
5. Configuring protocol settings
Enabling system automatic discovery

HP SIM uses automatic discovery to find and identify systems on the network. The System Automatic Discovery task is enabled during installation. If you select this task, it runs when installation is completed and populates the HP SIM database. A system must first be discovered for HP SIM to collect data and track system status. To discover new systems, use either of the following methods:

- Automatic discovery—This process enables HP SIM users to find and identify the systems on your network to populate the database with that information. A system must first be discovered to collect data and track system status.
- Manual discovery—This process enables you to bypass a fully automatic discovery and add single and multiple systems to the database, create or import the HP SIM database Hosts file, and create or import a generic Hosts file.

If you do not perform an automatic discovery during the installation, then you must configure general settings for automatic discovery. To initially configure general settings for automatic discovery:

1. Configure global Web Based Enterprise Management (WBEM) credentials to enable access to target systems.
   a. Select **Options>Protocol Settings>Global Protocol Settings**.
   b. Configure your WBEM settings by entering the user name and password needed to authenticate remote systems. These settings are used for discovery and by the Vulnerability and Patch Management Pack. Choose one of the following options:
      - If the Vulnerability and Patch Management Pack is on the HP SIM server, then enter the user account without the domain name.
      - If the Vulnerability and Patch Management Pack is on a separate server, then enter the user account with the domain name (DOMAIN\user account). If you are managing Windows and Linux servers, enter the Windows administrator account credentials in the Default 1 box and Red Hat administrator group credentials in the Default 2 box.
   c. Click **OK**.

2. Configure SNMP to enable the sending of messages to different parts of a network. For more information, see the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*.

3. Select **Options>Discovery**. The Discovery page appears with the Automatic tab selected.

4. In the For all automatic discoveries section, select **Configure general settings**. The General Settings section appears.

5. Select **Automatically discover a system when an event is received from it**. This option enables systems to be discovered when a trap or some other supported event is received by HP SIM. The option uses the discovery filters and IP address exclusion ranges for additional filtering of these events.
6. Verify that the Automatically discover a server blade when its Integrated Lights Out management processor is identified box is selected. This option adds servers that were indirectly discovered through its management processor. When these servers are discovered, they are listed in a Disabled state on the system table view page and the only information that appears is the system serial number and the association to the Integrated Lights-Out (iLO) and the enclosure. Two additional options are included with this step:
   a. **Discover systems in an enclosure when Onboard Administrator is discovered.** Use this option to add systems known by the Onboard Administrator, even if those systems are not in the configured discovery range.
   b. **Automatically discover HPVM guest(s) when the host is identified.** Use this option to add all HP Integrity Virtual Machine (HPVM) guest systems to the HP SIM database when the HPVM host system is discovered and identified.

7. In the Ping exclusion ranges, templates, and hosts files boxes, specify the IP addresses, templates, or host files containing IP addresses to exclude from the automatic discovery process. This setting applies to both range pinging and event-based autodiscovery.

   **IMPORTANT:** When discovering clusters, the ping inclusion range must include the IP addresses of the cluster members.

8. Select the **Enable discovery filters** checkbox.

9. In the Discover the following system types section, select the type of systems to be discovered.

   **IMPORTANT:** When discovering clusters, you must include the server system type so that the cluster members are not filtered out.

   **NOTE:** The Discover the following system types section is available only when you select the Enable discovery filters checkbox.

10. In the Limit discovery to systems that meet the following criteria section, choose one of the following options:
    o Any system that matches the listed filters when the Enable discovery filters checkbox is selected
    o All manageable systems (WBEM, SNMP, Desktop Management Interface [DMI], WMI, or HTTP support)
    o Manageable systems with HP agents only

   **NOTE:** The Manageable systems with HP agents only option is only available when you select the Enable discovery filters checkbox.

11. To save your settings, click **OK.**
Adding users to the Central Management Server

In HP SIM, user administration involves adding, editing, and removing users. To configure users, select **Options>Security>Users and Authorizations.** Additional configuration options such as user groups and reports are available in the GUI.

Creating users

1. Select the Users tab, and then click **New.** The New User section appears.
2. In the Login name [on central management server (CMS)] box, you must enter the operating system login account name to be used to log in to HP SIM.

   **NOTE:** You cannot log in to HP SIM if the account is not a valid login. The account is not validated until you attempt to log in to HP SIM.

3. In the Domain (Windows domain for login name) box, enter the Windows domain name for the login name if the CMS is running a Windows operating system. If left blank, the system name of the CMS is used as the domain.
4. (Optional) Enter the user’s full name, phone number, and e-mail address in the appropriate boxes.
5. In the Copy all authorizations of this user or [template] box, select a template or user that has the authorizations you want to assign to the login account you are creating. The following predefined templates are available:
   - **Administrator**—This template gives the user full configuration rights on the CMS and includes the All Tools toolbox for the CMS and for All Managed Systems.
   - **Operator**—This template gives the user limited configuration rights on the CMS and includes authorizations for the Monitor Tools toolbox on the CMS and the All Tools toolbox on All Managed Systems.
   - **User**—This template gives the user no configuration rights on the CMS and includes authorizations for the Monitor Tools toolbox for the CMS and All Managed Systems.

   If you do not want to select an existing user or template, select **None.**

6. In the Central Management Server configuration rights section, you must select the level of authority to assign to the new user from the following options. This setting is required. If you already selected an existing user or template in step 5, this information is already entered.
   - **Full,** allowed to modify all Central Management Server settings—Enables the user total control of the database. The user can run discovery of systems and data collection; define users and authorizations; set Cluster Monitor configuration; configure licensing and protocol settings; and create, modify, delete, and run reports, snapshot comparisons, tools, custom commands, events, automation tasks, and so on.
   - **Limited,** allowed to create/modify/delete all reports and their own tools—Enables the user to create new reports, edit any reports, and delete any reports (including the predefined reports).
   - **None,** no configuration of Central Management Server allowed—Enables the user to view and run predefined reports on the CMS and All Managed Systems. However, the user has no configuration rights on the CMS or on the managed systems.

7. To save and close the New User section, click **OK,** or to save this user and enter more users, click **Apply.**
8. When you finish entering users, click **Next** to go to the next First Time Wizard step.
Editing users
1. Select a user, and then click **Edit**. The Edit User section appears.
2. Make changes to the user information, and then click **OK**.

Deleting users
1. Select a user, and then click **Delete**. HP SIM prompts you to confirm the deletion.
2. Click **OK**.

Configuring e-mail settings
Because the CMS can send notifications, you must configure the e-mail settings that it uses. For more information, see the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*.

Setting up managed systems
Before performing installation and configuration, the following steps must be completed.
1. Install HP SIM on the CMS.
2. Complete the First Time Wizard.
3. You can configure Automatic Discovery during the First Time Wizard setup. Run Automatic Discovery.
4. Install the required Management Agents software and configure the supported protocols to communicate with HP SIM, including the ProLiant Support Pack installed on a ProLiant server using Windows or Linux. For more information on configuring HP SIM, see the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*.

Installing the ProLiant Support Pack on Windows systems for the first time
For Windows systems not currently running the ProLiant Support Pack, you must install the latest ProLiant Support Pack with preconfigured components on all managed systems using the HP Systems Insight Manager feature Initial ProLiant Support Pack Install. To install a ProLiant Support pack, you must have Windows administrator privileges on the target systems.

The initial ProLiant Support Pack installation process enables you to install the support pack on a Windows system. The process also configures certificate-based trust between HP SIM and target nodes. After you have run the Initial ProLiant Support Pack Install tool, you can use the Install Software and Firmware tool in HP SIM to update multiple systems.

The Install Software and Firmware feature in HP SIM requires a properly configured HP Version Control Repository Manager (VCRM). Installing and configuring the VCRM is not part of this procedure. For more information about installing and configuring the VCRM, see the *HP Version Control Installation Guide* at http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.

**NOTE:** The Install Software and Firmware and VCA features are only available after the Initial ProLiant Support Pack Install process has been run. For more information about ProLiant Support Packs, see the *HP ProLiant Support Pack and Deployment Utilities User Guide* at http://www.hp.com/servers/psp.
Installing an HP ProLiant or Integrity Support Pack on a Linux system for the first time

To use the Linux Deployment Utility on a local system, install the latest support pack with the preconfigured components on the local system. For more information about installing a support pack using the Linux Deployment Utility, see [http://www.hp.com/servers/psp](http://www.hp.com/servers/psp).

Installing the required software on HP-UX

Installing the required software on an HP-UX system involves the following steps:

- Understanding the basic managed system software for HP-UX
- Ensuring the managed system software is installed
- Acquiring and installing the managed system software, if not previously installed

For more information about this procedure, see the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*.

To modify Management Agents from the Control Panel, see the “Modifying Management Agents from the Control Panel” section in this guide.

Configuring protocol settings

You must configure protocol settings to define what systems are added to HP SIM using discovery. For more information, see the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*.

HP SIM has additional functionality to help you manage your infrastructure. For more information, see the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*.

Configuring the HP Service Essentials Remote Support Software Pack

The HP Service Essentials Remote Support Pack provides remote monitoring to supplement local monitoring of HP SIM. It also provides real-time hardware event monitoring and secure event submission to HP Support to help identify and prevent potentially critical problems on your HP ProLiant servers, Linux-based Integrity servers, and their associated internal devices.

The HP Essential Services Remote Support Pack includes three components:

- **HP Remote Support Software Manager (SWM)**—SWM, bundled with HP SIM 5.1 and installed to the CMS, facilitates the download and installation of HP Remote Support applications.
- **Remote Support Configuration and Services Option**—The Remote Support Configuration and Services Option is installed and updated by SWM. When installed, the Remote Support Option is accessed through HP SIM and is used to enable remote support of eligible systems in your Enterprise.
- **HP Remote Support Client**—The Remote Support Client enables communication of reactive hardware events from the CMS to the HP Support Center.

This section focuses on SWM. SWM is bundled with the installation of HP SIM on a supported Windows ProLiant CMS. SWM is installed to the CMS desktop and runs independently of the HP SIM user interface. SWM is installed on the CMS during HP SIM installation. The inclusion and installation of SWM are part of the standard HP SIM installation. Although optional, SWM is preselected in the custom HP SIM installation and upgrade.
The SWM installation is not interactive. When installed, SWM can be accessed from an icon on the CMS desktop.

After the HP SIM installation is complete, configure SWM to fit your enterprise specifications. When configured, SWM downloads and installs the Remote Support Tool.

SWM offers the following functionality and benefits:

- Upgrades can be performed remotely, reducing HP Support Engineer time on your site for installations.
- Automated e-mail notifications of new software, deployment statistics, and the state of your configurations improve communications, planning, and management of the Customer Enterprise.
- Software configuration data is collected to facilitate the following activities:
  - Target updates based on existing software versions present on a system
  - Track deployment of software updates
  - Report on the state (installed, update available, failed, and so on) of the software on a system

**Remote Support Pack Setup**

This process describes the preliminary steps you must perform to obtain Contract and Warranty information (HP contract, HP Care Pack, and HP warranty entitlement) and Remote Support capabilities. For complete information about this process, see the *HP Service Essentials Remote Support Pack Quick Start Guide* or the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*.

**IMPORTANT:** Perform the following steps before starting the processes to obtain Contract and Warranty information and Remote Support capabilities.

**NOTE:** HP Service Essentials Remote Support Pack must be installed on a physical drive, and is not supported on virtual machines.

1. Verify that all prerequisites are met, including installing SWM through HP SIM and configuring SWM to install the Remote Support Pack core components. The HP SIM installer installs the SWM. You must invoke, configure, and register SWM after the system reboots by double-clicking the Remote Support Software Manager icon on the desktop to ensure that the Remote Support Pack components are downloaded and installed.

2. Verify that HP SIM has discovered the systems for which you will enable remote support and contract and warranty reporting. You must supply a valid serial number and product number information.

3. Register the CMS and Remote Support Client using the Remote Support and Service Option. You must complete the boxes designated by asterisks. For more information, see the *HP Service Essentials Remote Support Pack Quick Start Guide* or the appropriate version of the *HP Systems Insight Manager Installation and Configuration Guide*. 
4. Verify that each system to be remotely monitored has the proper information supplied in HP SIM using System Properties. You must configure all boxes in the Contract and Warranty Information section designated by asterisks. For more information, see the \textit{HP Service Essentials Remote Support Pack Quick Start Guide} or the appropriate version of the \textit{HP Systems Insight Manager Installation and Configuration Guide}.

\textbf{NOTE:} Beginning with HP Open Service Event Manager (OSEM) version 1.4.2, the Manage By setting enables you to manage system information from either OSEM or HP SIM 5.1 or later. The Manage By setting includes selections of either OSEM or HPSIM 5.1+ and is located in the OSEM Managed Systems summary page on the top left. By default, the Manage By setting is Manage By OSEM. In this case, OSEM requires that entered system and customer information be provided by OSEM Managed System Pages. For OSEM to use information from HP SIM 5.1 System Properties boxes, you must change the default Manage By setting from Manage By OSEM to HPSIM5.1+. The Manage By setting only appears if HP SIM 5.1 or later is detected by OSEM 1.4.2 or later.

5. Verify that designated boxes contain valid information. For example, a numeric phone number must be entered in the System Properties Contact Phone box rather than text. If designated boxes are blank or contain invalid data, the Remote Support Pack might not be able to supply contract and warranty data, and might not be able to create remote support cases.

\section*{Performing additional Vulnerability and Patch Management Pack post-installation configuration tasks}

After the Vulnerability and Patch Management Pack is installed for the first time, you must perform the following steps to complete the configuration and install the latest vulnerability updates.

To locate and identify target systems in the network for use with the Vulnerability and Patch Management Pack, perform an automatic discovery. For information about performing a discovery and other basic HP SIM tasks, see the \textit{HP Systems Insight Manager Installation and Configuration Guide}.

\section*{Modifying the Vulnerability and Patch Management Pack settings}

Before this step can be completed successfully, perform the following steps:

1. Run the patch acquisition using the VPM Acquisition Utility.
2. Save the patch acquisition to the designated directory.
3. Select \textbf{Options}>\textbf{Vulnerability and Patch Management}>\textbf{Settings}.
4. Select the source from which patch and vulnerability updates are obtained by choosing one of the following options.
   - If the VPM server has direct Internet access, then to use the VPM server to obtain updates, you must select \textbf{Acquire updates from Internet}. If you use a proxy server, select the appropriate checkbox and then enter your configuration information. If the proxy requires authentication, select the appropriate checkbox, and then enter your user credentials. Only basic (nonencrypted) authentication is supported.
   - If the VPM server does not have Internet access, then to use the VPM Acquisition Utility on another system (with Internet access) to acquire updates, select \textbf{Acquire updates from local repository}. The update files can either be manually relocated to the VPM server or accessed from the network. Designate the directory path where the update files are located in the Source path box. If necessary, enter user credentials to access the designated directory. The VPM server must have read access to the designated directory.
5. Click \textbf{Apply}.
Configuring Vulnerability and Patch Management Pack acquisition for Red Hat Enterprise Linux

If Red Hat patch acquisitions are run, to configure Red Hat Enterprise Linux acquisition settings:

1. Verify the Red Hat library, compat-libstdc++, is installed on all Red Hat target systems.
2. Verify that each Red Hat target system to be patched has a valid subscription and license for the Red Hat Network, which are required for patch acquisitions. For information about subscribing to the Red Hat Network, see http://www.redhat.com.
3. Log in to a Red Hat Enterprise or Advanced Server Linux 2.1, 3, or 4 system as root.
4. Execute the following command: rhn_register.
5. Select Existing, and then enter your user credentials.
6. Enter a unique profile name for this machine (such as the IP address or host name).
7. Exit the rhn_register application without applying any patches to the system.
8. Copy the file created by the rhn_register tool from /etc/sysconfig/rhn/systemid to C:\Program Files\HP\VPM\radia\IntegrationServer\etc.

![IMPORTANT: On a Red Hat Linux environment, configure the network connectivity between the CMS and the target systems by editing the correct /etc/hosts file. Verify that both CMS and target systems can reach each other by using the ping command execution with the host name.](image)

9. Rename the systemid file to reflect the appropriate Red Hat distribution:
   - If the system that created the systemid file was running Red Hat Enterprise Linux 4, rename the file redhat 4es.sid.
   - If the system that created the systemid file was running Red Hat Enterprise Linux 3, rename the file redhat 3es.sid.
   - If the system that created the systemid file was running Red Hat Enterprise Linux 2.1, rename the file redhat 2.1es.sid.
   - If the system that created the systemid file was running Red Hat Advanced Server Linux 4, rename the file redhat 4as.sid.
   - If the system that created the systemid file was running Red Hat Advanced Server Linux 3, rename the file redhat 3as.sid.
   - If the system that created the systemid file was running Red Hat Advanced Server Linux 2.1, rename the file redhat 2.1as.sid.

Acquiring Vulnerability and Patch Management Pack updates

Vulnerability and Patch Management Pack provides an acquisition utility that connects to the selected vendor website, downloads patch information and patch files, and places this information in the Vulnerability and Patch Management Pack database. Acquisitions can be run either from the VPM server when the VPM server has direct access to the Internet or using the VPM Acquisition Utility installed on another system.

After you install VPM for the first time, you must complete a patch acquisition to update the information in the Vulnerability and Patch Management Pack database. Also, to ensure that Vulnerability and Patch Management Pack is always up to date with the latest security information and obtain new vulnerability scan definitions and patches, you must complete patch acquisitions on a regular basis.
Acquisitions from the VPM server

When using a proxy to connect to the Internet, the proxy settings must be configured to acquire updates. For information, see the “Modifying the Vulnerability and Patch Management Pack settings” section.

Do not schedule patch acquisition tasks to run while vulnerability scans are running. Patch acquisition tasks cause vulnerability scans to abort.

If you use a proxy to connect to the Internet, you must configure the proxy settings to acquire updates. For more information, see “Modifying the Vulnerability and Patch Management Pack settings”.

1. Select Options>Vulnerability and Patch Management>Acquire Updates.
2. Follow the on-screen instructions, selecting the appropriate update information for your server environment when prompted.
3. Click Schedule, and then select a time to acquire daily Vulnerability and Patch Management Pack updates. Updates might not be available daily, but scheduling the event daily ensures that critical updates are obtained promptly.
4. To run the initial patch acquisition, select Run now, and then click Done. Patch acquisition progress can be monitored by accessing the log at C:\ProgramFiles\HP\VPM\Radia\IntegrationServer\logs\patch-acquire.log. The complete VPM acquisition event appears on the All Events screen after the acquisition is complete.
5. The acquisition event might contain raw HTTP error codes, which must be decoded to determine their cause. To decode HTTP error codes, see either http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html or the IIS help pages located at C:\WINNT\Help\iisHelp\common on a system where Microsoft Internet Information Services (IIS) is installed.

Acquisitions using the VPM Acquisition Utility

The VPM Acquisition Utility can be run from any system with Internet access to download patch information and patch files from selected vendor websites. This information can then be imported to the VPM server in the Vulnerability and Patch Management Pack database.

To run the acquisition tool, the VPM Acquisition Utility must be installed on the selected system.

Perform steps 2 through 7 the first time you use the VPM Acquisition Utility. If necessary, you can modify the information whenever you run the utility. To configure and use the VPM Acquisition Utility to acquire patch and vulnerability updates:

1. Access the VPM Acquisition Utility from the selected system.
2. Select one or more sources from which to acquire patch updates, and then click Next.
3. Select the appropriate operating system platforms and platform-related applications, and then click Next.
4. Select the appropriate languages for the required patches, and then click Next.
5. Enter the appropriate destination path for downloaded files, and then click Next. The destination can be either a local or shared directory. The designated directory must be accessible.
6. If you use a proxy, select the I use a proxy checkbox, and then enter the appropriate configuration information.
7. If your proxy requires authentication, select the My proxy requires authentication checkbox, and then enter the appropriate user credentials. Only basic (not encrypted) authentication is supported.
8. Click Next.
9. To run the patch acquisition, click **Run Now**. Patch acquisition progress can be monitored by accessing the log at C:\Program Files\HP\VPM Acquisition Utility\logs\patch acquire.log. To allow manual scrolling during the acquisition, clear the **Enable auto-scroll** checkbox.

10. When the acquisition process is complete, click **Done**.

11. On the VPM server, create a directory named **data** at C:\Program Files\HP\VPM\Radia\IntegrationServer. You can use a network share if the VPM server has read access to the share.

12. Copy downloaded files from the VPM Acquisition Utility server destination directory to the VPM server data directory.

13. From HP SIM, to configure your import setting, select **Options> Vulnerability and Patch Management>Settings**.

14. To start the import process, select **Options>Vulnerability and Patch Management> Acquire Updates**.

Managing Vulnerability and Patch Management Pack target systems

Target systems are managed by the Vulnerability and Patch Management Pack. HP recommends installing HP Management Agents on ProLiant target systems to enable HP SIM to better identify the target systems. For other target systems, enable WMI or Web-Based Enterprise Management (WBEM) for other target systems. The VPM Patch Agent is deployed when target systems are licensed to enable patches to be applied to the systems. SSH must be installed on Linux target systems.

For a list of supported target systems, see the **HP Insight Control Management Support Matrix**.

Performing Insight Power Manager post-installation configuration tasks

**IMPORTANT:** When Insight Power Manager is installed it is disabled. To enable Insight Power Manager, select **Options>Insight Power Manager Options**, and then select **Enable Insight Power Manager Plug-In**.

To set up and configure Insight Power Manager:

1. Verify that the CMS has discovered new ProLiant servers with power management capabilities. For a list of supported servers, see the **HP Insight Control Management Support Matrix**.

2. Select **Options>Insight Power Manager Options**, select **Enable**, and then click **Apply**. For more information about enabling Insight Power Manager, click **Options>Insight Power Manager Options** to access the Insight Power Manager Options menu.

3. Configure security access, and then apply security credentials. The Insight Power Manager plug-in must be configured with the iLO login name and password for the systems that are managed. For more information about enabling Insight Power Manager, click **Options>Insight Power Manager Options** to access the Insight Power Manager Options menu.

4. Install Integrated Lights-Out (iLO) 2 Advanced or Select license on managed systems. For more information, see [http://www.hp.com/servers/ilo](http://www.hp.com/servers/ilo).
5. Install the Insight Power Manager license with security credentials on a CMS to enable Insight Power Manager data collection. See “Adding and applying licenses to iLO Power Management Pack” section in this guide. For more information, see http://www.hp.com/products/ipm.

You must have security credentials on the CMS to enable IPM. You must also run Discovery to discover the system and run iLO to successfully configure security credentials.

6. Refresh the data by performing the following steps:
   a. Select the licensed server, and then click Reports>Insight Power Manager.
   b. To retrieve the latest information from the server, click Refresh Data. The process of refreshing the data might take several minutes.

Configuring domain accounts for Rapid Deployment Pack

When you deploy a Windows system to be part of a Windows domain, you must configure that system by using an account with domain privileges that can be configured in the domain.

To configure one or more domain accounts that Rapid Deployment Pack uses to add systems to a Windows domain during deployment:
1. Launch the Rapid Deployment Pack Deployment Console tool.
2. Select Tools>Options.
3. Select the Domain Accounts tab.
4. Click Add.
5. Enter the Microsoft domain and credentials.
6. Click OK.

After you add the domain, the next provisioning request that uses this domain can automatically join the domain.

Setting up virtual machine hosts for Virtual Machine Management Pack

Before using the Virtual Machine Management Pack you must first perform the procedures in the following sections.

Performing an HP SIM discovery

HP SIM must discover virtual machines to perform certain Virtual Machine Management Pack tasks.

**IMPORTANT:** You must perform these configuration steps before attempting to use the Virtual Machine Management Pack.

**CAUTION:** Do not manually alter serial numbers on virtual machine hosts unless you are restoring the original serial number. For more information about restoring server serial numbers, see the server documentation.
To perform an HP SIM discovery:

1. Log in to HP SIM from an account with administrator privileges.
2. Select **Options>Protocol Settings>Global Protocol Settings**, and configure the default Web Based Enterprise Management (WBEM) settings with appropriate credentials to enable access to target systems. If some target systems use individual protocol settings, select **Options>Protocol Settings>System Protocol Settings** to configure settings for individual systems.
3. Perform an HP SIM discovery of virtual machine hosts and guests to enable the Virtual Machine Management Pack to access target systems in the network.

For information about performing basic HP SIM tasks, see the **HP SIM User Guide**.

**Setting up virtual machine guests for Virtual Machine Management Pack**


**Installing Microsoft Virtual Server Additions**

1. Verify that the virtual machine guests are started before starting the installation.
2. Go to the Microsoft Virtual Server 2005 Administration website.
3. From the Microsoft Virtual Server 2005 Administration home page, select **Configure** in the Virtual Machines box. A list of virtual machine guests appears.
4. Select the appropriate virtual machine guests. The virtual machine guest configuration details appear.
5. Click **Install Virtual Machine Additions**.
6. Select the **Install Virtual Machine Additions** checkbox, and then click **OK**.

For more information, see [http://www.microsoft.com](http://www.microsoft.com).

**Installing VMware tools**

To install VMware ESX Server™ and VMware GSX Server™ tools on VMware virtual machine guests from the VMware Management Interface:

1. Verify that the virtual machine guests are started before starting the installation.
3. Log in to the VMware Management Interface.
4. Select the appropriate virtual machine guest, and then open the remote console.
5. From the selected virtual machine console, right-click the selected virtual machine guest.
6. Select **Install VMware Tools**.

For more information, see [http://www.vmware.com/support/](http://www.vmware.com/support/).
Licensing Insight Control Management suites

This section describes the licensing procedures for Insight Control Management suites.

You must have HP SIM administrative rights to add or deploy Insight Control Management licenses. Table 15 lists the sections to be reviewed and the steps to be performed, for licensing Insight Control Management suites.

**Table 15** Steps required for adding Insight Control Management suite licenses

<table>
<thead>
<tr>
<th>To license this suite</th>
<th>Perform steps described in the following sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insight Control Environment</td>
<td>• Preparing for Insight Control Environment, Insight Control Environment for BladeSystem, and Insight Control Data Center Edition licensing</td>
</tr>
<tr>
<td></td>
<td>• Adding and applying licenses to Insight Control Environment</td>
</tr>
<tr>
<td></td>
<td>• Licensing the Rapid Deployment Pack</td>
</tr>
<tr>
<td></td>
<td>• Adding iLO 2 license keys</td>
</tr>
<tr>
<td></td>
<td>• Registering for Software Technical Support and Update Service</td>
</tr>
<tr>
<td>Insight Control Environment for BladeSystem</td>
<td>• Preparing for Insight Control Environment, Insight Control Environment for BladeSystem, and Insight Control Data Center Edition licensing</td>
</tr>
<tr>
<td></td>
<td>• Adding and applying licenses to Insight Control Environment for BladeSystem</td>
</tr>
<tr>
<td></td>
<td>• Licensing the Rapid Deployment Pack</td>
</tr>
<tr>
<td></td>
<td>• Adding iLO 2 license keys</td>
</tr>
<tr>
<td></td>
<td>• Registering for Software Technical Support and Update Service</td>
</tr>
<tr>
<td>Insight Control Data Center Edition</td>
<td>• Preparing for Insight Control Environment, Insight Control Environment for BladeSystem, and Insight Control Data Center Edition licensing</td>
</tr>
<tr>
<td></td>
<td>• Adding and applying licenses to Insight Control Data Center Edition</td>
</tr>
<tr>
<td></td>
<td>• Licensing the Rapid Deployment Pack</td>
</tr>
<tr>
<td></td>
<td>• Registering for Software Technical Support and Update Service</td>
</tr>
<tr>
<td>iLO Power Management Pack</td>
<td>• Adding and applying licenses to iLO Power Management Pack</td>
</tr>
<tr>
<td></td>
<td>• Adding iLO 2 license keys</td>
</tr>
<tr>
<td></td>
<td>• Registering for Software Technical Support and Update Service</td>
</tr>
<tr>
<td>iLO Power Management Pack for BladeSystem</td>
<td>• Adding and applying licenses to iLO Power Management Pack</td>
</tr>
<tr>
<td></td>
<td>• Adding iLO 2 license keys</td>
</tr>
<tr>
<td></td>
<td>• Registering for Software Technical Support and Update Service</td>
</tr>
</tbody>
</table>
Preparing for Insight Control Environment, Insight Control Environment for BladeSystem, and Insight Control Data Center Edition licensing

Before licensing servers for Insight Control Environment, Insight Control Environment for BladeSystem, or Insight Control Data Center Edition, verify that the servers have a supported operating system or that you plan to deploy a supported operating system. For more information about discovering and updating the server list in HP SIM, see the appropriate version of the HP Systems Insight Manager Installation and Configuration Guide. For information about supported operating systems, see the HP Insight Control Management Support Matrix.

HP BladeSystem c-Class enclosures ship with an eight-server, 30-day evaluation version of Insight Control Environment for BladeSystem. A fully licensed version for 8 or 16 servers is also available with c-Class enclosure purchases.

Adding an Insight Control Environment, Insight Control Environment for BladeSystem, or Insight Control Data Center Edition license in HP SIM applies licenses for all components except Rapid Deployment Pack and iLO. You must add the Rapid Deployment Pack and iLO licenses separately.

Adding and applying licenses to Insight Control Environment

HP Insight Control Environment includes three license keys: Insight Control Environment key, Rapid Deployment Pack registration code, and iLO Advanced license key. For successful operation, all three keys must be applied to each managed target system.

To add and apply an Insight Control Environment license key:

1. Select Deploy>Insight Control Licenses>Insight Control Environment Keys (ML/DL).
2. After selecting target systems, click Add Key, and then enter the key code.
3. To apply the license key, select a license to apply to the target servers, and then click Apply License.

For instructions on adding RDP registration code and iLO Advanced license key, see the following sections.

Adding and applying licenses to Insight Control Environment for BladeSystem

HP Insight Control Environment for BladeSystem includes three license keys—Insight Control Environment for BladeSystem key, RDP registration code, and iLO Select license key. For successful operation, all three keys must be applied to each managed target.

To add and apply the Insight Control Environment license key:

1. Select Deploy>Insight Control Licenses>Insight Control Environment Keys (BL).
2. After selecting target systems, click Add Key, and then enter the key code.
3. To apply the license key, select a license to apply to the target servers, and then click Apply License.

For instructions on adding the RDPk registration code and iLO Select license key, see the following sections.
Adding and applying licenses to Insight Control Data Center Edition

HP Insight Control Data Center Edition includes two license keys—Insight Control Data Center Edition key and RDP registration code. For successful operation, both keys must be applied to each managed target.

To add and apply the Insight Control Data Center Edition license key:

1. Select Deploy>Insight Control Licenses>Insight Control Data Center Edition.
2. After selecting target systems, click Add Key, and then enter the key code.
3. To apply the license key, select a license to apply to the target servers, and then click Apply License.

For instructions on adding the RDP registration code, see the following sections.

Licensing the Rapid Deployment Pack

**NOTE:** The term server used in this context refers to a physical server or a virtual machine. One license is required for each physical server or virtual machine.

Use your unique product registration number to obtain a license file. A 16-character alpha or 20-character alphanumeric registration number is located on an insert card in the kit. The registration number is in the form:

xxxxxxxx-xxxx-xxxx-xxxx-xxxx

**IMPORTANT:** Keep your product registration number for reference.

2. Follow the instructions to complete the registration process. A license file is e-mailed to you.

Additional purchased licenses can be transferred or combined with registered licenses. Follow the instructions at http://www.hp.com/servers/rdp/register.

Applying a RDP license file

To apply a license file to your Deployment Server:

1. Power down all connections to the Deployment Server Console and Deployment Server Web Console.
2. Run the Altiris Product Licensing Utility by clicking Start>Programs>Altiris>Deployment Solution>Product Licensing Utility.
3. Enter the path to the new license file in the Activation Key File Information box, and then click Next.
4. Follow the instructions to apply your additional licenses.

To view the number of additional licensed servers from the console, select Help>About.
Adding and applying licenses to iLO Power Management Pack

Your iLO Power Management Pack license includes a key for both the IPM and iLO Advanced Pack or iLO 2 Select Pack. For successful operation both keys must be applied to each managed target system.

Your IPM license key might contain one or more licenses. One license is required for each managed target system. To add the license key:

1. Select Deploy>License Manager.
2. Select Add New Product, and then click Manage Licenses.

Your iLO 2 license key activates and enables access to iLO Advanced or iLO Select features. It must be installed so that the Insight Power Manager works properly. The license key can be entered in the Administration tab of the iLO 2 user interface for a specific system.

Managing Insight Power Manager license keys

You must have HP SIM already installed to perform this procedure.

After the IPM license is installed, you can manage the license using the HP SIM License Manager feature.

To use the License Manager to manage keys:

1. Select Deploy>License Manager. The following information appears for each licensed product:
   - Product—The name of the product
   - Licensed Systems—The number of systems licensed to use the product
   - Licenses (For detail, select Manage Licenses)—The total number of product licenses in the License Manager database for the product
2. Select Add New Product. The Manage Licenses section appears.
3. Click Add Licenses. The Add License section appears.
4. In the Specify a key string box, enter the license key that you purchased or obtained, and then click Open. The system is licensed and the Key details sections displays the Product, License Version, License Type, Licenses Purchased, and Days Max.
5. Click Add Licenses Now. A dialog box appears, indicating the key has been added.
6. Click OK. The new key appears under Product License Information.
7. (Optional) To add more licenses, click Add Licenses Now, and then repeat steps 2 through 6.

For instructions on adding the iLO 2 license key, see the “Adding iLO 2 license keys” section in this guide.

Licensing Insight Power Manager managed systems

You must install a license to use IPM. If a server is not licensed, a prompt appears when you click Reports>Insight Power Manager or Options>Insight Power Manager Options indicating that licenses are not installed.

To install an Insight Power Manager license:

1. Select the servers to be licensed from the Systems and Events panel.
2. Click Reports>Insight Power Manager or Options>Insight Power Manager Options. The Step 1 page appears with the Status indicating the server is not licensed.
3. Select the server to be licensed, and then click Apply License. The Step 2: License unlicensed systems (Optional) page appears indicating the number of licenses remaining.
4. Click Next. The Insight Power Manager page appears.
Adding iLO 2 license keys

The Licensing page enables you to view the current license status and enter a key to activate iLO 2 licensed features. Use the same procedure to activate the iLO 2 Advanced Pack or iLO 2 Select Pack.

To add an iLO 2 license key:
1. Log in to iLO 2 through a supported browser.
2. Click the Administration tab.
3. Click Licensing. The iLO 2 license activation screen appears.
4. Enter the license key in the spaces provided. To move between boxes, press Tab, or click inside a box. The Activation key box advances as you enter data. To clear the boxes and reload the page, click Licensing.
5. Click Install.
6. Click OK.

To create a script that enables licenses to be pushed from a central point and to update and activate the license key, enter the following from the command line interface:

    set / map1 license=1234500006789100000000001

You can also perform other license operations, such as Show and Delete, and use the command line interface with SSH.

Registering for Software Technical Support and Update Service

HP offers a number of software support services, many of which are provided to our customers at no additional charge.

Software Technical Support and Update Service—Insight Control suites and select ProLiant Essentials software products include one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems. The service also provides access to software updates and reference manuals either in electronic form or on physical media as they are made available from HP. (Customers who purchase an electronic license to use are eligible for electronic updates only.) With this service, Insight Control and ProLiant Essentials customers will benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see http://www.hp.com/services/insight.

Registration for Software Technical Support and Update Service:

There are two methods for registering:

- If you received a license entitlement certificate, automated registration for this service will take place upon online redemption of the license certificate/key.
- If the license information you received for your product instructs you to register for Software Technical Support and Update Service, follow the instructions to be eligible for telephone support and product updates.
Establishing security

The integrated installer used by Insight Control Management provides a single process for installing and configuring HP management software quickly and consistently. This process includes establishing the following secure access patterns:

- Administrator access to and authentication of HP SIM CMS and the Rapid Deployment Pack
- WBEM access to managed systems
- Database accounts for HP SIM and Rapid Deployment Pack

When HP SIM is accessed from a web browser, an HTML login page appears. The HP SIM CMS username, password, and domain requirements must be entered on the HTML login page.

Information that is accessed is securely transmitted using the Secure Socket Layer (SSL) protocol. SSL provides data encryption and server authentication by using public and private key technology. The web server on the CMS uses a certificate for server authentication. By default, this certificate is self-signed, but it can be replaced by a certificate that is signed by a trusted certificate authority. Your web browser must import this certificate to trust the CMS.

To maintain a secure CMS environment, perform the following actions:

- Restrict to a minimum the number of local users.
- Restrict or remove remote users.
- Enable high-security measures, such as audit logging and enhanced password restrictions.
- Remove remote shares when possible.

**IMPORTANT:** The Insight Control Management installation does not establish security beyond the minimum required for the HP SIM host server. For environments where additional security or certificate-based access is required, this security must be implemented in an additional process.
## Accessing Insight Control Management component interfaces in HP SIM

Table 16 lists the steps to access the various Insight Control Management components in HP SIM.

<table>
<thead>
<tr>
<th>To access</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Insight Control Management</strong></td>
<td>• Tools&gt;Insight Control Management&gt;Software Updates</td>
</tr>
<tr>
<td></td>
<td>• Tools&gt;Insight Control Management&gt;Insight Control Environment Advisor</td>
</tr>
<tr>
<td></td>
<td>• Deploy&gt;Insight Control Licenses&gt;Insight Control Data Center Edition Keys (BL)</td>
</tr>
<tr>
<td></td>
<td>• Deploy&gt;Insight Control Licenses&gt;Insight Control Environment Keys (BL)</td>
</tr>
<tr>
<td></td>
<td>• Deploy&gt;Insight Control Licenses&gt;Insight Control Environment Keys (ML/DL)</td>
</tr>
<tr>
<td><strong>HP BladeSystem Integrated Manager</strong></td>
<td>• Tools&gt;Integrated Console&gt;HP BladeSystem</td>
</tr>
<tr>
<td><strong>Extensions for HP SIM on Microsoft Windows</strong></td>
<td>• Deploy&gt;Ignite-UX</td>
</tr>
<tr>
<td></td>
<td>• Deploy&gt;Software Distributor</td>
</tr>
<tr>
<td></td>
<td>• Configure&gt;HP-UX Configuration</td>
</tr>
<tr>
<td></td>
<td>• Diagnose&gt;GlancePlus</td>
</tr>
<tr>
<td></td>
<td>• Optimize&gt;Workload Manager</td>
</tr>
<tr>
<td><strong>Rapid Deployment Pack</strong></td>
<td>• Deploy&gt;Rapid Deployment Pack</td>
</tr>
<tr>
<td><strong>Insight Power Manager</strong></td>
<td>• Reports&gt;Insight Power Manager</td>
</tr>
<tr>
<td></td>
<td>• Options&gt;Insight Power Manager Options</td>
</tr>
<tr>
<td><strong>Performance Management Pack</strong></td>
<td>• Diagnose&gt;Performance Management Pack</td>
</tr>
<tr>
<td></td>
<td>• Reports&gt;Performance Management Pack Reports</td>
</tr>
<tr>
<td></td>
<td>• Options&gt;Performance Management Pack Options</td>
</tr>
<tr>
<td><strong>Vulnerability and Patch Management Pack</strong></td>
<td>• Deploy&gt;Vulnerability and Patch Management</td>
</tr>
<tr>
<td></td>
<td>• Diagnose&gt;Vulnerability and Patch Management</td>
</tr>
<tr>
<td></td>
<td>• Options&gt;Vulnerability and Patch Management</td>
</tr>
<tr>
<td><strong>Virtual Machine Management Pack</strong></td>
<td>• Configure&gt;Virtual Machine Host Registration</td>
</tr>
<tr>
<td></td>
<td>• Options&gt;Virtualization Management</td>
</tr>
</tbody>
</table>
Adding Virtual Machine Management Pack licenses (optional)

This section describes the basic procedures for adding licenses for the Virtual Machine Management Pack. For more information, see the HP ProLiant Essentials Virtual Machine Management Pack User Guide.

Licensing a Virtual Machine Management Pack

1. From the console toolbar, select Deploy>License Manager>Manage Keys.
2. To enter one or more new key strings, click Add Key, and then click OK.

Using free licenses

Five fully-functional, 30-day trial licenses are provided with the Virtual Machine Management Pack for evaluation purposes. These licenses are available after the Virtual Machine Management Pack is installed and can be applied to systems from the HP SIM License Manager. For more information, or to purchase more licenses, see http://www.hp.com/go/vmmanage.

Preparing for licensing

Before licensing servers for the Virtual Machine Management Pack, verify that the servers have supported virtualization software installed.

For more information about discovering and updating the server list in HP SIM, see the appropriate version of the HP Systems Insight Manager Installation and Configuration Guide. For information about supported virtualization software, see the HP ProLiant Essentials Virtual Machine Management Pack Support Matrix.

Applying licenses to virtual machine hosts

After you have applied a license to a specific server, the license cannot be removed or transferred to another server. If a demo license key is used, it is overridden by purchased licenses.

To apply licenses to virtual machine hosts:

1. From the console toolbar, select Deploy>License Manager.
2. In the product table, select VMM.
3. Click Manage Licenses.
4. Select the licenses to apply.
5. Click Assign Licenses.
6. Select the target virtual machine hosts to be licensed.
7. Click Apply.
8. Verify that the correct target hosts appear in the list.
9. (Optional) To add targets, click Add Targets, or to remove targets, click Remove Targets.
10. Click Next.
11. To apply to the selected target host, select the appropriate Virtual Machine Management Pack license.

12. Click **Assign Now**.

After a few minutes, the screen update to reflect the changes.

**Supported configurations**

The configurations are supported both in a Windows domain and a workgroup.

- If any server is in a Windows domain, all servers must be in the same Windows domain. Servers in different Windows domains are not supported.
- If any server is in a Windows domain, the domain server must be a separate server from the servers shown in the preceding figure. Installation of Insight Control Management is not supported on domain servers.
- If any server is in a workgroup, each server must have a local account with the same name and same password (both for services and database credentials).

The following figure shows the supported configurations for the CMS with Insight Control Management installed.
Unsupported configurations

- CMS does not support remote MSDE or SQL Express (see configurations 1, 2, 3, and 4).
- CMS does not support SQL Server Express 2005 database (see configurations 5 and 6).

The following figure shows the unsupported configurations for the CMS with Insight Control Management installed.
3 Managing server blades from HP SIM

This chapter provides an overview of managing server blades from HP SIM using the HP BladeSystem Integrated Manager. This chapter also provides information on the optional Extensions for HP SIM on Microsoft Windows software package.

Using the HP BladeSystem Integrated Manager

The HP BladeSystem Integrated Manager enables you to manage blade systems from HP SIM. HP BladeSystem Integrated Manager is composed of server blades, integrated connectivity to data, and shared power subsystems. The HP BladeSystem Integrated Manager enables you to quickly navigate your HP blade environments, including server blades and desktops, enclosure infrastructures, racks, and integrated switches through hierarchical tree views. You can configure and manage individual or groups of server blades.

The HP BladeSystem page (accessible through the predefined HP BladeSystem collection in the left hand side of the main HP SIM page) defaults to a tree view displaying the following:

- All c-Class racks for c-Class components, including c-Class server blades (ProLiant and Integrity), switches, HP BladeSystem Onboard Administrator, enclosures, and racks
- All p-Class racks for p-Class components, including p-Class server blades, switches, enclosures, and racks

The HP BladeSystem page provides the following views:

- Tree view—Provides an automatically populated representation of the actual physical hierarchy of blade components. For example, in this view, you can create and utilize collections of components.
- Icon view—Lists the system name of all discovered systems as well as the system health status for each system. The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown.
- Table view—Lists the system name and type and sorts information into columns. The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown.

Managing racks and enclosures

A server blade is typically a very dense server containing microprocessors, memory, and network connections that can be easily inserted into a rack-mountable enclosure to share power supplies, fans, switches, and other components with other server blades. Server blades tend to be more cost-efficient, faster to deploy, and easier to adapt to growth and change than traditional rack-mounted or tower servers.

A rack is a set of components connected to communicate together. An enclosure is a physical container for a set of server blades and switches. It consists of a backplane that routes power and communication signals, and additional hardware for cabling and thermal issues. It also hosts the CPU or server power supplies. A rack is a container for an enclosure although both racks and enclosures are considered containers.
• **c-Class**—This collection consists of the HP BladeSystem c-Class enclosures, HP ProLiant BL c-Class server blades, HP Integrity BL c-Class server blades, network interconnect components, Onboard Administrator, and management tools that enable adaptive computing, optimized for rapid deployment.

• **p-Class**—This collection forms a rack if a set of enclosures are networked on the hardware level. A p-Class enclosure hosts the ProLiant and Integrity BL p-Class servers, ProLiant BL p-Class switches, and multiple workstation types.

HP SIM discovers and identifies server blade racks and enclosures. Two default collections are related to racks and enclosures and are listed under the System Type collection:

- All Racks
- All Enclosures

On the system table view page, racks appear in these formats:

- Enclosure in Rack 1
- Rack 1

When you click the link to the rack or the enclosure from any BladeSystem view, the Picture View page appears.

If the server, switch, or Onboard Administrator is part of an enclosure in a rack, the Picture View page appears. The view shows a diagram of the discovered systems in the enclosure and, if available, in the rack. In picture view, when you place the cursor over a server, switch, or Onboard Administrator, information appears about that particular device, including server blade name, slot number, device name, and the enclosure in which the server is located.

**Rack view**

The Rack View page is available for p-Class and c-Class collections. The Rack View page is not available for e-Class collections. The Rack View page displays the following tabs:

- System(s)
- Events

**System(s) tab**

The picture view page for racks and enclosures contains a diagram of discovered systems in the rack or enclosure (if available). The rack name appears along with a picture view, table view, or iconic view of the rack. In rack view, when you place the cursor over a device shown, information appears about a particular device, including slot number, device name, and model number for the device. To view more information about a particular device, click that device to open the System page.

**Events tab**

The Events tab for racks or enclosures appears in event table view. The event table view page is divided into the following sections:

- Filter Criteria
- Event Status Legend
- Event Collection Columns
- Event Details
- Event Management Buttons
Enclosure view

The enclosure picture view page contains a diagram of discovered systems in the enclosure (if available). The enclosure name appears along with a picture view, table view, or iconic view of the enclosure. In enclosure view, when you place the cursor over a device shown, information appears about a particular device, including slot number, device name, and model number for the device. To view more information about a device, click that device to open the System page.

The following systems appear in the picture view for racks and enclosures:

- Servers, workstations, or desktops
- Interconnect switches
- Onboard Administrators
- Power supply enclosure

Slots that have no devices identified also appear as empty slots in the enclosures picture view.

The following sections appear in the picture view for racks and enclosures:

- System Status
- Identification
- Power and Thermal section (available only for the p-Class and c-Class enclosure and Rack view)
- Fans section (available only for the c-Class enclosure and Rack view)
- Virtual connect domain name

Working with the System page

The System page displays information that is related to a specific system and includes the following tabs:

- Identity—Includes general system and status information
- Tools & Links—Includes links to System Management pages, HP SIM pages, and other tools and information
- Events—Displays the event table view page for the system
- Performance—Includes general information about system performance
- Port Mapping—Displays port mappings for only c-Class blades and switches
- VM Performance—Includes general information about virtual machine hosts or virtual machine guests. In cases where the system is a virtual machine host, the information included covers all the virtual machine guests hosted in that system.

Using Extensions for HP SIM on Microsoft Windows

Extensions for HP SIM on Windows is a software package that extends HP SIM running on a Windows CMS to include additional features. Extensions for HP SIM on Windows version 1.0 includes links to server management tools for HP-UX 11i and Linux. The server management tools run on the HP-UX 11i and Linux managed systems, and include OpenView GlancePlus and HP-UX 11i tools such as Ignite-UX, Software Distributor, HP-UX Workload Manager, and web-based system configuration tools. HP-UX 11i and Linux server management tools can be licensed separately as part of an HP-UX 11i Operating Environment.
Extensions for HP SIM on Windows version 1.0 includes five categories of additional features for HP SIM. During the installation dialog, you can select which of these are to be installed:

- Ignite-UX (HP-UX 11i OS Deployment)
- Software Distributor (HP-UX 11i software management)
- HP-UX Configuration (manage peripherals/devices, kernel, file systems, LVM, users, and so on)
- HP-UX Workload Manager (optimize CPU utilization)
- OpenView GlancePlus (performance monitoring for HP-UX 11i, Linux, and so on)

After successful installation of the Extensions for HP SIM on Windows, you have new menu options to launch system management tools for HP-UX 11i and Linux management. You can continue to launch the System Management Homepage (SMH) from HP SIM and access various management tools from SMH, or use the direct launch capabilities provided through the new menu options.

Table 17 summarizes the new menu options enabled, and the existing menu options already present in HP SIM. Descriptions of each tool follow the table.

<table>
<thead>
<tr>
<th>New option</th>
<th>HP SIM menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch of OpenView GlancePlus for HP-UX 11i or Linux (X-based)</td>
<td>Diagnose</td>
</tr>
<tr>
<td>Launch of Ignite-UX for HP-UX OS deployment (X-based, CLI)</td>
<td>Deploy</td>
</tr>
<tr>
<td>Launch of HP-UX Disk and File Systems management tool (SMH/fsweb)</td>
<td>Configure</td>
</tr>
<tr>
<td>Launch of HP-UX Kernel Configuration tool (SMH/kcweb)</td>
<td>Configure</td>
</tr>
<tr>
<td>Launch of HP-UX Peripherals and Devices management tool (SMH/pdweb)</td>
<td>Configure</td>
</tr>
<tr>
<td>Launch of HP-UX Users and Groups management tool (SMH/ugweb)</td>
<td>Deploy</td>
</tr>
<tr>
<td>Launch of Software Distributor tools that run on the CMS</td>
<td>Tools&gt;Command Line</td>
</tr>
<tr>
<td>Launch of Workload Manager tools (WLM)</td>
<td>Optimize</td>
</tr>
</tbody>
</table>

Features already included with HP SIM for Microsoft Windows

<table>
<thead>
<tr>
<th>Feature</th>
<th>HP SIM menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch of the System Management Homepage (SMH)</td>
<td>Tools&gt;System Info</td>
</tr>
<tr>
<td>Launch of Process Resource Manager (PRM)</td>
<td>Optimize</td>
</tr>
<tr>
<td>Launch of Event Monitoring System (EMS) tools (X-based)</td>
<td>Diagnose</td>
</tr>
<tr>
<td>Launch of SAM-based tools (x-based, for older HP-UX systems)</td>
<td>Configure</td>
</tr>
<tr>
<td>Launch of Software Distributor tools that run on the managed system</td>
<td>Deploy</td>
</tr>
<tr>
<td>Launch of simple command line tools such as bdf, ls, and so on</td>
<td>Tools&gt;Command Line</td>
</tr>
</tbody>
</table>

Some tools enable their launch from HP SIM when installed to the CMS. For example, when Serviceguard Manager is installed on a Windows-based HP SIM CMS, it creates the appropriate links to enable direct launch.
OpenView GlancePlus


Ignite-UX

Ignite-UX addresses the needs of HP-UX 11i system administrators who perform fast deployment for one or many servers. Ignite-UX provides the means for creating and reusing standard system configurations, enables replication of systems, permits post-installation customization, and can operate in both interactive and unattended modes. For more information, see [http://www.hp.com/go/ignite-ux](http://www.hp.com/go/ignite-ux). With Extensions for HP SIM on Windows, Ignite-UX options are available under the HP SIM Deploy menu. The Ignite-UX server must be configured and accessible, and the installer collects information for accessing the server.

Software Distributor-UX

Software Distributor-UX (SD-UX) is the HP-UX 11i administration toolset used to deliver and maintain the HP-UX 11i operating system and layered software applications. Delivered as part of HP-UX 11i, SD-UX helps manage the HP-UX 11i operating system, patches, and application software on HP servers. The HP SIM Deploy menu includes options for SD operations on HP-UX target nodes, and Extensions for HP SIM on Windows includes additional Deploy menu options for SD operations executed from the Central Management Server. Since the Central Management Server in this case is Windows-based, the installer configures these SD tools to run from the same HP-UX server designated as the Ignite server.

HP-UX Configuration Tools

HP supplies a variety of tools for configuring, monitoring, and managing the HP-UX operating system. These tools run on the HP-UX managed node and provide monitoring and management of peripherals and devices, kernel configuration, file systems and LVM, users and groups, and other aspects of the HP-UX operating system. HP-UX servers running 11i v2 or later can use web-based versions of tools. These tools are integrated aspects of the System Management Homepage, and are also available for direct launch from HP-UX and HP SIM. Older HP-UX servers have X-based versions of the configuration management tools that are integrated with SMH or the System Administration Manager (SAM). For more information, see [http://www.hp.com/go/integrityessentials](http://www.hp.com/go/integrityessentials). Extensions for HP SIM on Windows integrate many of these tools into the HP SIM Configure menu.

System Management Homepage

The HP-UX System Management Homepage (SMH) provides not only management of various aspects of the system, but also a visual assessment of the health of the system and its components and access to various log files. SMH is integrated with HP SIM, and can be launched from the same Tools>System Information menu, from the HP SIM system page of a server, or by clicking on the health status icon of a server in the HP SIM HS (health status) column. This integration is available with all HP SIM environments, so it is not included in Extensions for HP SIM on Windows.
Process Resource Manager

Process Resource Manager (PRM) for HP-UX is a resource management tool used on HP-UX to control the amount of resources that processes use during peak loads. PRM can manage allocation of CPU, memory, and disk bandwidth. PRM is included with the HP-UX 11i Enterprise Operating Environment and is integrated with all HP SIM environments so it is not included in Extensions for HP SIM on Windows.

HP-UX Workload Manager

HP-UX Workload Manager is an intelligent policy engine that provides automatic CPU resource allocation and application performance management based on prioritized service level objectives (SLOs). WLM improves response time for critical users, enables system consolidation, and helps manage user expectations for performance. WLM is included with the HP-UX 11i Mission Critical Operating Environment. WLM menu options are available under the HP SIM Optimize menu with Extensions for HP SIM on Microsoft Windows.
4 Monitoring and controlling servers

This chapter provides an overview for using the Insight Control Management software to manage server power consumption through the IPM, and ensure and monitor server health and performance through PMP.

Configuring Insight Power Manager options

**IMPORTANT:** When Insight Power Manager is installed it is disabled. To enable Insight Power Manager, select Options>Insight Power Manager Options, and then select Enable Insight Power Manager Plug-In.

The Insight Power Manager Options menu enables you to configure HP Insight Power Manager settings and display options.

The Insight Power Manager Options menu enables you to:

- Enable or disable HP Insight Power Manager capabilities on managed systems. If disabled, no network activity related to the gathering of power data is performed. This setting is global and affects all users.
- Configure up to five iLO 2 username and password pairs for access to managed systems. You can also configure an alternate SSL port number. This setting is global. The default setting is 443.
- Configure a designated time period to keep historical data. The data is deleted automatically after the specified time period has elapsed. This setting is global.
- Indicate whether to display temperature for a user in Celsius or Fahrenheit. This setting is configured by the user.
- Indicate whether to display power for a user in watts or Btus. This setting is configured by the user.

To configure IPM options:

1. Click Options>Insight Power Manager Options. The Insight Power Manager Options page appears.
2. To enable HP Insight Power Manager, select Enable HP Insight Power Manager Plug-In.
3. The Graph and Analysis Settings section provides the following options:
   - Temperature Unit of Measurement—Select a unit of measurement for the temperature from the list. Choices include Fahrenheit and Celsius. This setting is configured by the user.
   - Power Unit of Measurement—Select a unit of measurement for power from the list. This setting is configured by the user.
   - Use GMT for all timestamps in the graphs—Select this option if you want to use Greenwich Mean Time (GMT) when graphing data. This setting is configured by the user.
   - Cost of Power per kWh—Enter the average cost of power per kilowatt-hour. This box is used to calculate the cost of operation for the server and cooling. For ease of data entry, only one box is provided. If more cost analysis is required, use the Export option in the Power Regulator Actions section of the graphs. This box is used to calculate the cost and annual cost of operation for the server and cooling. This setting is configured by the user.
   - Currency Type—Enter the currency type. This box is used for display purposes only and is used in the Analysis section of the graphs that display cost information. The default value is USD, but the value can be changed to $, EUR, £, ITL, JPY, ¥, or any other printable character set that represents your currency. This setting is configured by the user.
○ Cooling Multiplier—Enter a cooling multiplier. This value represents the relative cost of cooling the server compared to the cost of powering the server. The default value of 1.5 indicates that it costs 1.5 times as much to cool the server as it does to power the server. This value is multiplied by the kilowatt-hours used by the server to arrive at a cooling kilowatt-hours value used in the Analysis section of the graphs that display power consumption information. This setting is configured by the user.

○ Power Line Voltage—Select the power line voltage from the dropdown list. This box is used to calculate the amperage consumed value in the Analysis section of the graphs that display power consumption information. This setting is configured by the user.

4. The Default Integrated Lights Out (iLO) Settings section enables you to configure a Secure Socket Layer (SSL) port number and provide login credentials for up to five managed systems.

The following options are available. The settings are global and affect all users:

○ Default SSL Port—Enter the SSL port number to be used by IPM to communicate with iLO. The default is 443.

○ User Name—Enter the user names used to connect to the iLO for the managed systems. You can enter up to five user name and password pairs in the Default 1-5 boxes.

○ Password—Enter the password for the previously named managed system iLO.

○ Confirm password—Re-enter the password for the iLO of the managed system exactly as you entered it in the Password box.

NOTE: IPM tests each name and password pair on managed systems until it successfully accesses power data.

5. The Default Power Regulator Data Expiration Settings section enables you to configure how long to keep historical data.

In the first Remove data older than list, select the time to be selected in the second list. For example, you can select Remove data older than 6 Month(s). All data that is 6 months or older is removed permanently.

6. To save your settings, click Apply.
Using the iLO browser interface

The iLO browser interface enables easy access to daily tasks through a selection of tabs. Each tab groups similar tasks for easy navigation and work flow. Typical tabs used are System Status, Remote Console, and Virtual Devices.

Using the System Status tab

The System Status tab displays the following options:

- **Summary**—The Summary tab displays high-level details about the system and iLO 2 subsystems and links to commonly used features.
- **System Information**—The System Information tab displays the health of the monitored system. Many features necessary to operate and manage the components of HP ProLiant servers migrated from the health driver to the iLO 2 microprocessor.
- **System Information Summary**—The System Information Summary tab displays the state of monitored host-platform subsystems status at a glance, summarizing the condition of all the monitored subsystems, including overall status and redundancy (the ability to handle a failure). The subsystems can include fans, temperature sensors, power supplies, and voltage regulator modules.
- **Fans**—iLO 2, working with additional hardware, controls the operation and speed of the fans. Fans provide essential cooling of components to ensure reliability and proper operation.
- **Temperatures**—The Temperatures tab displays the location, status, temperature, and threshold settings of temperatures sensors in the server chassis. The temperature is monitored to maintain the location temperature below the caution threshold. If one or more sensors exceed this threshold, iLO 2 implements the recovery policy to prevent damage to server components.
- **Power**—The VRMs/Power Supplies tab displays the state of each VRM (voltage regulator module) or power supply. VRMs are required for each processor in the system. VRMs adjust the power to meet the needs of the processor supported. A VRM can be replaced if it fails. A failed VRM prevents the processor from being supported.
- **Processors**—The Processors tab displays the available processor slots, the type of processor installed in each slot, and a brief status summary of the processor subsystem. If available, installed processor speed (in MHz) and cache capabilities appear.
- **Memory**—The Memory tab displays the available memory slots and the type of memory (if any) installed in the slot.
- **NIC**—The NIC tab displays the MAC addresses of the integrated NICs. This tab does not display add-in network adapters.
- **iLO 2 Log**—The iLO 2 Log tab displays the iLO 2 Event Log, which is a record of significant events detected by iLO 2. Logged events included major server events, such as a server power outage or a server reset, and iLO 2 events such as unauthorized login attempts.
- **IML**—The IML tab displays the Integrated Management Log, which is a record of historical events that have occurred on the server as reported by various software components. Events are generated by the system ROM and by services such as the System Management (health) driver.
- **Diagnostics**—The Diagnostics option displays the Server and iLO 2 Diagnostics screen which provides iLO 2 self-test results and a reset iLO 2 option, as well as comprehensive diagnostic information.
- **Virtual NMI (non-maskable interrupt) button**—This button halts the operating system for debugging purposes. This function is an advanced feature, and only use it for kernel-level debugging.
• iLO 2 self-test results—iLO 2 performs a series of initialization and diagnostic procedures on the subsystems of the iLO 2 system. The results appear on the Server and iLO 2 Diagnostics tab. All tested subsystems should display Passed under normal situations. Any test can display one of three results: Passed, Fault, or N/A.

• Insight Agents—The HP Insight Management Agents support a browser interface for access to runtime management data through the HP System Management Homepage. The HP System Management Homepage is a secure web-based interface that consolidates and simplifies the management of individual servers and operating systems. By aggregating data from HP Insight Management Agents and other management tools, the System Management Homepage provides an intuitive interface to review in-depth hardware configuration and status data, performance metrics, system thresholds, and software version control information.

**Using the Remote Console tab**

The Remote Console tab provides access to different views of the Remote Console and enables you to define keystroke sequences that are transmitted to the remote host server by pressing a hot key. iLO 2 uses virtual KVM technology to prove remote console performance that is on-par with other KVM solutions.

While standard iLO 2 enables remote console access from server power-on through POST, it might require an optional license key to continue to access the server console from there. For more information, see the *HP Integrated Lights-Out 2 User Guide*. The Remote Serial Console is available without an additional license and is suitable for host operating systems that do not require access to the graphical console.

The Graphical Remote Console turns a supported browser into a virtual desktop, giving you full control over the host-server display, keyboard, and mouse. The operating system-independent console supports graphic modes that display remote host server activities, including shutdown and startup operations.

• Integrated Remote Console Fullscreen—Enables you to resize the IRC to the same display resolution as the remote host. To return to your client desktop, exit the console.

• Integrated Remote Console option—Offers a high-performance remote console interface for Windows clients, combining KVM, Virtual Power, and Virtual Media functionality. The Integrated Remote Console option is an ActiveX control that runs from Internet Explorer.

• Remote Console Information screen—Appears when you click the Remote Console tab of the iLO 2 web browser-based interface, this screen shows all available Remote Console options and a link to download an updated Java™ Runtime Environment.

• Remote Console display—Redirects the host server console to the network client browser, providing full-text (standard) and graphical mode video, keyboard, and mouse access to the remote server (if licensed with iLO).

• Remote Serial Console—Enables you to access a VT320 serial console from a Java applet-based console connected to the iLO 2 Virtual Serial Port, with a broad browser compatibility that includes Windows and Linux browsers.

• Acquiring the Remote Console—Displays the Acquire button when the Remote Console Acquire setting on the Remote Console Settings screen is enabled. If you have opened the Remote Console page and are notified that another user is using Remote Console, to end the other user’s Remote Console session, click Acquire, and then in your current window, start a Remote Console session.

• Optimizing mouse performance for Remote Console or Integrated Remote Console—Enables you to set the mouse acceleration, which must be set correctly for the remote console to behave properly in certain Windows configurations.

• High-performance mouse settings—Enables the High Performance Mouse feature when using the Remote Console. This feature improves pointer performance and accuracy on Windows Server 2003 and Windows 2000 Service Pack 3 or later.
Using the Virtual Devices tab

The Virtual Devices tab provides the following options:

- **Virtual power button**—Enables control of the power state of the remote server and simulates physically pressing the power button on the server. If the remote host server is not responding, this feature enables an administrator to initiate a cold or warm reboot to bring the server back online.
- **Power Regulator for ProLiant**—Enables you to view and modify power regulation settings and view processor states and power meter readings.
- **Virtual media**—Enabled by licensing the optional iLO. If the iLO is not licensed, the following message appears: iLO 2 feature not licensed.
- **Virtual indicators**—The Unit ID LED is the blue LED on the HP server that is used for identifying systems in a rack of servers. iLO 2 enables you to view the status of the Unit ID LED and change the status using iLO 2 Web pages.

Monitoring PMP parameters

Servers are monitored based on monitoring parameters. The monitoring status and the number of samples must be configured in PMP for servers to be monitored.

Default PMP settings

The following are default monitoring settings:

- Monitor and Alert selected
- Number of samples to determine status—5

The default monitoring settings can be changed on the Monitoring Administration page.

Sample rate

**NOTE:** Sample rate is populated automatically.

PMP does not control the amount of time between samples. Instead, the sample rate (data collection interval) is set from within the HP Management Agents.

After you start monitoring a server, the sample rate that appears on the Monitoring Administration page is synchronized to equal the sample rate of the agents for the monitored server.

The servers connected to an enclosure determine the sample rate for a network storage enclosure. The sample rate for the storage enclosure is the highest sample rate of the connected servers.

Number of samples

PMP enables you to specify the number of samples from which the monitoring service calculates a running average of gathered entries to determine system performance status.
Using the PMP interface

This section provides an overview of PMP functionality. A usage scenario demonstrates setup, administration, and server monitoring.

Online and Offline Analysis

The PMP Online and Offline Analysis tools provide an intuitive interface to detail the performance status and inventory of monitored servers and processor memory, local and external storage, network storage, network connections, host bus, and virtual machine host components for each server. The tools provided for Online and Offline Analysis are similar in overall functionality. The major difference in performing Offline Analysis is that the data comes from a database rather than a real-time data stream.

Additionally, for performance analysis in a static setting, PMP provides many tools to assist in monitoring server performance. For more information about Offline Analysis, see the “Offline Analysis” section in this guide.

When you select a monitored server icon from the PF column of the Systems Insight Manager console or when you select Diagnose>Performance Management Pack>Online Analysis from the console toolbar, the PMP Online Analysis screen appears in a new browser window, as shown in the following screen. The analysis starts in the performance status view for the server.
**Systems detail frame**

The Systems detail frame appears at the top left side of the browser window below the banner and provides the following information:

- **Server name**—Displays the name of the server currently being monitored
- **Server OS**—Displays the operating system version of the server currently being monitored
- **Server IP**—Displays the IP address assigned to the server currently being monitored
- **Sample Rate**—Displays the frequency with which the agents are collecting performance data on the monitored server
- **Samples for Status**—Displays the number of samples averaged to determine system performance status
- **Alert**—Indicates if alerts are to be sent when certain server performance status conditions occur
- **Log**—Indicates if the performance data is currently being logged for the selected server
- **Set Threshold**—Provides a link for modifying the performance threshold values for the selected server

**Server Tree frame**

The Server Tree frame appears on the left side of the browser window. This frame is used to navigate between system components. Component performance and status information appear in a hierarchical tree with nodes for each level of the component. This frame provides a view of the server, processors, memory, network connections, storage, host bus components, and virtual machine host components.

**Results frame**

The Results frame displays the status, inventory, and graphical representation for the selected server and its components. Use the tabs in the Results frame to switch between these views. A list of the values corresponding to each server and its components is provided in the “PMP measurement categories” section of this guide.

The Results frame includes tabs to access the different representations of the information available for the server and its components. The tabs provide the following general information:

- **Status**—Lists the performance counters (metrics) associated with the selected component. The table provides the average, maximum, minimum, and last (current) values for all the counters. A status icon indicates the performance of the component. An increasing level of severity is indicated as the status changes from normal to major. The Status tab includes:
  - Analysis Explanation—Explaining why a bottleneck exists
  - Recommendation—Providing possible actions to relieve the bottleneck
  - Configuration Issues—Providing details about any issues detected for the components

  The server metrics and their definitions for data analyzed by PMP to determine the status of a particular component are provided in the “PMP measurement categories” section of this guide.

- **Graph**—Displays a graphical representation of the performance metrics associated with the selected component. The graph is dynamic, changing as the values change, and contains the last 25 measurements taken.

- **Inventory**—Displays information about the selected component configuration, such as the processor or NIC configuration. Information provided in the Inventory view is detailed in the “PMP measurement categories” section of this guide.

The Results frame provides the icon in the top right corner, which displays a context-sensitive help page.
Network Storage Analysis

Network storage Online Analysis appears in a new window separate from server analysis.

The usage scenario provides examples of bottleneck conditions with and without a recommended hardware upgrade, as well as examples of static and offline analysis.

PMP Reports

PMP can generate reports illustrating the percentage of time a system was in a bottleneck state and the overall performance utilization for a system categorized by its components. A System Summary Report can be generated from data in the performance database in HTML format. CSV File Generator can generate comma-separated value (CSV) files for import into desktop analysis or reporting tools. A Static Analysis Report is an analysis of the hardware configuration for the server as a whole, identifying potential problem areas. The Server availability report in the HTML format consolidates information on availability of servers at any point in time.

The CSV file documents each individual sample for every component analyzed, collecting different measurements for each. All report formats can generate reports for either one designated system or a group of systems as a whole.
For a sample CSV file and a list of associated values measured for each server and its components, see the “Sample PMP CSV file” section in this guide. This section also includes a sample System Summary report and Static Analysis report.

The reports that are generated through PMP are stored in
C:\Program Files\HP\Performance Management Pack 4\PMTools\htm\Reports
This is the default location for the generated reports.
Offline Analysis

Offline Analysis is used to view recorded data sessions from the database, enabling review of specific logged information sampled from the database. For more information about using Offline Analysis to view recorded data sessions, see the “Online and Offline Analysis” section in this guide.

During the session, data is shown in two refresh modes.

- **Auto mode**—Plays the data back at the selected playback rate. To enable auto mode, select the Auto Refresh checkbox.

- **Manual mode**—Enables you to advance the samples manually. To enable manual mode, click any navigation button. Manual mode navigation buttons include:
  - To the first sample
  - To the previous bottleneck
  - To the previous sample
  - To the next sample
  - Forward to the next bottleneck
  - To the latest sample
Manual Log Purge

Manual Log Purge enables the recorded sessions for a logged server or network storage enclosure, logged in the PMP performance database and occupying hard disk storage space, to be deleted. Use this tool regularly to remove unwanted recorded sessions and reduce database size.

To delete records in the performance database:

1. From the Systems Insight Manager console toolbar, select **Options > Performance Management Pack Options > Manual Log Purge**.
2. Select the checkbox next to the server or network storage enclosure for which to delete logged data.
3. Specify to delete data older than a specified number of days or a specified date.

**NOTE:** Data acquired for the current date of the analysis server cannot be deleted.

4. To remove the data from the performance database, click **Delete Selected Data**.

---

**Performance Management Pack**

**Manual Log Purge**

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Serial Number</th>
<th>Earliest Data Items</th>
<th>Latest Data Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.30.50.117</td>
<td>172.30.50.117</td>
<td>US06550192</td>
<td>03/02/2007 11:36:52 AM</td>
<td>03/05/2007 4:20:01 PM</td>
</tr>
<tr>
<td>172.30.50.126</td>
<td>172.30.50.126</td>
<td>US06550192</td>
<td>03/03/2007 3:35:45 PM</td>
<td>03/05/2007 4:20:47 PM</td>
</tr>
<tr>
<td>172.30.50.212</td>
<td>172.30.50.212</td>
<td>US06550192</td>
<td>03/03/2007 3:30:49 PM</td>
<td>03/05/2007 4:20:65 PM</td>
</tr>
<tr>
<td>172.30.50.130</td>
<td>172.30.50.130</td>
<td>HSE0000192</td>
<td>03/03/2007 3:34:51 PM</td>
<td>03/05/2007 4:21:19 PM</td>
</tr>
<tr>
<td>172.30.50.166</td>
<td>172.30.50.166</td>
<td>US06550192</td>
<td>03/03/2007 3:35:45 PM</td>
<td>03/05/2007 4:20:34 PM</td>
</tr>
<tr>
<td>172.30.50.121</td>
<td>172.30.50.121</td>
<td>US06550192</td>
<td>03/03/2007 11:34:01 AM</td>
<td>03/05/2007 4:21:13 PM</td>
</tr>
<tr>
<td>172.30.50.193</td>
<td>172.30.50.193</td>
<td>US06550192</td>
<td>03/03/2007 3:30:19 PM</td>
<td>03/05/2007 4:15:18 PM</td>
</tr>
<tr>
<td>172.30.50.1</td>
<td>172.30.50.1</td>
<td>US06550192</td>
<td>03/03/2007 3:37:25 PM</td>
<td>03/05/2007 4:19:41 PM</td>
</tr>
<tr>
<td>172.30.50.110</td>
<td>172.30.50.110</td>
<td>US06550192</td>
<td>03/03/2007 3:35:19 PM</td>
<td>03/05/2007 4:20:38 PM</td>
</tr>
</tbody>
</table>

**Remove Data Older than**

- [ ] Day(s)
- [ ] YYYY-MM-DD

**Delete Selected Data**

---

**Monitoring and controlling servers**
Using PMP

These sections provide an overview of PMP functionality. A usage scenario demonstrates setup, administration, and monitoring of servers.

Opening the HP SIM console

The HP SIM console, which appears in a Microsoft Internet Explorer browser window, shows performance status in the PF column. Icons in this column indicate the current performance state of a server.

In the following figure, an amber (Major) icon indicates a bottleneck condition exists on the server named pmpserver. This server is referenced in the following sections.
Debugging a server bottleneck condition

The following sections discuss the appropriate actions to take when a bottleneck condition exists on a server. In this scenario, the server name is pmpserver.

Selecting the server

To display the PMP Online Analysis window for pmpserver, click the **Major** icon.

The screen displays the server tree in the left navigation pane and the Status tab in the right pane. The counters that appear in the following figure are selected items from the various components. The Analysis Explanation indicates that at least one component has a critical performance issue.

[Image of PMP Online Analysis window]

Server problems can also be viewed in the Server Configuration pane. The tree structure in the Server Configuration frame displays the configuration of each server, including the individual components monitored by PMP. The icons shown in the tree next to a server or component indicate the performance status for that item or the item under the server. The performance status icon for the selected server also appears in the Results pane. PMP indicates multiple problems for the server in this example. Generally, only one component has a critical performance issue because bottlenecks tend to mask one another.
Displaying the memory status

In the Server Configuration frame, to access the memory information and display the Status page for memory in the Results frame, select **Memory**. Related and important memory counters appear in the Analysis Data table.

```
<table>
<thead>
<tr>
<th>Counter</th>
<th>Last</th>
<th>Average</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Mbytes</td>
<td>101</td>
<td>100.2</td>
<td>99.53</td>
<td>101.8</td>
</tr>
<tr>
<td>Page Faults/sec</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Page Faults/sec</td>
<td>241</td>
<td>241</td>
<td>241</td>
<td>241</td>
</tr>
</tbody>
</table>
```

The Analysis Explanation details an above-average page-read rate (below 5 is normal), however, there is still less than 15 MB of available memory.

In this example, the situation might have occurred because a new batch job was assigned to run on the server at night. The remainder of this scenario examines other performance information available to assist in troubleshooting to determine if immediate action is required to resolve the performance bottleneck.
Displaying the memory graph

To show a graphical display of memory counters in the Results pane, click the **Graph** tab.

This graph displays the last 25 samples taken for the server. The duration of the graph is 25 times the sampling rate of 10 seconds, or 4.16 minutes, as shown near the upper right corner of the screen. The graph displays what occurred on the server from 1:13 p.m. to 1:17 p.m.

The pattern of the graph shows rising, peaking, and declining, which might be caused by the completion of the new batch job. The batch job no longer causes a problem. However, the performance information is logged in the database for later review with the Offline Analysis tool.
Contrasting the graphical display

The following sections further demonstrate the graphical display and the full depth of analysis.

Expanding the local storage

To expand the tree structure, click the + icon next to Storage in the configuration tree, and then select the storage node.
Displaying the controller

To display the tree structure for the Smart Array 5i controller, click the + icon next to SA 5i in the configuration tree. The arrays defined for that controller and the SCSI bus entries (ports) appear.
Displaying the port

To open the tree structure for the storage system:

1. Click the + icon next to Port 1 Internal Drive Cage in the configuration tree.
2. Scroll the pane to the right to display the physical drives on that SCSI bus. Some drives have a major icon.
Displaying the drive

Click the **ID 0: 146G 15K U320 (Array A)** drive. The graph displays the performance statistics for that drive over the last 4.16 minutes.

The graph in the previous figure trends upward to the right and levels high. These characteristics indicate that the system is not returning to normal and might require immediate action.
Displaying the inventory

To display information for the selected drive, select the **Inventory** tab.

Hardware or configuration details for the currently selected device appear.
Debugging a network storage bottleneck condition

The following sections detail the appropriate responses when a bottleneck condition exists on network storage. In this scenario, the server name is pmp-client2k, sharing network storage MSA1500cs. An amber (Major) icon in the PF column indicates a bottleneck condition exists on the server pmp-client2k.

Selecting the server

To display the PMP Online Analysis window for pmp-client2k, click the **Major** icon.

The screen displays the server tree in the Server Configuration frame and the Status tab in the Results frame. The counters that appear in the following figure are selected items from the various components. The Analysis Explanation indicates that at least one component has a critical performance issue.

Server problems can also be seen within the Server Configuration frame. The tree structure in the Server Configuration frame displays the configuration of each server, including individual components monitored by PMP. The icons appearing in the tree next to a server or component indicate the performance status for that item or the item under the server. The performance status icon for the selected server also appears in the Results frame. PMP indicates multiple problems for the server in this example. Generally, only one component has a critical performance issue because bottlenecks tend to mask one another.
Displaying the storage status

Trace the performance issue by using the information that appears next to the amber (Major) icon.

In the Server Configuration frame, to access the storage information and display the storage status page in the Results frame, select Storage. Related and important storage counters appear in the Analysis Data table.

The Analysis Explanation indicates that at least one storage controller or network storage enclosure is reporting a performance issue.

The remainder of this scenario examines other performance information available to assist in troubleshooting the critical performance issue to determine if immediate action is required to resolve the performance bottleneck.
Displaying the network storage status

In the Server Configuration frame, to access the storage information and display the storage status page in the Results pane, click SGA04300BE (Enclosure name of MSA1500cs). Related and important storage counters appear in the Analysis Data table.

The Analysis Explanation indicates that the network storage enclosure is experiencing a performance issue.
Displaying the logical drive under network storage

In the Server Configuration frame, to access the network storage information and display the storage status page in the Results pane, click **Disk 4H**. Related and important storage counters appear in the Analysis Data table.

The Analysis Explanation indicates that this logical drive is experiencing a performance issue.
Displaying the network storage enclosure

In the Server Configuration frame, to access the network storage enclosure page, click the icon next to the SGA04300BE (Enclosure name of MSA1500cs) listing. The Storage Enclosure Online Analysis page appears. This page displays the storage status page in the Results pane. Related and important storage counters appear in the Analysis Data table.

The Analysis Explanation indicates that this network enclosure is experiencing a performance issue.
Displaying the array

In the Server Configuration frame, to access the array information and display the array status page in the Results frame, select **Array B (1 drives)**. Related and important array counters appear in the Analysis Data table.

The Analysis Explanation indicates that high disk activity is detected.
Displaying the hard disk status

In the Server Configuration frame, to access the hard disk information and display the hard disk status page in the Results frame, select ID 6: 18G 10K U3 (Array B). Related and important hard disk counters appear in the Analysis Data table.

The Analysis Explanation indicates that a high-level disk queue is detected, which indicates a performance bottleneck on a hard disk in Array B.

Debugging a virtual machine host and guest bottleneck condition

The following sections detail the appropriate actions to take when a bottleneck condition exists on virtual machine hosts and guests. In this example, the server name of the server hosting virtual machine guests is pmpserver-3. An amber (Major) icon in the PF column indicates a bottleneck condition exists on the server (virtual machine host) named pmpserver-3.

**IMPORTANT:** The virtual machine host must be licensed in the Virtual Machine Management Pack before licensing and monitoring by PMP.
Selecting the server (virtual machine host)

To display the PMP Online Analysis window for pmpserver-3, click the amber (Major) icon.

The screen displays the server node tree in the left configuration navigation pane and the Status tab in the right pane. The counters that appear in the following figure are selected items from the various components. The Analysis Explanation indicates that at least one node has a problem.

Problems with a server can also be seen in the configuration navigation pane. The tree structure in the configuration navigation displays the configuration of each node down to the individual components monitored by PMP. The icons used in the tree next to a node or component indicate the performance status for that item or the item under the node. The performance status icon for the selected node is in the Results frame. In this example, PMP indicates the server has multiple problems. Generally, only one node has a problem because bottlenecks tend to mask one another.
Displaying the virtual machine host status

Trace the performance issue by using the information that appears next to the amber (Major) icon.

From the navigation tree, to access the virtual machine host information and display the status page for the host in the right pane, click **VMware GSX Server**. Related and important counters for the virtual machine host appear in the Analysis Data table.

![Online Analysis](image)

In this example, the Analysis Explanation indicates that the virtual machine host or at least one virtual machine guest is reporting a performance issue.

The remainder of this example examines other performance information available to assist in making a judgment regarding the problem and determines if immediate action is required to resolve the performance bottleneck.
Displaying the virtual machine guests page

From the navigation tree, to access the virtual machine guests page, click next to the VMware GSX Server. The VM Online Analysis page appears. This page displays the status page for the virtual machine host in the right pane. Related and important counters for the virtual machine host appear in the Analysis Data table.

In this example, the Analysis Explanation indicates that this virtual machine host is experiencing a performance issue.
Displaying the virtual machine guest

From the navigation tree, to access the virtual machine guest and display the status page in the right panel, click the associated virtual machine guests tree. Related and important counters for the virtual machine guest appear in the Analysis Data table.

In this example, the Analysis Explanation indicates that at least one component has a critical performance issue.
Displaying the virtual machine guest processor status

From the navigation tree, to access the virtual machine guest processor information and display the status page for the virtual machine guest processor in the right pane, click Processor. Related and important counters for virtual machine guest processor appear in the Analysis Data table.

In this example, the Analysis Explanation indicates that processor utilization is extremely high (over 90%) and probably causing performance degradation.
Addressing performance issues with no hardware upgrade recommendation

The following scenario provides an example of a recommendation that does not suggest additional hardware.

In the following figure, a major status icon appears for the processors. Online Analysis recommends that you determine if the processing load can be distributed more evenly across the available processors.

This recommendation indicates that more than one logical processor exists in the system and at least one processor is not fully utilized. This recommendation demonstrates not only a solution without involving hardware, but also the specificity of PMP. Online Analysis recommendations for these types of performance issues are component-specific.
Performing a static analysis

The following sections provide examples of using static analysis.

General usage

Performance issues are often introduced during system configuration. This condition might be caused by a planning error, an error in following the prescribed configuration path, or as a result of the system receiving many updates to a system over time. Regardless of the cause, PMP can analyze static configurations and make suggestions about areas of concern before a change occurs.

To see a static analysis report:

1. From the Systems Insight Manager console toolbar, click **Reports>Performance Management Pack Reports>Static Analysis Report**.
2. Select the **pmpserver** checkbox.
3. To display the Static Analysis Report for pmpserver, click **Generate Report**. These results can be printed from the browser.

### Static Analysis Report

- **Server Name:** pmpserver
- **Server IP:** 172.28.55.89
- **Serial Number:** 0D081621609

**Processors**
- 2 processors detected & supported.
- No multi-processor configuration issues identified.

**Memory**
- 4 memory modules (8) in 8 memory sockets.
- No memory configuration issues identified.

**Network Connections**
- NIC781 (1): No configuration issues identified.
- NIC781 (2): No configuration issues identified.

**Storage**
- One or more configuration issues detected on SA 5a
- One or more configuration issues detected on SA 5300 in Slot 1
- One or more configuration issues detected on SA 5300 in Slot 2
- SA 5c: At least one drive is running at a reduced SCSI speed on SCSI Port 1. SA 5300 in Slot 1:
  - Controller inserted into PCI slot, but no drive detected.
  - SA 5300 in Slot 2:
  - Controller inserted into PCI slot, but no drive detected.
Half duplex port

Review the report shown in the following figure.

The report shows the first potential issue, indicated by the **At least one port is running in Half Duplex mode** message. PMP indicates that a network port is running in half-duplex mode, which can cause a bottleneck. In this case, half duplex was set in error, and that setting is causing an artificial bottleneck for network traffic over that port.

```
Static Analysis Report

Server Name: prepserver
Server IP: 172.20.05.69
Server Number: 00000000000000

Processors
2 processor(s) detected (6 supported),
No multi-processor configuration issues identified.

Memory
4 memory module(s) in 6 memory sockets,
No memory configuration issues identified.

Network Connections
NIC7761 (1):
At least one port is running in Half-Duplex mode

Storage
One or more configuration issues detected on S A 5 i
One or more configuration issues detected on SA 5300 in Slot 1
One or more configuration issues detected on SA 5300 in Slot 2
SA 5 i:
At least one drive is running at a reduced SCSI speed on SCSI Port 1.
SA 5300 in Slot 1:
Controller inserted into PCI slot, but no drive detected.
SA 5300 in Slot 2:
Controller inserted into PCI slot, but no drive detected.
```
Unassigned disks

The next message in the report that might indicate a problem is One or more physical disks are not assigned to an array. In many cases, this condition can be expected, particularly if online spare drives are configured because they are not part of an array set. However, this condition might be unexpected if there is an interrupted array configuration attempt.

<table>
<thead>
<tr>
<th>Static Analysis Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name:</td>
</tr>
<tr>
<td>Server IP:</td>
</tr>
<tr>
<td>Serial Number:</td>
</tr>
<tr>
<td>Processors</td>
</tr>
<tr>
<td>Memory</td>
</tr>
<tr>
<td>Network Connections</td>
</tr>
<tr>
<td>Storage</td>
</tr>
</tbody>
</table>
Reduced SCSI speed

The next message in the report that might indicate a problem is at least one drive is running at a reduced SCSI speed on SCSI Port 1. In this example, the HP ProLiant DL380 server was configured correctly with a new Smart Array controller and Ultra320 drives, but the drives are not running at Ultra320 speed. Further examination of the hardware might reveal an older SCSI cable as a potential problem. Testing might reveal that the differential pin on the SCSI cable is bad, causing the drive and controller to revert to SCSI-2 speed for transmission. PMP detects the potential performance problem and helps narrow the cause before any product work is done on the server.

Host bus balancing

Although no error messages appear in this static analysis, PMP can determine how the devices in a system are laid out across the host buses and what issues might arise from bus overloading.
Performing Online Analysis

The PMP Online Analysis tool enables performance data to be viewed from a real-time data stream and provides an intuitive interface to detail the performance status and inventory of monitored servers and their components.

Online Analysis is used to determine that the system required more physical memory to handle the assigned load balance.

To use Online Analysis, choose either of the following options:

- From the Systems Insight Manager PF column, click the monitored server icon.
- Perform the following steps:
  1. From the Systems Insight Manager console toolbar, click Diagnose> Performance Management Pack>Online Analysis.
  2. Select the checkbox next to the server or servers for which to view performance data. The checkbox at the top of the column can be used to select all of the servers listed on the page.
  3. Click Apply Selections>Run Now. Online Analysis appears in a new window.

When Online Analysis is started for a server, an Online Analysis session is started automatically for any network storage enclosure connected to that server.

PMP supports VMware ESX 2.5.2, 2.5.3, 2.5.4, 3.0, and 3.0.1, but there are differences in the way PMP analyzes servers running with VMware ESX operating systems. If you have VMware ESX operating system installed and you have not configured Virtual Machines, PMP treats this ESX operating system as a server similar to a Linux operating system. However, there is no difference in the data analysis.

If you have VMware ESX operating system installed, and you have configured Virtual Machines, PMP treats this server as a VM host. When PMP identifies the server as a VM host, you must license the server through Virtual Machine Management Pack. When the VM host is licensed through Virtual Machine Management Pack, PMP collects performance data of the host. However, PMP displays only limited performance data. PMP analyzes performance of the processor subsystem and is presented to the server. In addition, in the Online and Offline Analysis pages, only the Inventory Tab appears for the Storage, NIC, and Host Bus subsystems.

The Redirect icon for the VM Host will appear only when the associated VM Guests are being monitored.

Performing Offline Analysis

The Offline Analysis tool enables performance data to be viewed from a database that has been captured and logged over a specified time. This tool enables manipulation of the rate at which data is played back for analysis by speeding or slowing the refresh rate or selecting specific points in the presentation of previously captured events without regard to chronology.

In the previous example, it was determined that the system required more physical memory to handle the assigned load balance. Offline Analysis enables examination and analysis of precisely what occurred on pmpserver between 3:01 to 3:37 P.M. when a problem occurred.

The Offline Analysis tool enables you to view recorded data sessions from the PMP database.

To use Offline Analysis:

1. From the Systems Insight Manager console toolbar, click Diagnose> Performance Management Pack>Offline Analysis.
2. Select the checkbox next to the server or servers for which to view performance data. The checkbox at the top of the column can be used to select all of the servers listed on the page.
3. Click **Apply Selections→Run Now**.

4. Select the start date and refresh rate for which to display performance data. The refresh rate determines the rate at which the logged data is played back.

5. Click **Start Offline Analysis**.

After selecting offline analysis parameters, the session appears as illustrated in the following figure. For information about navigation tools and the tabs provided with this interface, see the “Using PMP” section in this guide.

The following icons are provided for bottleneck navigation:

- ![Go back](image) Go back to the previous bottleneck
- ![Go forward](image) Go forward to the next bottleneck

For example, if a status change happens at 6:00 a.m. from green to amber, yellow to amber, or green to yellow, click the **Next** or **Previous** bottleneck navigation button and the Offline Analysis page for 6:00 a.m. appears. However, if the status changes at 6:00 a.m. from amber to yellow, amber to green, or yellow to green, the next bottleneck button does not navigate to that time.

PMP Offline Analysis can detect hardware configuration changes. A message appears when a configuration change is identified, as shown in the following figure.
Data reporting

Because PMP can be configured to store all performance data measurements that are analyzed, stored data can be converted to reports. Reports are generated from HP SIM. The report, when generated for a specific server, provides a summary of the performance statistics for the time period selected.

To generate a report:

1. Select **Reports > Performance Management Pack Reports**.
2. Click the format in which to generate the report. Available formats are:
   - Static Analysis Report
   - System Summary Report
   - CSV File Generator
   - Server Availability Report

For a description of these report types, see the following sections.
Generating a Static Analysis Report

1. When a separate browser window appears listing the selected servers, select the server for which you want to generate a report.
2. Enter the appropriate dates in the Report on Data From and Report on Data To boxes to get the period for which you want to generate the report. Leave these boxes blank to generate a report from the current performance data.
3. Click **Generate Report**. The report appears in a separate browser window.

Generating a SQL queries list

1. From the Static Analysis Report screen, select the server for which you want to generate a list.
2. Enter the appropriate dates in the Report on Data From and Report on Data To boxes to get the period for which you want to generate the list. Leave these boxes blank to generate a list from the current performance data.
3. Click **Show SQL queries**. The SQL query appears in a separate browser window. The static analysis report is not available for VM guests.

Reviewing scenario information

Because PMP supports VMware ESX 2.5.2, 2.5.3, 2.5.4, 3.0, and 3.0.1, there are differences in the manner PMP analyzes servers working with different VMware ESX operating systems.

Scenario 1—VMware ESX operating system installed without configured virtual machines

PMP treats this server as a server similar to that with a Linux operating system. However, there is no difference in the data analysis.
Scenario 2—VMware ESX operating system installed with configured virtual machines

PMP treats this server as a virtual machine host. After PMP identifies the server as a virtual machine host, you must license the host through the Virtual Machine Management Pack. After the virtual machine host is licensed through the Virtual Machine Management Pack, the PMP collects performance data of the host. However, PMP displays only limited performance data. PMP analyzes performance of the processor subsystem and is presented to the server. In addition, in the Online and Offline analysis pages, only the Inventory tab is present for the child nodes of Storage, NIC, and Host Bus subsystems.

Generating a System Summary Report

1. When a separate browser window appears listing the selected servers, select the server for which you want to generate a report.
2. Enter the appropriate dates in the Report on Data From and Report on Data To boxes to get the period for which you want to generate the report.
3. Enter an appropriate file name with an .htm extension in the File Name box.
4. Click **Generate Report**. The report appears in a separate browser window.

Generating a SQL queries list

1. From the System Summary Report screen, select the server for which you want to generate a list.
2. Enter the appropriate dates in the Report on Data From and Report on Data To boxes to get the period for which you want to generate the list.
3. Click **Show SQL queries**. The SQL query appears in a separate browser window.
Generating a CSV File Generator Report

1. When a separate browser window appears listing the selected servers, select the server for which you want to generate a report.
2. Enter the appropriate dates in the Extract Data From and Extract Data To boxes to get the period for which you want to generate the report.
3. Enter an appropriate file name with a .csv extension in the File Name box.
4. Click Generate File. The report appears in a separate browser window.

Generating a SQL queries list

1. From the CSV File Generator screen, select the server for which you want to generate a list.
2. Enter the appropriate dates in the Extract Data From and Extract Data To boxes to get the period for which you want to generate the list.
3. Click Show SQL queries. The SQL query appears in a separate browser window.
Generating a Server Availability Report

1. When a separate browser window appears listing the selected servers, select the server for which you want to generate a report.
2. Enter the appropriate dates in the **Report on Data From** and **Report on Data To** boxes to specify the period from which to generate the report.
3. Enter an appropriate file name with an .htm extension in the **File Name** box.
4. Click **Generate Report**. The report appears in a separate browser window.

Generating a SQL queries list

1. From the Server Availability Report screen, select the server for which to generate a list.
2. Enter the appropriate dates in the **Report on Data From** and **Report on Data To** boxes to specify the period from which to generate the list.
3. Click **Show SQL Queries**. The SQL query appears in a separate browser window.

**NOTE:** Server availability reports are not available for virtual machine guests.

Licensing Integrity and Storage Systems

You do not need a license for monitoring Integrity and storage systems.
Licensing virtual machine hosts and virtual machine guests

The procedure to license virtual machine hosts is not the same as the procedure to license other servers. However, as a prerequisite, the virtual machine host must be licensed in Virtual Machine Management Pack. The VM Host cannot be licensed for PMP if it is not licensed in Virtual Machine Management Pack. The virtual machine guests do not have any license for PMP, and all virtual machine guests appear in the Licensing Administration page in the All Devices Not Available for licensing list with the license status as VM Guest.

**Configuration**

**Step 2: Licensing Setup**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>IP Address</th>
<th>License Status</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host-vm1</td>
<td>172.20.10.2</td>
<td>Licensed</td>
<td>VMGuest</td>
</tr>
<tr>
<td>Host-vm2</td>
<td>172.20.10.3</td>
<td>VMGuest</td>
<td>Windows</td>
</tr>
<tr>
<td>Host-vm3</td>
<td>172.20.10.4</td>
<td>VMGuest</td>
<td>Windows</td>
</tr>
</tbody>
</table>

**IMPORTANT:** If you license a server for PMP and then convert that server to a virtual machine host, you are not required to license the virtual machine host again for PMP. However, this virtual machine host must be licensed for Virtual Machine Management Pack. The virtual machine host can be monitored only when licensed by Virtual Machine Management Pack. Similarly, if a virtual machine host is converted to a physical server, it is not expected to be licensed again for PMP.

For more information about licensing Virtual Machine Management Pack, see the Virtual Machine Management Pack documentation.
Monitoring administration

Servers are monitored based on monitoring parameters. The monitoring status and the number of samples are set in PMP for servers and storage enclosures that you want to monitor.

**NOTE:** The Update Server List populates only the latest licensed servers in the Monitoring administration table.

Changing server monitoring status

Servers that are licensed for monitoring appear on the Monitoring Administration page. Servers that are currently being monitored by PMP appear with Started as the value in the Monitor Status column. Servers that are not currently being monitored have no value in the Monitor Status column. The default values for monitoring status and number of samples are listed beside each server.

The server list that appears on the Monitoring Administration page can be filtered to display all devices, all monitoring devices, all devices available for monitoring, all alerting devices, all devices available for alerting, all logging devices, or all devices available for logging. Select the appropriate filter from the View list box. Use the page links that appear when there are multiple pages to navigate between pages.

The view filter is not applicable for VM Guests. The VM Guest does not appear for the All devices available for monitoring filter, even though it is not marked for monitoring when the host is being monitored. The VM Guest only appears in the list depending on the VM Host status. If the VM Host is not marked for monitoring, then all associated VM Guests appear in this list. Similar conditions apply for Alert and log. Monitoring of VM Guests is stopped if the associated VM Host is stopped for monitoring.
To change the monitoring status for a particular server:

1. From the Systems Insight Manager console toolbar, select **Options > Performance Management Pack Options > Configuration**.
2. Click the **Server** tab. Servers or network storage enclosures available for monitoring appear in the list.
3. Identify the server for which you want to change monitoring parameters from the server list, and then select or clear the box next to the server. The checkbox at the top of the column can be used to select or clear all servers listed on the page.
4. Select or clear the monitoring parameters (Monitor/Alert/Log) for the server, and then select the number of samples to use to determine status from the list.
5. Click **Apply**. The changes made to the monitoring status of the server are updated.
6. Selected servers begin a new monitoring session with the updated parameters, terminating any current monitoring session.

### Enabling network storage logging

Network storage enclosures that are licensed and connected to servers currently being monitored are automatically monitored. These enclosures appear on the Monitoring Administration page.

To enable logging for a network storage enclosure:

1. From the Systems Insight Manager console toolbar, select **Options > Performance Management Pack Options > Configuration**. The Monitoring Administration page appears in a new window.
2. Click the **Network Storage** tab. Network storage enclosures currently being monitored appear in the list.
3. Select the storage enclosures for which you want to enable logging, or use the checkbox at the top of the column to select or clear all items listed on the page.
4. Select the Log checkbox, and then select the number of samples to use to determine status from the menu.

5. To begin logging, click Apply.

6. To disable logging, repeat steps 1 through 5, clearing the Log checkbox.

Data is only logged to the PMP database for storage enclosures after logging is selected and parameters are applied. Network storage logging is independent of the connected servers. For example, data can be logged for a storage enclosure, and not be logged for the connected servers.

Enabling virtual machine host and virtual machine guests logging

Virtual machine guests that are configured on the virtual machine host currently being monitored are not automatically monitored. These virtual machine guests appear on the Monitoring Administration page with a checkbox and can either be selected individually or collectively using the Virtual Machine Guests checkbox.

To enable logging for virtual machine guests:

1. From the HP SIM console toolbar, select Options>Performance Management Pack Options>Configuration. The Monitoring Administration page appears in a new window.

2. Select the Server tab. Servers or virtual machine hosts and virtual machine guests available for monitoring appear in the list.

3. Select the virtual machine guest for which to change monitoring parameters. To select all the items listed on the page, select the checkbox at the top of the column.

4. Select the monitoring parameters (Monitor, Alert, and Log) for the virtual machine guests.
5. Click **Apply**. The changes made to the monitoring status of the server are updated.

Selected virtual machine guests begin a new monitoring session with the updated parameters and terminate any current monitoring session.

Data for virtual machine hosts and virtual machine guests is only logged to the PMP database after logging is selected and parameters are applied. Logging of virtual machine guests is not independent of the connected virtual machine hosts. For example, data cannot be logged for a virtual machine guest if not also logged for the connected virtual machine host.

**IMPORTANT:** To monitor, alert, and log virtual machine guests, enable the monitor, alert, and log parameters for the associated virtual machine host.

**NOTE:** The sample rate, log days, and number of samples cannot be set for the virtual machine guests. These values are the same as those of the virtual machine host.

### Monitoring parameters

PMP monitoring can operate in four modes:

- **Monitor**—This mode enables server status monitoring, updating information that HP SIM and PMP display. Analysis information and debug performance issues can be viewed using the Online Analysis tool.
- **Monitor & Alert**—This mode, in addition to the capabilities enabled with Monitor, sends alerts to HP SIM when the status of a server changes.
- **Monitor, Log, & Alert**—This mode, in addition to the capabilities enabled with Monitor & Alert, stores detailed performance information in the PMP database for later reporting or playback, using the Offline Analysis tool.
- **Monitor & Log**—This mode enables monitoring of servers and stores the performance information in the PMP database for playback later.

When monitoring begins for a server, the alert and log status in the table reflect that the Alert and Log options are chosen. When the monitoring ends, the table shows the previous state of Alert and Log status. The following figure illustrates the details.

<table>
<thead>
<tr>
<th>SI #</th>
<th>Check box options</th>
<th>Results in the table</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monitor</td>
<td>Alert</td>
</tr>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Row number 1:** Monitoring is started, Alert and Log enabled. The results are Started, Tick and Tick in the table.
- **Row number 2:** Monitoring, Alert and Log disabled. The results are Blank, Tick and Tick in the table reflecting the previous state of Alert and Log when the monitoring is stopped.
• Row number 6: Monitoring is started, Alert enabled and Log disabled. The results are Started, Tick and Blank reflecting the current status whenever the monitoring is started.
• Row number 7: Monitoring, Alert and Log disabled. The results are Blank, Tick and Blank reflecting the previous state of the Alert and Log when the monitoring is stopped.

Number of samples
The Number of samples setting enables adjustment of PMP analysis to account for highly variable or stable system performance. A higher number of samples results in smaller average changes in performance. Therefore, it generates fewer performance bottleneck indications for a server whose performance changes significantly. Fewer samples can be used for servers with more stable performance or when the sampling rate is higher.

Performance threshold setting
The hyperlink To Set Performance Threshold values click here enables setting the performance threshold values for the selected server in a separate page. For more information, see the “Performance threshold setting” section in this guide.

Modifying the sample rate
PMP does not control the amount of time between samples. Instead, the sample rate (data collection interval) is set from within the HP Management Agents. The Management Agents can be modified from the Control Panel or Internet Explorer.

The sample rate for a network storage enclosure is determined by the servers to which the enclosure is connected. The sample rate for storage enclosures is the highest sample rate of the connected servers.

Modifying log days
The log days option enables you to choose the number of days for which you need data logged. You can select a value for this option using the two lists. The first list contains values from 1 through 20. The second list has options such as days, months, and years. For example, if you select 2 in the first list and Years in the second list, data is logged for 760 days. The data that was logged first is replaced cyclically as new data is logged.
Modifying Management Agents from the Control Panel

1. From the Control Panel, open **HP Management Agents**.
2. Click the **SNMP Settings** tab.
3. Modify the **Data Collection Interval** (sample rate) as necessary.
Modifying Management Agents from Internet Explorer

1. Browse to the server where you have installed the Management Agents (for example, http://servername:2301/, where servername is the name of your server and 2301 is the active port).

2. Log in as an administrator.

3. Click the **Settings** tab.

4. Click **SNMP Configuration** > **Management Agents**.

5. Modify the **Data Collection Interval** (sample rate) as necessary, and then click **Apply**.

6. After the sample rate is changed, restart the Management Agents.
Setting performance thresholds

The Set Performance Threshold option enables you to set performance threshold values for processor, memory, NIC, storage, and PCI subsystems of the servers.

You can set performance by navigating through any of the following options:

- HP SIM menu
- Monitoring Administration page
- Online Analysis page

To set thresholds using the HP SIM menu:

1. From the HP SIM menu, select **Options>Performance Management Pack Options>Set Performance Threshold**.
2. Select the servers for which to set thresholds. Thresholds cannot be set for the network storage and virtual machine guests.
3. To set thresholds, click **Apply**.

To set thresholds from the Monitoring Administration page:

1. From the Monitoring Administration page, click the **To Set Performance Threshold values click here** link.
2. Select the servers for which to set thresholds. Thresholds cannot be set for the network storage and virtual machine guests.
3. To set thresholds, click **Apply**.

To set thresholds using the Online Analysis page:

1. From the Online Analysis page, System Details frame, click the **Set Threshold** link. Thresholds cannot be set for network storage and virtual machine guests. Threshold values are set only for the server being analyzed.

2. To set thresholds, click **Apply**. To return to the Online Analysis page, click **Cancel**.

**Threshold values**

Threshold settings for the various subsystems enable PMP analysis adjustment to account for highly variable or stable system performance. A higher value used results in smaller average changes in performance. A higher value used also generates fewer performance bottleneck indications for a server whose performance changes dramatically. A smaller value can be used for servers with more stable performance or when the sampling rate is higher.
Manual Log Purge

Manual Log Purge enables the recorded sessions for a logged server or network storage enclosure, logged in the PMP performance database and occupying hard disk storage space, to be deleted. Use this tool regularly to remove unwanted recorded sessions and reduce database size.

To delete records in the performance database:

2. Select the server or network storage enclosure for which to delete logged data.
3. Specify to delete data older than a specified number of days or a specified date.

NOTE: Data acquired for the current date of the analysis server cannot be deleted.

4. To remove the data from the performance database, click Delete Selected Data.
This chapter provides an overview for using the Rapid Deployment Pack to deploy servers and the Vulnerability and Patch Management Pack to perform vulnerability scanning and deploy patches and fixes.

Predeployment configuration

The Physical Devices view in the Deployment Server Console displays the physical relationship among the racks, enclosures, and server blades using the rack name and enclosure name for each HP BladeSystem server. The display name for a new server blade is a combination of the rack name, enclosure name, and bay number. Before you connect the first server in an enclosure to the Deployment Server, assign the rack and enclosure with unique names to prevent conflicting database entries.

If the BladeSystem servers are powered up before the rack name and enclosure name have been changed, then the names are recorded in the Deployment Server database and appear in the Deployment Server Console. If the names are changed after being recorded in the Deployment Server database, then the servers must be rebooted for the new rack name and enclosure name to be discovered. In addition, the original default rack names and the default enclosure names must be manually deleted from the console.

To change the rack name and enclosure name, follow the procedure specific to each server type:

- **ProLiant BL p-Class servers**—Place at least one server blade in each enclosure, and before powering up the server blade, change the rack and enclosure information using the Integrated Lights-Out (iLO) interface. For details about accessing iLO to change the rack name and enclosure name, see the documentation shipped with your server blade.
- **HP BladeSystem c-Class servers**—To access the Onboard Administrator and change the rack name and the enclosure name, see the server documentation.
Configuring image installs

**IMPORTANT:** By default, the Create Disk Image and Distribute Disk Image tasks operate on the first disk. The disks are enumerated using a proprietary algorithm. The first disk might not be the system boot disk. The Altiris showdisk utility can be used to generate human-readable disk enumeration output. This utility is called in the provided Read Hardware Configuration job. For more information on reading the showdisk output, see the Rapid Deployment Pack Knowledge Base at [http://www.hp.com/servers/rdp/kb](http://www.hp.com/servers/rdp/kb).

Configuring imaging jobs

When capturing or deploying an image to a server with multiple disks, either DAS or SAN, you might have to specify the system boot disk in the job.

To specify a particular disk:

1. In the Deployment Server Console, copy, rename, and then edit the job.
2. Modify the **Create Disk Image** or **Distribute Disk Image task**.
3. In the Additional Parameters box, add the -dx switch, where x is an integer that represents the appropriate disk number.

   When deploying Red Hat Enterprise Linux with LVM, x must be a comma-separated list of integers representing all of the disk numbers that the LVM volume will span. For example, to deploy an LVM image that spans the first three disks, use -d1, 2, 3.

Configuring Windows Sysprep jobs

In addition to the steps in the “Configuring imaging jobs” section, the Windows Sysprep jobs require a product key and cannot use the product keys entered during the Integration Module installation.

1. For each Capture Windows Sysprep Image job:
2. Select the **Create Disk Image** task.
3. Click **Modify**.
4. In the Sysprep settings box, select **Add new** from the Operating System list.
5. On the OS Product Key screen, select the appropriate operating system.
6. To enter a new product key, click **Add**.
7. Enter the product key in the Product Key box, and then click **OK>Finish**.
8. For each Deploy Windows Sysprep Image job:
9. Select the **Distribute Disk Image** task.
10. Click **Modify**.
11. In the Sysprep settings box, select the appropriate operating system from the Operating System list.
12. Select the appropriate product key from the Product key list, and then click **Finish**.
Configuring scripted installs

Configuring scripted install jobs

The scripted install jobs use a small image to partition and format the disk. When deploying to a server with multiple disks, either DAS or SAN, you might have to specify the system boot disk in the job for the NTFS.img or GRUB.img images. For more information, see the “Configuring image installs” section.

To specify a particular disk:

1. In the Deployment Server Console, copy, rename, and then edit the job.
2. Modify the Distribute Disk Image task.
3. In the Additional Parameters box, add the -dx switch, where x is an integer that represents the appropriate disk number.
4. Additionally, for Red Hat Linux in a multiple disk scenario, the kickstart file must specify the system boot disk.
5. On the Deployment Server, copy and then rename the kickstart file.
6. Modify the new kickstart file by replacing the autopart command with separate part command lines and adding the --ondisk=XXX option to each where XXX is the device label.

   Example for non-LVM:
   
   ```
   part /boot --size 75 --ondisk=cciss/c0d0
   part swap --size=1000 --ondisk=cciss/c0d0
   part / --size 5120 --grow --ondisk=cciss/c0d0
   ```

   Example for LVM:
   
   ```
   part /boot --size 100 --fstype=ext3 --ondisk=cciss/c0d0
   part pv.01 --size=100 --grow --ondisk=cciss/c0d0
   volgroup VolGroup00 --pesize=32768 pv.01
   ```

7. In the Deployment Server Console, copy, rename, and then edit the job.
8. Edit the Run Script – Create Boot Environment task in the new job to use the new kickstart file created in step 2.

Configuring SAN-attached scripted install jobs

1. In addition to the steps in the “Configuring scripted install jobs” section, other steps might be necessary.
2. For VMware ESX Server 3.0.x, Disconnect the SAN. After the operating system install is complete, reconnect the SAN and create a VMFS datastore on it.
3. For VMware ESX 2.5.3:
4. On the Deployment Server, copy, rename, and then edit the job.
5. Modify the Run Script – Create Boot Environment task in the new job by changing the default.cfg file reference in the # replacetokens statement to sanattach.cfg.
6. Execute the new job.
7. After the operating system installation is complete, using the MUI, create the core dump partition.
   a. When the following warning message appears:
      No core dump partition is configured or none is accessible, click Refigure.
   b. Select the LUN on which to place the core dump partition. The core dump partition cannot be
      created on the local ATA drive.
   c. Set the size of the core dump partition. VMware recommends 100 MB for each VMware ESX
      Server. The partition size defaults to all remaining available LUN space.

   a. Select Storage Management. Available storage volumes and available space appear. The VMFS
      cannot be created on a local ATA drive.
   b. Select Create Volume/Name.
   c. Select Typical or Custom. A typical volume allocates all remaining space to the VMFS.

Configuring Boot from SAN scripted install jobs

1. In addition to the steps in the “Configuring scripted install jobs” section, other steps might be
   necessary.

2. For VMware ESX Server 2.5.3:

3. On the Deployment Server, copy, rename, and edit the job.

4. Modify the Run Script – Create Boot Environment task in the new job by uncommenting the export
   bootfromsan=yes line.

Using the Rapid Deployment Pack

This section provides a walkthrough of the following topics:
- Connecting the server blades
- Creating a reference server and image
- Deploying the captured image to other similar servers
- Reconfiguring the new servers
- Maintaining the servers with rip-and-replace
- Performing a Boot from SAN installation

Although this example uses server blades, the process can be duplicated for other supported servers.
When performing an image capture and deployment, the hardware configuration of the target systems
must be identical to the hardware configuration of the reference server. Certain functionality is only
available for server blades, which is noted where applicable in the following sections.

This example assumes that all necessary installation, post-installation, and predeployment configuration
steps provided in this guide and the HP ProLiant Essentials Rapid Deployment Pack Installation Guide
have been performed.
Connecting the server blades

To connect the server blades as new servers to the Deployment Server:

1. Connect the enclosure to the network that contains your Deployment Server, and then power up the enclosure.

2. Insert the server blades into the enclosure, but do not power on the server blades.

3. Change the default rack and enclosure names.

4. Power up the server blades.

5. To view target servers available for deployment and management, open the Deployment Server Console. The following panes appear in the console:
   - Computers—This pane is located on the upper-left side of the console and displays, by default, New Computers and All Computers. Virtual Machines and Physical Devices also appear (if enabled).
   - Jobs—This pane is located on the lower-left side of the console and lists the jobs provided with the Rapid Deployment Pack.
   - Details—This pane is located on the right side of the console and displays details for the selections highlighted within the Computers pane or the Jobs pane.


**NOTE:** The Physical Devices view is an additional view available only for BladeSystem servers in the Computers pane. A job can be executed on a server listed in this view.

![Diagram of Computer and Physical Devices views](image)
Table 18 lists the server icons that appear in the Physical Devices view of the Deployment Server Console.

**Table 18** Server icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌟</td>
<td>Indicates a grouping of physical devices</td>
</tr>
<tr>
<td>🌟</td>
<td>Indicates a rack</td>
</tr>
<tr>
<td>🌟</td>
<td>Indicates an enclosure</td>
</tr>
<tr>
<td>🌟</td>
<td>Indicates a single server blade in a bay</td>
</tr>
<tr>
<td>🌟</td>
<td>Indicates an unconfigured server blade in a waiting state designated by the user</td>
</tr>
<tr>
<td>🌟</td>
<td>Indicates a virtual bay</td>
</tr>
</tbody>
</table>

7. From the Computers pane, right-click a server blade.
8. Select **Power Control>RILOE/iLO – Interface**. This action accesses the iLO, iLO 2, or RILOE interface to enable remote viewing of the deployment.
Creating a reference server and image

The initial server blade must be deployed using a scripted installation job. Subsequent server blades can be deployed by capturing and deploying the image of the initial server blade.

1. In the Jobs pane, select a Windows-scripted installation job in the Server Deployment folder. Drag the job onto the initial server blade in the Computers pane.

2. Select **Run this job immediately**, and then click **OK**.

**NOTE:** The Details pane displays the job currently running. Double-clicking the job in the Details pane shows the tasks and status.

**NOTE:** The Windows-scripted installations perform a token-replace of the computer name from the Deployment Server Console name. This computer name is truncated to the right-most 15 characters to comply with the NETBIOS limitation. The Linux- and VMware-scripted installs use the Deployment Server Console display name as the server host name.
3. In the Jobs pane, find the Read ProLiant ML/DL/BL System and Array Configuration and Windows Image (WinPE) job in the Server Replication folder. Drag the job onto the initial server blade in the Computers pane.

**NOTE:** The Server Replication jobs provided with the Rapid Deployment Pack create and deploy images using an image name based on the computer model names. If you use the provided jobs without modification, each time you capture a new image on the same computer model, the previous image is overwritten.

4. Select **Run this job immediately**, and then click **OK**.

5. If the scripted installation job is still running on the server, click **OK** when the warning message appears.
Deploying a captured image to other similar servers

1. In the Computers pane, select the rest of the server blades. Drag them onto the Write ProLiant ML/DL/BL System and Array Configuration and Windows Image (WinPE) job in the Server Replication folder in the Jobs pane.

If you are deploying the image to all server blades in an enclosure, you can select the enclosure from the Physical Devices view.

2. Select Run this job immediately, and then click OK.
Reconfiguring the new servers

1. In the Computers pane, select all the server blades, right-click the selection, and then select Configure.

2. Click Microsoft Networking, enter a new workgroup or domain name (if applicable), and then click Define Range.

3. Enter the fixed portion of the new server names, and then click OK.
4. Click **TCP/IP**, enter the IP information for the first server blade, and then click **OK**. Subsequent server blades are assigned the same information, except that the IP address increases incrementally for each server blade.

5. Select **Run this job immediately**, and then click **OK**.
Maintaining server blades with rip-and-replace

When a failed server blade is replaced, the Deployment Server can automatically replay the job history of the failed server blade on the new server blade. This feature is available only for BladeSystem servers.

**NOTE:** The new server blade requires a new license. The existing license cannot be transferred to the new server blade.

To enable rip-and-replace, perform the following steps for each server blade:

1. In the Computers pane, right-click a single server, and then select **Properties**.
2. Scroll down, and then click **Bay**.
3. Select **Re-Deploy Computer** from the Server change rule list, and then click **OK**.

The following server change rule options are available:

- **Re-Deploy Computer**—Takes the job history of the previous server blade and replays it on the new server blade. The replay starts from the last deployment type job. This option is available only after the server blade is deployed or a virtual bay has been created.
- **Run Predefined Job**—Processes any job specified by the user, including the Initial Deployment job.
- **Wait for User Interaction**—Performs no job. The Deployment Agent on the server blade is instructed to wait and the icon in the console is changed to reflect a waiting server.
- **Ignore the Change**—Ignores the new server blade, meaning that no jobs are initiated. If the new server blade existed in a previous bay, the history and parameters for the server are moved or associated with the new bay. If the server blade is not listed in the database, its properties are associated with the bay, and the normal process defined for new servers (if any) is followed.
Performing a Boot from SAN installation

A Boot from SAN (BFS) installation requires several manual steps before starting the operation system installation.

Be sure the following prerequisites are met:

- The target server is cabled in a single-path configuration (with only one channel active). You can cable both paths after the operating system is installed and the multipathing software is installed.
- Only one LUN is presented to the target server.
- Review HP StorageWorks Booting Windows Systems from a Storage Area Network Application Notes and HP StorageWorks Booting Linux Systems from a Storage Area Network Application Notes for details about SAN configuration and minimum firmware requirements.

1. Configure the SAN storage for the target server.
   a. Run the appropriate platform Read HBA Configuration job from the Server Deployment Toolbox \ Hardware Configuration \ HBA job folder on the target server. This job creates the .\lib\hwconfig\hba\ID.ini file, where ID is the target server computer ID. The following is an example of a generated file:

```
[HBA0]
WWID=500508b200713e72
HostAdapterBiosEnable=1
SelectBootEnable=1
BootDeviceWWID=
BootDeviceLUN=

[HBA1]
WWID=500508b200713e73
HostAdapterBiosEnable=0
SelectBootEnable=0
BootDeviceWWID=
BootDeviceLUN=
```

**NOTE:** To determine the target server computer ID, in the Computers pane, double-click the target server and read the ID field.

b. Create a LUN for the boot volume of the target server. Record the created LUN and the World Wide Identification (WWID) of the boot controller.

c. Using the target server HBA WWID from the file created in step 1a, configure the SAN switches for zoning or Selective Storage Presentation as needed in your environment.
2. Configure the target server HBA to boot from the configured SAN storage.
   a. Edit the ID.ini file created in step 1a, adding the previously recorded boot controller WWID and LUN. The boot volume must be set up as the first visible LUN. The following is an example of an edited file:

   ```
   [HBA0]
   WWID=500508b200713e72
   HostAdapterBiosEnable=1
   SelectBootEnable=1
   BootDeviceWWID=395442c135713a41
   BootDeviceLUN=01
   
   [HBA1]
   WWID=500508b200713e73
   HostAdapterBiosEnable=0
   SelectBootEnable=0
   BootDeviceWWID=395442c135713a42
   BootDeviceLUN=01
   ```
   b. Run the appropriate platform Write HBA Configuration job from the Server Deployment Toolbox—Hardware Configuration\HBA job folder on the target server.
   c. For ProLiant servers, run the **Deploy ProLiant BL System Configuration (Boot From SAN) {LinuxPE} or {WinPE}** job from the Server Deployment Toolbox—Hardware Configuration\System job folder on the target server. This job disables the embedded array controller and places the HBA controller first in the boot order.

3. Execute the appropriate operating system installation job from the Server Deployment Toolbox.

**Vulnerability scanning and deploying patches and fixes**

This section describes the setup and use of the Vulnerability and Patch Management Pack scanning functionality.

Vulnerability scanning is powered by technology from the PatchLink Corporation STAT Scanner. PatchLink Corporation is an international communications equipment company focused on providing mission-critical, assured communications for commercial and government customers.

PatchLink Corporation STAT network security solutions are backed by decades of expertise in information security. STAT vulnerability management products provide proactive protection of information and computer networks from hackers, viruses, worms, and other threats.

Vulnerability and Patch Management Pack enables you to:
- Enhance system lifecycle management by incorporating vulnerability assessment and patching as an integral part of the system management process
- Accelerate resolution of vulnerabilities by reducing the research time to understand the criticality of the vulnerability and the expected behavior for patches and fixes
- Reduce the risk of security threats by automating the acquisition, scheduling the deployment, and continuously enforcing the persistence (desired state) of patches
Built on industry-leading scanning (PathLink Security Threat Avoidance Technology) and patch management technology (HP OpenView using Radia), and integrated into HP SIM, Vulnerability and Patch Management Pack provide the following features:

- Combined vulnerability assessment and patch management—A single tool seamlessly combines the assessment and the remediation of vulnerabilities, reducing operational complexity that arises from managing separate tools for vulnerability assessment and patch management.

- Integration into HP SIM—This integration enables use of already existing functionality, such as discovery, identification, scheduling, role-based security, notification, and group-based actions, eliminating the need to recreate these tasks in multiple tools for vulnerability assessment and patch management.

- Comprehensive vulnerability assessment—Coverage of vulnerabilities reported in all leading vulnerability databases ensures comprehensive assessment. Powered by Harris Security Threat Avoidance Technology (STAT®) Scanner (the only Common Criteria Certified scanner), the vulnerability assessment identifies vulnerabilities reported in the Common Vulnerabilities and Exposures (CVE) list, the Federal Computer Incident Response Center (FedCIRC) vulnerability catalog, the SANS Top 20 Internet Security Vulnerabilities list, the Computer Emergency Response Team (CERT) advisories list, and the U.S. Department of Energy Computer Incident Advisories Center (CIAC) bulletins.

- Automated acquisition, scheduled deployment, and continuous enforcement of patches:
  - Automatically collects new vulnerability updates and patches directly from vendor sources, such as a vendor’s Web-based patch repository. Updates can be acquired outside the firewall and imported into the patch repository in infrastructures where firewall policies prevent HTTP and FTP downloads.
  - Schedulable deployment, schedulable reboots after deployment, and checkpoint-restarts ensure that patches are deployed with minimal impact on network resources and enable patches to be managed from a central point.
  - Unique desired-state management automatically and continuously ensures that patches remain applied in their proper state. If patches are corrupted in any way, they are automatically reinstalled to bring the system to the desired level of patches.
The following figure illustrates the process for using Vulnerability and Patch Management Pack.

For more information about Vulnerability and Patch Management Pack requirements, installation instructions, shared or distributed server environments, and Vulnerability and Patch Management Pack troubleshooting, see “Appendix B Vulnerability and Patch Management Pack additional information.”
The Vulnerability and Patch Management Pack interface

Vulnerability and Patch Management Pack vulnerability information appears in the VPM column of the HP SIM console, shown circled in the following figure. Initially, the icon depicted in the column displays Vulnerability and Patch Management Pack eligibility information for the target system in the specific row. After target servers are licensed and a vulnerability scan is performed, the column displays the combined status of the last vulnerability scan on the target system (patch status does not appear in the column). Click the icon to display detailed information about the system status of the Vulnerability and Patch Management Pack.

Table 19 Vulnerability and Patch Management Pack icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Risk assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>Critical vulnerabilities have been detected.</td>
<td>High</td>
</tr>
<tr>
<td>⚠</td>
<td>Major vulnerabilities have been detected.</td>
<td>Medium</td>
</tr>
<tr>
<td>!</td>
<td>Minor vulnerabilities have been detected.</td>
<td>Low and warning</td>
</tr>
<tr>
<td>✔</td>
<td>No vulnerabilities have been detected.</td>
<td>None</td>
</tr>
</tbody>
</table>

The Unknown icon might appear for the following reasons:

- Vulnerability and Patch Management Pack cannot access the system because proper authentication information was not provided.
- The system is either not supported or connected.
- Vulnerability and Patch Management Pack cannot access the system registry or file system.
Table 19  Vulnerability and Patch Management Pack icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Risk assessment</th>
</tr>
</thead>
</table>
| 📱  | This system is available for licensing, but Vulnerability and Patch Management Pack cannot run for the following reasons:  
- Vulnerability and Patch Management Pack is not installed.  
- The system is not licensed.  
- The system is licensed, but a scan has not yet been performed. | Unknown |
| No icon | Vulnerability and Patch Management Pack cannot be licensed on this system. | Unknown |

Click any status icon to display additional information for the system. Clicking the normal, minor, or major icons opens a new informational page where you can view the last scan results for the system. A new scan can also be launched from this page.

Clicking the Unknown icon for a system displays an explanatory page listing possible reasons why status is not available for the system and options to enable the Vulnerability and Patch Management Pack.

Provided scan definitions

Vulnerability and Patch Management Pack provides a large variety of scan definitions. You can use these definitions to search for vulnerabilities or modified to suit the specific needs of your environment. For specific information about the provided scan definitions, see “Appendix B Vulnerability and Patch Management Pack additional information.”

To use the provided scan definitions, see the “Scanning for vulnerabilities” section in this guide.

Scanning for vulnerabilities

To perform a vulnerability scan:

1. Select Diagnose>Vulnerability and Patch Management>Scan>Scan for Vulnerabilities.
2. Select the target systems to scan by selecting a group from the list or by selecting the individual system.
3. Click Apply.
4. Verify that the correct target systems appear in the lists. To reselect target systems, click Add Targets or Remove Targets, and then click Next.
5. If any selected systems are unlicensed or licensed with a time-limited license, permanent licenses can be applied at this time. If licenses are available, select any unlicensed system in the list to license, and then click Apply License. Server and client licenses are automatically applied to the appropriate systems, if available. To add licenses using a key string, click Add Key. Enter the key string in the box, and then click OK.

If systems listed as Unknown or Unmanaged in HP SIM are selected for licensing, a server license is assumed and automatically applied. HP recommends modifying the HP SIM settings to properly identify systems before licensing. Any unlicensed target systems not licensed at this time are not included in the patch agent deployment.

The license validation page does not appear if all target systems initially selected for the task are licensed with permanent licenses.
6. Click Next.
7. Enter a name for the vulnerability scan, and then select a scan definition from the list.
8. To run the vulnerability scan immediately, click Run Now. To schedule the scan to run later, select Schedule, and complete the following instructions:
   a. To schedule the vulnerability scan to run on a regular basis, select Periodically, or to run the scan one time, select Once.
   b. Designate a time and date to run the patch deployment task, and click Done.

Scans are run one system at a time in a serial process from the VPM server. You can view scan results after the task completes either by clicking the system status icon or viewing the VPM Events list.

Viewing, modifying, or canceling a scheduled task
1. Select Tasks & Logs>View All Scheduled Tasks.
2. Select the appropriate task from the list, and then click Edit.
3. Review the event details to modify. If necessary, you can change the target systems on which the task is scheduled to run by clicking either Add Targets or Remove Targets. Click Next.
4. Review the task schedule, and then modify as necessary. Click Done.

Viewing vulnerability scan results
Vulnerability and Patch Management Pack scan results are available for either a specified vulnerability scan or for an individual system. When a vulnerability scan is run for a group of target systems, results are generated for the group as well as for each individual system. You can view Vulnerability scan results as .pdf files of the following formats:
- Executive Summary—A high-level summary of all vulnerabilities found in a scan
- Detailed Listing—A list of vulnerabilities found on each system, as well as a description and risk evaluation of each
- Simple Listing—A list of vulnerabilities found on each system sorted by vulnerability name
- Scan Summary—A list of scans performed and vulnerabilities found, sorted by system name
- Ports and Services—A list of ports, services, and unknown services, sorted by system name

Vulnerability scan results guidelines
- You cannot view or delete vulnerability scan results when the scan status Scanning or Pending appears. If you abort the scan, the scan results might not be accurate.
- If the vulnerability scan results display the message No file access, verify that the WBEM settings in HP SIM have appropriate credentials listed for the target systems. For additional information, see the “Performing post-installation configuration tasks” section.
- You can also view scan results using the links in the completed scan event in HP SIM.
- Vulnerabilities listed are the total vulnerabilities found in the group of systems scanned. Individual systems in the group might not have every vulnerability listed.

Viewing vulnerability scan results by scan name
1. Select Diagnose>Vulnerability and Patch Management>Scan>View Results by Scan Name.
2. Select the appropriate vulnerability scan, select the format in which to view the results from the dropdown list, and then click View. The vulnerability scan results appear in a separate window.
Viewing scan results by system
1. Select Diagnose>Vulnerability and Patch Management>Scan>View Results by System.
2. Select the individual system for which you want to view scan results, and then click Apply.
3. Verify that the correct target systems appear in the lists. To reselect target systems, click Add Targets or Remove Targets, and then click Next.
4. Results for all scans performed on the selected system appear. Select the scan results you want to view, and then click View.

Customizing vulnerability scan definitions
You can create custom scans from the default system scans. Custom scans are updated automatically when the default system scans are updated.

To customize the provided vulnerability scans or previously created custom vulnerability scans:
1. Select Diagnose>Vulnerability and Patch Management>Customize Scan.
2. Select a default system scan or a previously created custom scan to modify, and then click Edit. A list of vulnerabilities appears. Clicking the entry in either the Vulnerability ID or Advisory column displays additional information about the vulnerability.
3. Select one or more vulnerabilities to include in the custom scan definition.
4. Enter a name and description for the new customized scan, and then click Save.
5. You must rename the customized vulnerability scan. You cannot save a modified default Vulnerability and Patch Management Pack scan using the original scan name. To use a customized vulnerability scan, see the “Scanning for vulnerabilities” section in this guide.

Deleting a customized vulnerability scan
Only custom vulnerability scans can be deleted. Default system scans provided with the Vulnerability and Patch Management Pack cannot be deleted.

To delete a custom vulnerability scan:
1. Select Diagnose>Vulnerability and Patch Management>Scan>Customize Scan.
2. Select the custom vulnerability scan to delete, and then click Delete.
3. When prompted to confirm the deletion, click OK.

Deleting vulnerability scan results
Vulnerability and Patch Management Pack scan results can be deleted for a specified scan or for an individual system. Removing results breaks the links to the results in the events and the system list. Run another scan to create new results for the system.

Deleting scan results by scan name
1. Select Diagnose>Vulnerability and Patch Management>Scan>View Results by Scan Name.
2. Select the appropriate scan or scans, and then click Delete. All results associated with the selected scan are deleted.
Deleting scan results by system

1. Select Diagnose>Vulnerability and Patch Management>Scan>View Results by System.
2. Select the individual system for which to delete results, and then click Apply.
3. Verify that the correct target systems appear in the lists. To reselect target systems, click Add Targets or Remove Targets, and then click Next.
4. Results from all scans performed on the selected system appear. Select the scan results to delete, and then click Delete.

Deploying patches and fixes

Patches and configuration fixes can be deployed immediately or scheduled for deployment later. Patches can be selected individually from the database for deployment to all systems or any combination of specified systems without performing a scan, or patches and fixes can be deployed for all vulnerabilities identified in a particular scan.

Patches come from the software vendor and can be updated to existing software, registry, or configuration settings or files. Configuration fixes resolve incorrect system settings that can leave the system open to security threats, such as open ports or services running that are not required.

Some vulnerability issues found cannot be automatically fixed or patched. Scan results often provide a suggested fix that must be manually performed.

Important information about patches and fixes

- Target systems are rebooted if required by the installed or removed patch, based on the reboot information obtained from the original patch source. Reboot information might occasionally inaccurately indicate that a patch installation requires a reboot.
- If multiple patches requiring reboots are applied, target systems are only rebooted once after all patches are applied. Required reboots can be deferred and performed later. HP recommends performing required reboots as soon as possible, because the status of patched systems might be unstable when a required reboot is deferred.
- To determine patch applicability, the Vulnerability and Patch Management Pack can enhance patch detection criteria to be more precise than vendor information. These patches appear with an asterisk in the Patch Source column. HP does not modify the patch.
- Risk and Vulnerability ID information might not appear because this information was not available at the time the patch was acquired. The information appears when the vulnerability database is updated to include this information.
- By default, patches are sorted by the latest release date. Select a column heading to resort patches.
- Target systems that are down during a scheduled patch application are patched when the system is brought online.
Deploying patches and fixes based on a vulnerability scan

After a vulnerability scan indicates that security vulnerabilities or configuration errors exist, perform the steps in the following sections to deploy patches, configuration fixes, or both.

Vulnerabilities that require manual fixes (those for which the patch has not been acquired) are listed but are not available for selection.

To deploy patches, configuration fixes, or both to systems based on a specific vulnerability scan:

1. Select **Deploy>Vulnerability and Patch Management>Patch-Fix Based on a Scan**.
2. Select the completed vulnerability scan, and then click **Next**.
   
   Vulnerabilities appear for all systems included in the scan. All vulnerabilities listed might not be applicable for every system. Clicking the listing in the Vulnerability ID or Advisory column displays additional information about the vulnerability. The Requires Reboot column indicates if the patch requires the system to reboot after deployment.

3. Select the vulnerabilities to patch or fix, and then click **Next**.

4. Select the systems on which to apply patches or fixes, and then click **Next**.

5. Designate when the patched systems are rebooted. Reboots can be performed immediately after the patches or fixes are installed or can be postponed. The local user can also accept or reject the reboot. If the local user rejects the reboot, then another automatic reminder does not appear.
6. To deploy patches or fixes immediately, click **Run Now**.

7. To schedule the patch or fix deployment:
   a. Click **Schedule**.
   b. Enter an appropriate name for the task, or accept the default name, and then select **Once**.
   c. Designate a time and date to run the task, and then click **Done**.

8. View task results in the VPM Events list after the task is completed.

   To view the list of target systems that require reboot, see the “Viewing the patch reboot status” section in this guide.
Deploying patches without a vulnerability scan

If a patch is released that must be deployed immediately, the patch can be applied without running a scan. In normal circumstances, HP recommends running a scan before deploying patches. If the VPM Patch Agent is removed from a system for any reason or is not properly deployed to the target system, complete the following instructions to deploy the VPM Patch Agent.

To deploy patches, configuration fixes, or both to systems based on a specific vulnerability scan:

1. Select Deploy>Vulnerability and Patch Management>Patch-Fix Based on a Scan.
2. Select the completed vulnerability scan, and then click Next. Vulnerabilities appear for all systems included in the scan.
3. All vulnerabilities listed might not be applicable for every system. Clicking the entry in the Vulnerability ID or Advisory column displays additional information about the vulnerability. The Requires Reboot column indicates if the patch requires the system to reboot after deployment.
4. Select the vulnerabilities to patch or fix, and then click Next.
5. Select the systems on which to apply patches or fixes, and then click Next.
6. Designate a time to reboot the patched systems. You can reboot systems immediately after the patches or fixes are installed or postpone the reboot until later. Also, you can give the local user the option to accept or reject the reboot. If the local user rejects the reboot, no additional automatic reminder appears.
7. To deploy patches immediately, click Run Now. To schedule the patch deployment, click Schedule and then complete the following instructions:
   a. Enter an appropriate name for the deployment task or accept the default name, and select Once.
   b. Designate a time and date to run the task, and then click Done.

To view the list of target systems that require reboot, see the “Viewing the patch reboot status” section in this guide.

Viewing the patch repository

1. Select Diagnose>Vulnerability and Patch Management>View Patch Repository.
2. To filter the list of displayed patches that appear, select the appropriate patch source from the list. To view information about a specific patch, click the patch identification number in the Advisory or Vulnerability ID column.

Viewing the patch reboot status

Certain patches require that the server be rebooted after installation. During patch deployment, the option can be selected to reboot the server later. The patch deployment is not complete until the server has rebooted.

To view the patch status and initiate reboots for selected systems:

1. Select Diagnose>Vulnerability and Patch Management>View Patch Reboot Status.
2. Select the target systems for which you want to view the reboot status by selecting a group from the list or by selecting the individual system.
3. Click **Apply**.

4. Verify that the correct target systems appear in the lists. To reselect target systems, click **Add Targets** or **Remove Targets**, and then click **Next**. The patch reboot status for the selected systems appears in the Reboot Status column.

5. Select the systems to reboot, and the local user of all the listed systems is given the option to accept or reject the reboot. If the local user rejects the reboot, then another automatic reminder does not appear. The Reboot Status column does not indicate that reboots are required for systems until after the patch deployment task is complete. If the local user rejects the reboot, no additional automatic reminders appear.
6. To reboot the selected systems immediately, click Run Now. To schedule the reboot, click Schedule.

7. To schedule the reboot task:
   a. Enter an appropriate name for the reboot task, or accept the default name, and then select Once.
   b. Designate a time and date to run the reboot task, and then click Done.

Validating installed patches

Patch validation identifies any missing patches on target systems and immediately reinstall them, creating a patch deployment event in HP SIM. If a VPM Patch Agent update has been acquired, the update is also automatically applied. If reinstalled patches require selected target systems to be rebooted, this action is automatically deferred. The reboot status can be viewed after a validation task has completed by selecting Diagnose>Vulnerability and Patch Management>View Patch Reboot Status.

Schedule a task to periodically verify that deployed patches are still installed on the target systems. Scheduling the task determines how often the VPM Patch Agent performs the verification.

1. Select Deploy>Vulnerability and Patch Management>Validate Installed Patches.
2. Select the target systems for which to validate installed patches by selecting a group from the list or selecting the individual system.
3. Click Apply.
4. Verify that the correct target systems appear in the lists. To reselect target systems, click Add Targets or Remove Targets, and then click Next.
5. Enter an appropriate name for the validation task or accept the default name.
6. To validate the installed patches immediately, select Run now, and then click Done. To schedule the validation task, choose one of the following:
   ○ To run on a regular basis, select Periodically, designate a time and date, and then click Done.
   ○ To run the task one time, select Once, designate a time and date, and then click Done.

You can schedule multiple patch validation tasks at different frequencies for groups of target systems. You can view task results in the VPM Events list after the task completes.
Deploying the VPM Patch Agent

The VPM Patch Agent automatically deploys when target systems are licensed to allow patches to be applied to the systems. If the VPM Patch Agent deployment fails, verify that the WBEM credentials are configured correctly. To verify the WBEM credentials, select Options>Protocol Settings>System Protocol Settings.

To deploy the VPM Patch Agent to systems to enable patching:

1. Select Deploy>Vulnerability and Patch Management>VPM Patch Agent.
2. Select the target systems on which to deploy the VPM Patch Agent by selecting a group from the list or by selecting the individual system.
3. Click Apply.
4. Verify that the correct target systems appear in the lists. To reselect target systems, click Add Targets or Remove Targets, and then click Next.
   If any selected systems are unlicensed or licensed with a time-limited license, permanent licenses can be applied at this time.
5. If licenses are available, select any unlicensed system in the list to license, and then click Apply License. Server and client licenses are automatically applied to the appropriate systems, if available. To add licenses using a key string, click Add Key. Enter the key string in the box, and then click OK.
6. The license validation page does not appear if all target systems initially selected for the task are licensed with permanent licenses.
   If systems listed as Unknown or Unmanaged in HP SIM are selected for licensing, a server license is assumed and automatically applied. HP recommends modifying the HP SIM settings to properly identify systems before licensing.
   Any unlicensed systems are not included in the VPM Patch Agent deployment.

   **NOTE:** If one or more target systems can use a VPM client license, but an adequate client license is not available, you are prompted to select whether to apply a server license (if available) to license the selected client systems. After a server license has been applied, it cannot be revoked or replaced with a VPM client license later.

   If all target systems initially selected for the task have permanent licenses, the license validation page does not appear.

7. Click Next.
8. If the server type is identified as Unknown or Unmanaged with no identified operating system in the HP SIM console, select the appropriate operating system. Click **Next**.

9. To deploy the VPM Patch Agent immediately, select **Run now**, and then click **Done**.

   To schedule the agent deployment, select **Once**, designate the appropriate date and time, and then click **Done**.

   You cannot apply patches to the systems until after the scheduled task completes and the VPM Patch Agent is applied successfully.

   View task results in the VPM Events list after the task is completed.

**Removing patches**

Only patches that can be removed appear on the patch removal page. Only Microsoft patches including vendor-provided uninstallation capability can be removed, provided these patches were installed by Vulnerability and Patch Management Pack. Vulnerability and Patch Management Pack cannot remove configuration fixes or Red Hat patches. Vulnerability and Patch Management Pack does not perform dependency checking before removing patches. HP recommends extreme care when removing patches.

To remove patches after they have been applied to systems:

1. Select **Deploy>Vulnerability and Patch Management>Remove Patch**.
2. Select the patches to remove, and then click **Next**.
   Certain patches might require a manual reboot of the target system to completely remove the patch.

3. Select the systems on which to remove the designated patches.
4. To remove the patches immediately, click **Run Now**. To schedule the patch removal, click **Schedule**.
5. If scheduling the patch removal task:
   a. Enter an appropriate name for the removal task or accept the default name, and then select **Once**.
   b. Designate a time and date to run the removal task, and then click **Done**.

6. View task results in the VPM Events list after the task completes.
   
   If the patch removal requires the target system to be rebooted, this reboot action is automatically deferred. The reboot status can be viewed after a patch removal task has completed by selecting **Diagnose > Vulnerability and Patch Management > View Patch Reboot Status**.

**Vulnerability and Patch Management Pack events**

Vulnerability and Patch Management Pack creates events in HP SIM. These events can be viewed with all HP SIM events in the Events list, or independently in the VPM Events list. For a complete listing of events see “Appendix B Vulnerability and Patch Management Pack additional information.”
This chapter provides an overview of server virtualization and consolidation using the Virtual Machine Management Pack component of Insight Control Management. This component might be installed as part of an Insight Control Management suite installation, but is licensed separately.

Virtual Machine Management Pack

The Virtual Machine Management Pack provides tracking, monitoring, and control functions for organizing an effective virtualized environment. HP leverages key industry alliances to provide best-in-class management capability across most contemporary virtualization software platforms and industry-standard servers.

The Virtual Machine Management Pack provides central management and control for virtual machines with Microsoft Virtual Server 2005, VMware Server, VMware GSX Server, or VMware ESX Server. The Virtual Machine Management Pack is fully integrated with HP SIM.

The Virtual Machine Management Pack also detects virtual machine status changes initiated by other supported virtualization technology consoles. These status changes are indicated by the System Status icons on the HP SIM System Page. To access the System Page, click an icon in the VM column for a virtual machine host or guest in the HP SIM console.

- If Microsoft Virtual Server is used, the Launch SCVMM button appears.
- If VMware ESX Server is used, the Launch VC button appears.

The left frame of the HP SIM console displays a node navigational tree. A list of the virtual machine hosts and their virtual machine guests appears in the Systems>Shared>Systems by Type directory.
To display all virtual machine hosts and guests managed by the Virtual Machine Management Pack in the HP SIM console, expand the Systems>Shared>Systems by Type directory in the navigational tree, and then click All Virtual Machine Hosts or All Virtual Machines.

Virtual machine host

Depending on the host configuration, additional details might appear. Click a virtual machine host in the HP SIM console, and then to display the following information for the host, click the System tab.

- If Microsoft Virtual Server is used, the Launch SCVMM button appears.
- If VMware ESX Server is used, the Launch VC button appears.

- System status—The health and virtual machine status represented by color-coded icons.
- Identification—The address, preferred system name, and network name.
- Product Description
  - System type—The type of system on which the software is running
  - System subtype—A virtual machine host or guest
  - Hardware description—Details of the physical system on which the software is running
  - OS name—The operating system used
  - OS for tool filtering—The type of operating system being used for filtering
  - OS description—The level of operating system being used
  - OS version—The version of the operating system
  - Management protocols—The protocols being used for tool filtering

- Virtual Machine Host Configuration Details
  - Virtualization—The type of virtualization software installed (This detail also links to the remote console.)
  - Performance alert—The threshold values set by the user. For example, when over 44% CPU utilization for more than 55 minutes
  - Storage details—The disk space information
• Virtual machines—A list of virtual machines associated with the virtual machine host
  ○ Status—The status of the virtual machine
  ○ State—The state of the virtual machine
  ○ VM name—The name of the virtual machine
  ○ System IP address—The IP address of the virtual machine
  ○ Legend—To display the VMM Status Icon Legend window, which displays the icons and their definitions, click **Legend**.
  ○ VM control—Virtual machine status is listed, and the controls enable you to launch the Remote Desktop and the Remote Console, as well as start, stop, reset, and pause the virtual machine.
• Disk partitions—A list of how the disk is separated, its capacity, and percentages of used and available space
• VirtualCenter information—Details about the VirtualCenter, such as IP address of the host system and virtual machines associated with the VirtualCenter
• Associations—A list of associations as created by HP SIM

**Virtual machine guest**

Depending on the guest configuration, additional details might appear. Click a virtual machine guest in the HP SIM console, and then to display the following configuration information for the host or guest. Information appears only for virtual machine guests that are fully configured, click the **System** tab.

- If Microsoft Virtual Server is used, the Launch SCVMM button appears.
- If VMware ESX Server is used, the Launch VC button appears.

- System status—The health and virtual machine status is represented by color-coded icons.
- Identification—The address, preferred system name, and network name
- Product Description
  ○ System type—The type of system on which the software is running
  ○ System subtype—A virtual machine host or guest
  ○ Hardware description—Details of the physical system on which the software is running
  ○ OS name—The operating system being used
  ○ OS for tool filtering—The type of operating system being used for filtering
• OS description—The level of operating system being used
• OS version—The version of the operating system
• Management protocols—The protocols being used for tool filtering

• Virtual machine controls—Virtual machine status is listed, and the controls enable you to launch the Remote Desktop and Remote Console, as well as start, stop, reset, and pause virtual machines. For detailed status legend information, click Legend.

• Virtual machine configuration details
  • Virtual machine host—The system name of the virtual machine host
  • Virtualization—The virtualization technology installed on the virtual machine host
  • Alternate host—The failover host set by the user
  • Configuration file—The name and location of the configuration file
  • Configuration folder—The name and location of the configuration folder
  • Memory—The amount of memory on the virtual machine host
  • Virtual NIC—The type of network card and MAC address
  • Virtual disk—The type of virtual disk
  • CD/DVD RM—Details about the drive
  • Floppy drive—Identity of the floppy drive

• Virtual machine backups—Information about the backups for the virtual machine
  • Source host—The host source name
  • Source path—The source path
  • Configuration file—The configuration file name
  • Virtualization layer—The virtualization layer
  • Backup repository—The backup repository information
  • Backup repository location—The location of the backup repository
  • Date—The date of the last backup

• Virtual machine disk partition—A list of virtual machines controlled by the host
  • Disk name—The name of the disk
  • Partition—The partition on the drive where the disk is found
  • Capacity—The capacity of the disk
  • %Used—The percentage of disk space used
  • Format—The format type of the disk
  • Type—The type of disk used

• VirtualCenter information—Details about the VirtualCenter, such as IP address of the host system and virtual machines associated with the VirtualCenter

• Backup details—Details about the most recent backup of the virtual machine, such as source host IP address, source path, configuration file, virtualization layer, and backup repository.

To view completed events involving the selected host or guest, click the Events tab. For more information, see the HP ProLiant Essentials Virtual Machine Management Pack User Guide.
Configured and unconfigured virtual machine guests

Configured and unconfigured virtual machine guests can appear in HP SIM CMS and have the following attributes.

Configured

Configured virtual machines meet at least one of the following criteria:

- Proper providers are installed, and the credentials are saved in HP SIM.
- HP SIM can discover and identify the guest operating system running inside the virtual machine host along with the virtual machine serial number.
- Proper virtual machine host to virtual machine guest association appears.
- Full Virtual Machine Management Pack functionality is available.
- Turning off the virtual machine host does not change its status as a configured virtual machine.
- If the virtual machine host is deleted using the HP SIM interface, the virtual machine host becomes unconfigured until it is rediscovered by HP SIM.

Unconfigured

Unconfigured virtual machines meet at least one of the following criteria:

- Have never been turned on
- Have no guest operating system installed
- Do not have proper providers installed
- Have credentials unknown to HP SIM

Unconfigured virtual machines have the following limitations:

- They are not HP SIM manageable.
- Permissions cannot be assigned to them.
- Schedules cannot be defined.
- Tools such as creating virtual machine backups, setting performance alerts, setting failover host, or moving virtual machines are limited.

Unconfigured virtual machines can create templates.

Task execution process

Multiple Virtual Machine Management Pack tasks involving separate virtual machine hosts or virtual machines can be performed simultaneously, but they take longer to execute than if only one task is running.

Multiple Virtual Machine Management Pack tasks involving the same virtual machine host or virtual machine guest that are queued at the same time are executed sequentially. One Virtual Machine Management Pack read function and one write function can be performed for each virtual machine host simultaneously. Any additional functions are queued.
Using the Virtual Machine Management Pack tools and controls

Various tasks can be performed using the Virtual Machine Management Pack controls, available from the HP SIM host or virtual machine System Page, as described in the following sections. You must have administrative rights to perform Virtual Machine Management Pack tasks.

The time to complete a virtual machine operation that involves file transfers takes longer when Network Attached Storage (NAS) volumes are used because the Virtual Machine Management Pack shares a network connection with NAS. Be sure separate networks are set up for the Virtual Machine Management Pack and NAS.

The following Virtual Machine Management Pack tasks appear on the HP SIM host or guest System Page. By using these tasks, licensed virtual machine guests can be started, resumed, shut down, stopped, paused, reset, and restarted.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔊</td>
<td>Start/resume</td>
</tr>
<tr>
<td>🔴</td>
<td>Shutdown/stop</td>
</tr>
<tr>
<td>⏯</td>
<td>Pause</td>
</tr>
<tr>
<td>🔄</td>
<td>Reset/restart</td>
</tr>
</tbody>
</table>

In addition, the following tasks can be initiated from the HP SIM toolbar:

- Starting or resuming virtual machine guests
- Shutting down or stopping virtual machine guests
- Suspending virtual machine guests
- Resetting or restarting virtual machine guests
- Copying virtual machine guests
- Moving virtual machine guests
- Creating virtual machine guest templates
- Deploying virtual machine guest templates
- Creating virtual machine guest backups
- Restoring virtual machine guest backups
- Restoring the last virtual machine guest backup
- Recovering virtual machines of a failed host on a VMware ESX Server
- Setting alternate virtual machine hosts on a VMware ESX Server
- Removing alternate virtual machine hosts on a VMware ESX Server
- Launching remote access
- Launching the Remote Console
- Launching the Remote Desktop
- Launching VNC
- Restarting the VMM Agent
- Setting or removing the performance threshold
- Registering virtual machine hosts
- Unregistering virtual machine hosts
Starting or resuming virtual machine guests

A virtual machine guest can only be started or resumed if it is currently stopped, shut down, or paused.

To start or resume a virtual machine guest:
1. In the HP SIM All Systems page, select the virtual machine guests to be started.
2. From the HP SIM toolbar, select Deploy>Virtual Machine>Start Virtual Machine.
3. Verify the target system, and then click Next. Virtual machine source information appears.
4. Verify the details, and then click Schedule or Run Now.

To start or resume a virtual machine guest from the virtual machine host or guest System Page:
1. Click the Start/Resume icon (■).
2. Verify the target system, and then click OK when prompted.

If the virtual machine guest is stopped or paused, you can start or resume the guest by clicking the Start/Resume icon. If the virtual machine guest is currently suspended to disk (only possible with Microsoft Virtual Server 2005), then to restore the virtual machine guest to the previous state and power up the virtual machine guest, select Resume Virtual Machine Guest.

When the power-up process is complete, the status is updated to Normal (□). The Start icon is disabled, and the Shutdown/Stop, Pause, and Reset icons are enabled.

If a virtual machine guest does not respond during the start process, the Virtual Machine Management Pack displays User Interaction, and the status is updated to Major (▼).

Shutting down or stopping virtual machine guests

A virtual machine guest can only be shut down if it is currently powered up and either the Microsoft Virtual Server Additions or the VMware Tools are installed on the virtual machine guest.

For Microsoft Virtual Server 2005 virtual machine guests, select Stop VM or Shutdown VM when prompted. When you select Stop VM, the virtual machine guest powers down immediately without saving the current state. When you select Shut down VM, the virtual machine operating system shuts down, and then the virtual machine guest powers down.

To shut down or stop a virtual machine guest:
1. In the HP SIM All Systems page, select the virtual machine guests to be shut down.
2. From the HP SIM toolbar, select Deploy>Virtual Machine>Shutdown Virtual Machine.
3. Verify the target system, and then click Next. Virtual machine source information appears.
4. Verify the details, and then click Schedule or Run Now.
To shut down or stop a virtual machine guest from the virtual machine host or guest System Page:

⚠️ **CAUTION:** If you select Stop VM, unsaved data is lost.

1. Click the **Shutdown/Stop** icon (ıp).
2. Verify the target system, and then click **OK** when prompted.

When the shutdown or stop process is complete, the status is updated to Disabled (-disabled). The Stop, Pause, and Reset icons are disabled, and the Start icon is enabled.

**Suspending virtual machine guests**

A virtual machine guest can only be suspended if it is currently powered up and running.

For Microsoft Virtual Server 2005 virtual machine guests, select **Suspend to disk** or **Pause VM** when prompted. When you select Suspend to disk, the current state is saved and the virtual machine host memory used by the virtual machine is released. When you select Pause VM, the virtual machine execution is suspended but the virtual machine state in the virtual machine host memory is retained.

To suspend a virtual machine guest:

1. In the HP SIM All Systems page, select the virtual machine guests to be suspended or paused.
2. From the HP SIM toolbar, select **Deploy>Virtual Machine>Suspend Virtual Machine**.
3. Verify the target system, and click **Next**. Virtual machine source information appears.
4. Verify the details, and then click **Schedule** or **Run Now**.

To suspend a virtual machine guest from the virtual machine host or guest System Page:

1. Click the **Pause** icon (ıp).
2. Verify the target system, and then click **OK** when prompted.

When the suspend-to-disk or pause process is complete, the status is updated to Disabled (-disabled). The Stop, Pause, and Reset icons are disabled, and the Start icon is enabled.

**Resetting or restarting virtual machine guests**

For Microsoft Virtual Server 2005 virtual machine guests, select **Reset** or **Restart** when prompted. When you select Reset, the virtual machine guest powers down, and then powers up. When you select Restart, the virtual machine operating system shuts down and powers down, and then the virtual machine guest powers up.

To reset or restart a virtual machine guest:

1. In the HP SIM All Systems page, select the virtual machine guests to be reset.
2. From the HP SIM toolbar, select **Deploy>Virtual Machine>Reset Virtual Machine**.
3. Verify the target system, and then click **Next**. Virtual machine source information appears.
4. Verify the details, and then click **Schedule** or **Run Now**.
To reset or restart a virtual machine guest from the virtual machine host or guest System Page:

⚠️ **CAUTION:** If you select **Reset**, unsaved data is lost.

1. Click the **Reset/Restart** icon (🔥).
2. Verify the target system, and click **OK** when prompted.

When the reset or restart process is complete, the status is updated to **Normal** (✅). The **Start** icon is disabled, and the **Shutdown/Stop**, **Pause**, and **Reset** icons are enabled.

### Copying virtual machine guests

A virtual machine guest must be stopped or paused before it can be copied.

You can copy virtual machine guests from an existing virtual machine host to a new host when the same virtualization technology exists on both the source and target host servers.

1. Before you can copy a virtual machine guest, you must stop or pause it.
2. In the HP SIM All Systems page, select the virtual machine guests to be copied.
3. From the HP SIM toolbar, select **Deploy>Virtual Machine>Copy Virtual Machine**.
4. Verify the target system, and then click **Next**. Virtual machine source information appears.
5. Select the target virtual machine host from the list of authorized licensed hosts, and click **Next**.
6. Review the resources of all available hosts, select the target virtual machine host, and then click **Next**.
7. Specify a name for the target virtual machine guest being copied, or accept the default selection, and then specify the target path for the virtual machine guest and disk. The target folder on the virtual machine host must be empty.

   Microsoft requires that each virtual machine guest have a unique virtual machine name. If virtual machine disks or configuration files already exist with the designated name, an error occurs and the copy operation fails.

8. Verify that adequate available disk space exists on the target virtual machine host to accommodate the total transport volume, which consists of several disks and configuration files.
9. Click **Next**.
10. Verify the details of the copy operation that appear, and then click **Confirm**.

When the copy is complete, the new virtual machine guest is registered to the target virtual machine host. The virtual machine guest status is **Disabled** (🚫). Start the copied virtual machine guest using the Virtual Machine Management Pack as necessary and discover it in HP SIM.

You might need to manually reconfigure the virtual network connections on the new virtual machine guest. You might need to change the host name of the copied virtual machine guest.
Moving virtual machine guests

You can move VMware ESX Server using the following options:

- **Move**—The virtual disk is copied to the host. You must stop the virtual machine for this move operation type.
- **SAN Move**—The virtual disk is not copied to the target host. The target host accesses the virtual disks using storage area network (SAN) connectivity. The virtual machine must be stopped for this move operation type.
- **Live Move**—The powered-up virtual machine is moved using VMware VMotion Technology.

You must stop the Microsoft Virtual Server 2005, VMware GSX Server, or VMware Server virtual machine guest before moving them. If the virtual machine being moved is already part of the VirtualCenter cluster, a warning message appears.

To move a virtual machine guest:

1. In the HP SIM All Systems page, select the virtual machine guest to be moved.
2. From the HP SIM toolbar, select **Deploy>Virtual Machine>Move Virtual Machine.**
3. Verify the source virtual machine, and then click **Next.**
4. Select the target virtual machine host from the list of authorized licensed hosts, and then click **Next.**
   - If the selected virtual machine is associated with a VMware ESX Server and:
     - The virtual machine is currently running, a Live Move for VMware ESX Server using VMware VMotion Technology is performed.
     - The virtual machine is stopped, SAN Move or Move appears in the Move Type column. If the target host is in a SAN, a SAN Move can be performed.
   - To perform a Live Move, you must configure VMware VirtualCenter settings. For more information, see the *HP ProLiant Essentials Virtual Machine Management Pack User Guide.*
5. Specify a name for the target virtual machine guest being moved or accept the default selection, and specify the target path for the virtual machine guest and the disk. The target folder on the virtual machine host must be empty.
   - Microsoft requires that each virtual machine guest have a unique virtual machine name. If virtual machine disks or configuration files already exist with the designated name, an error occurs and the move operation fails.
6. Verify that adequate available disk space exists on the target virtual machine host to accommodate the total transport volume, which consists of several disks and configuration files.
7. Click **Next.**
8. Verify the details of the move operation that appears, and then click **Run Now.**

When the move is complete, the new virtual machine guest is registered to the target virtual machine host. The virtual machine guest status is Disabled (-disabled). Start the moved virtual machine guest using the Virtual Machine Management Pack as necessary, and discover it in HP SIM.

The Virtual Machine Management Pack does not delete virtual machine guest files after a move. For errors that might occur after performing a move or SAN move, see the *HP ProLiant Essentials Virtual Machine Management Pack User Guide.* For errors that might occur after performing a Live Move, see the *HP ProLiant Essentials Virtual Machine Management Pack User Guide.*

You might need to manually reconfigure the virtual network connections on the moved virtual machine guest.
Creating virtual machine guest templates

Before you can create a template, you must stop or pause a virtual machine guest. You must have administrative rights to create a template.

A template is an image of a complete virtual machine guest, including the operating system, configuration, and all relevant virtual machine disk information needed to create and register a new virtual machine on a host with the same virtualization technology. Any existing virtual machine guest on a licensed host can be used to create a template. The Create Virtual Machine Template screen enables you to view all available templates.

A template does not contain the serial number (UUID) and MAC address of the virtual machine guest used to create the template.

1. From the HP SIM toolbar, select Deploy>Virtual Machine>Templates> Create Virtual Machine Template.
2. Verify all the virtual machines in the Licensed Hosts section appear. Select Powered off VM, and then click Next.
3. Review the resources of the available hosts, select an appropriate target virtual machine host where the template is to be stored, and then click Next.
4. Enter a name for the template or accept the default selection, and then enter an optional description. Click Next. A list of licensed virtual machine hosts appears.
5. Select which disks you want to include in the template. You must select the operating system and boot disks.
6. Specify the target path for the virtual machine template, and then click Next. The target folder on the virtual machine host must be empty.
7. Click Next.
8. Verify the details of the operation that appear, and then to create the template now, click Run Now, or to create the template later, click Schedule.

Deploying virtual machine guest templates

The Virtual Machine Management Pack enables you to deploy a previously created virtual machine template to create a new virtual machine guest. A virtual machine template is an image of a complete virtual machine operating system, configuration, and all relevant virtual disk information. The template is needed to create and register a virtual machine on a virtual machine host with the same virtualization technology.

A template does not contain the serial number (UUID) and MAC address of the virtual machine guest used to create the template.

1. From the HP SIM toolbar, select Deploy>Virtual Machine>Templates> Deploy Virtual Machine Template.
2. Select a template from the list of available templates, and then click Next.
3. Select the target virtual machine host where the template is to be deployed, and then click Next.
4. Select the target virtual machine host directory location.
5. Specify the name of the virtual machine guest, memory size, and target file as necessary, and then click Next. The target folder must be empty.
6. Verify the details.
7. To deploy the template now, click Run Now, or to deploy the template later, click Schedule.
Creating virtual machine guest backups

Performing a backup requires administrative rights. If you perform a backup on a virtual machine guest that is currently running, the guest is automatically suspended and then restarted after the backup is complete.

Virtual Machine Management Pack enables you to perform an immediate backup of a virtual machine guest, schedule a single backup, or schedule a recurring backup on a daily or weekly basis. The Create Virtual Machine Backup screen enables you to view and delete all available backups.

1. In the HP SIM All Systems page, select the virtual machine guest to backup.
2. From the HP SIM toolbar, select Deploy>Virtual Machine>Backups>Create Virtual Machine Backup.
3. Verify the target system, and then click Next.
4. Verify the source virtual machine details, and then review the resources of the available virtual machine hosts.
5. Verify that adequate available disk space exists on the target virtual machine host to accommodate the total transport volume, which consists of several disks and configuration file.
6. Select the host to be used as the backup repository, and then click Next.
7. Select the target repository, and then click Next.
   The target repository must be on the same virtualization layer.
8. Specify where the backup files are to be placed on the virtual machine host, and then click Next.
   ○ For a VMware GSX Server, VMware Server, or Microsoft Virtual Server 2005 virtual machine, if the virtual machine is powered up, then the guest is suspended for the duration of the backup and resumed after the backup is completed. By default, the backup data is compressed.
   ○ For a VMware ESX Server virtual machine that is powered up, select one of the following:
     - Perform the backup while the virtual machine is running. During the backup operation, disk changes are written to a new redo log and applied when the backup completes.
     - Pause the virtual machine for the duration of the backup operation and resume processing when the backup completes. By default, the backup is compressed.
9. Select the option to delete older backups or to retain the maximum number of backups.
10. Click Next.
11. Verify the backup details, and then click Schedule or Run Now.

If other operations, such as a copy, are in progress a backup is not performed immediately. The backup is automatically queued to run after any pending operations are complete.

If you unregister a virtual machine host, it is no longer managed by the Virtual Machine Management Pack, and the backup information for the virtual machine guests associated with that host are permanently removed. The backup files, including disk files, are retained in the designated location and you can manually delete them, if necessary.
Restoring virtual machine guest backups

The Virtual Machine Management Pack enables you to restore a virtual machine guest using a previously created backup. When you perform the following procedure, the selected backup is restored automatically to the virtual machine.

1. From the HP SIM toolbar, select **Deploy>Virtual Machine>Backups> Restore Virtual Machine from Backup.**
2. Select the backup image to be used to restore a virtual machine, and then click **Next.**
3. Select the virtual machine host where the backup is to be deployed from the list of authorized licensed hosts.
4. Verify that adequate available disk space exists on the target virtual machine host to accommodate the total transport volume, which consists of several disks and configuration files.
5. Select a location for the configuration file and virtual machine drives on the designated host, and then click **Next.**
6. Verify the restore details, and then to restore the backup immediately, click **Run Now,** or to restore the backup later, click **Schedule.**

Restoring a virtual machine guest backup, including a VMware ESX Server 3.x or later that is running, using a memory state (a snapshot of the guest operating system at a specific time) to a virtual machine host with incompatible hardware might produce errors when the virtual machine is restored. If errors occur, then remove the memory state to resolve the issue. Be sure that the source virtual machine and the restored virtual machine are not registered in the landscape at the same time.

If the virtual machine guest being restored already exists on the selected host, then one of the following must occur:

- If a virtual machine guest with the same BIOS ID exists on the virtual machine host and is located in the folder to where the backup is to be restored, then you must first stop the existing virtual machine host. Existing files are overwritten.
- If a virtual machine guest with the same BIOS ID exists on the virtual machine host and the restore location is different, then you must first unregister the existing virtual machine host. The restore folder must be empty before restoring the backup.
- If a virtual machine guest with the same BIOS ID exists on a different virtual machine host, then a warning appears. The restore folder must be empty before restoring the virtual machine guest.

Restoring the last virtual machine guest backup

The Virtual Machine Management Pack enables you to restore a virtual machine guest using the last backup created. When you perform the following procedure, the last backup is restored automatically to the virtual machine.

1. On the HP SIM All Systems page, select the virtual machine guest.
2. From the HP SIM toolbar, select **Deploy>Virtual Machine>Backups> Restore Last Virtual Machine Backup.**
3. Verify the source virtual machine guest, and then click **Next.**
4. Verify the restore details, and then to restore the backup immediately, click **Run Now,** or to restore the backup later, click **Schedule.**
Recovering virtual machines of a failed host (VMware ESX Server only)

Alternate virtual machine host information in the Virtual Machine Configuration Details table is retained after recovery of a failed virtual machine and can be manually deleted, if necessary.

Recover virtual machines of a failed host to move all enabled virtual machines from a specified failed host to their defined recovery servers.

To recover a virtual machine of a failed host:
1. If the virtual machines are to remain on the recovery servers, set a new alternate virtual machine host. For more information, see the HP ProLiant Essentials Virtual Machine Management Pack User Guide.
2. In the HP SIM All Systems page, select the failed VMware ESX Server virtual machine host.
3. From the HP SIM toolbar, select Deploy>Virtual Machine>Recover Virtual Machines of Failed Host.
4. To recover the virtual machine now, click Run Now, or to perform the recovery later, click Schedule.

When you schedule VMM tasks, the Schedule option in HP SIM does not work reliably because the Virtual Machine Management Pack might not be activated when HP SIM is activated.
Scheduled tasks are evaluated every minute. The maximum time delay between the scheduled time of an event and when the event is actually performed is 59 seconds.

Setting alternate virtual machine hosts (VMware ESX Server only)

You must store all virtual disks for the virtual machine on a SAN-based VMware file system.

IMPORTANT: The failover host must have access to the VMware file system where the virtual machine virtual disks are stored.

Specifying an alternate virtual machine host for a virtual machine enables a recovery server to be designated for one or more virtual machines.
1. In the HP SIM All Systems page, select the VMware ESX Server virtual machine.
2. From the HP SIM toolbar, select Configure>Virtualization Management>Set Alternate Virtual Machine Host.
3. Verify the source virtual machine, and then click Next.
4. Select the recovery hosts from the list of authorized licensed hosts, and then click Run Now.

Removing alternate virtual machine hosts (VMware ESX Server only)

To remove the alternate host definition for all target systems:
1. In the HP SIM All Systems page, select the VMware ESX Server virtual machine.
2. From the HP SIM toolbar, select Configure>Virtualization Management>Set Alternate Virtual Machine Host.
3. Select Remove the alternate host definition, and then click Run Now.
Launching remote access

The Virtual Machine Management Pack provides direct access to the virtualization technology interface. The following sections provide detailed information on the type of virtualization technology installed depending on the virtual machine host and the operating system installed on the virtual machine guest.

Launching the Remote Console

Microsoft Virtual Server 2005 remote console is only supported by Microsoft Internet Explorer browsers. If you are using VMware versions other than VMware ESX Server 3.x, you must install the VMware Virtual Machine Console on the client that you are using.
If you are using VMware ESX Server 3.x, the Virtual Machine Management Pack directs you to the VMware ESX Server management website so that you can optionally download the VMware Virtual Infrastructure Client.

For VMware ESX Server 2.5.x
1. From the HP SIM All Systems page, click the virtual machine host name or the virtual machine guest name to go to the HP SIM System Page.
2. Click Remote Console.
3. In the Download Virtual Machine Console field from the ESX 2.5.x VMware Interface, click Windows.exe at [http://esx-server/vmware/en].

For VMware GSX Server
Install the VMware Virtual Machine Console from the VMware GSX installer package or download it from http://www.vmware.com.

For VMware Server
Install the VMware Management Console from the VMware Server installer package or download it from http://www.vmware.com.

Launching the Remote Desktop
The VMware Management Interface must be installed on a client or CMS. If you are launching a Remote Desktop from a VMware host, the VMware Remote Console application must be installed on a client or CMS.

The Remote Desktop option is enabled if the guest operating system has Windows 2000, Windows 2003, or Windows XP, the virtual machine has been identified in HP SIM with a valid IP address, and the virtual machine is running. This option is disabled if the virtual machine guest operating system is unknown.
To launch a Remote Desktop:

1. From the HP SIM All Systems page, click the virtual machine host name or the virtual machine guest name to go to the HP SIM System page.
2. Click **Remote Desktop**.

### Launching VNC

The VMware Management Interface **must** be installed on a client or CMS. If you are launching virtual network computing (VNC) from a VMware host, the VMware Remote Console application **must** be installed on a client or CMS.

The Launch VNC option is enabled if the guest operating system is Linux, the virtual machine has been identified in HP SIM with a valid IP address, and the virtual machine is running. This option is disabled if the virtual machine guest operating system is unknown.

To launch VNC:

1. From the HP SIM All Systems page, click the virtual machine host name or the virtual machine guest name to go to the HP SIM System page.
2. Click **Launch VNC**.

### Restarting the VMM Agent

You might need to restart the VMM Agent on the virtual machine host in various situations, such as:

- If the virtualization technology was installed on the host after the VMM Agent had been installed.
- If the virtual machine guest information becomes inaccessible from the Virtual Machine Management Pack.

To restart the VMM Agent:

1. In the HP SIM All Systems page, select the virtual machine host.
2. From the HP SIM toolbar, select **Configure>Virtualization Management>Restart VMM Agent**.
3. Verify the virtual machine host, and then click **Next**.

The status of the task can be monitored by viewing the Task Results screen.
Setting or removing the performance threshold

Set or remove the performance threshold for either virtual machine guests or virtual machine hosts to trigger an HP SIM event. If a designated threshold is reached, a major (⚠️) icon appears and an event is generated in HP SIM.

1. In the HP SIM All Systems page, select the virtual machine guest or virtual machine host.
2. From the HP SIM toolbar, select Configure>Virtualization Management>Set Performance Thresholds.
3. Verify the virtual machine guest or virtual machine host, and then click Next.
4. Determine whether existing values and intervals must be added, updated, or removed by selecting Add/Update or Remove.
5. Enter the appropriate values and intervals in the Processor Threshold, Memory Threshold, Network Throughput Threshold, and Storage Throughput Threshold sections. Valid values include the following:
   - Value (Percent)—Enter the value as a percentage
   - Interval (Minutes)—Enter the interval in minutes
   - Value (KB)—Enter the value in kilobytes
6. Click Run Now.

Registering virtual machine hosts from HP SIM

To register the virtual machine host from HP SIM:

1. In the HP SIM All Systems page, select the virtual machine host.
2. From the HP SIM toolbar, to register the virtual machine host, select Configure>Virtual Machine Host Registration>Register VM Host, or to register the Linux host, select Configure>Virtual Machine Host Registration>Linux Host.

   To perform the registration step, SSH must be configured for transferring the certificates onto the host through a secure channel.

   During the registration process, the HP SIM certificates are imported into the agents trust store. The following steps occur during the registration process:
   a. The HP SIM certificate cms.cer, generated during install, is copied to the host. For Windows, C:\Documents and Settings\Administrator is used, and for Linux, /root is used.
   b. The Importcert.bat file is copied to the Windows host or the importcert.sh file is copied for the Linux file.
   c. The batch file/sh file is run to import the HP SIM certificate into the agent trust store.
   d. After the HP SIM certificate is successfully imported, the VMM Agent is stopped and started, so that the agent service uses the updated keystore and agent trust store.
   e. The host is registered to the CMS and the CMS is enabled for communicating with agents using the CMS certificate.
3. Verify that the correct target host appears in the list, to add targets, click Add Targets, or to remove targets, click Remove Targets, and then click Next.
4. To register the host immediately, click Run Now.
Registering virtual machine hosts using the command line interface

To register a virtual machine host using the CLI:

1. Access the CLI.
2. Enter the following information:
   - `vmcli -deployVMMAgentCertificate <URI agent> <isWindows - boolean>`
   - `vmcli -registerAgent <URI agent>`

Deploying the HP SIM certificate on the Virtual Machine Management service

To deploy the HP SIM certificate on the Virtual Machine Management Pack, enter the following command from the command line:

```
C:\Program Files\HP\Virtual Machine Management Pack\bin\vmcli -updateVMMTruststore
```

Unregistering virtual machine hosts

⚠️ **CAUTION:** Unregistering a virtual machine host permanently removes all information from the Virtual Machine Management Pack database pertaining to the virtual machine guests located on this host, including backup information.

To unregister the virtual machine host:

1. In the HP SIM All Systems page, select the virtual machine host.
2. From the HP SIM toolbar, select **Configure>Virtual Machine Host Registration>Unregister VM Host.**
3. Verify that the correct target host appears in the list, to add targets, click **Add Targets,** or to remove targets, click **Remove Targets,** and then click **Next.**
4. To unregister the host immediately, click **Run Now.**

Configuring the polling frequency for virtual machine status checks

The Virtual Machine Management Pack provides a configurable parameter named VMConfigRefreshRate. This parameter controls the frequency with which the VMM Agent checks if the virtual machine configuration has changed, such as number of NICs on the virtual machine, size of the hard disk, and so on. Configuration changes on the virtual machines are updated by the Virtual Machine Management Pack. The default polling frequency is 5 seconds.

The polling frequency can be changed by updating `VMConfigRefreshRate=<value in milliseconds>` in the `hpvmm.conf` file.

The config file can be found in the following locations:

- For VMware ESX server—`/usr/share/vmm/bin/hpvmm.conf`
- For VMware GSX and Microsoft Virtual servers—`<HP VMM agent installation directory>/bin/hpvmm.conf`

If the `hpvmm.conf` file is not present, a text file named `hpvmm.conf` must be created in the appropriate location listed above. The value of the parameter can be between 5 seconds and 5 minutes. Any values entered outside this range are automatically adjusted to the max/min value of the range.
Because increasing the polling frequency also reduces the ability of the Virtual Machine Management Pack to learn the changes in virtual machine status, HP recommends changing only this parameter if you simultaneously use the VMware Consolidated Backup (VCB) and the Virtual Machine Management Pack.

**Event handling**

Virtual Machine Management Pack 3.0 supports event handling mechanisms, which receive host-specific events for the virtual hosts managed by both VirtualCenter 2.x and later and by the Virtual Machine Management Pack. When a host-specific event occurs, the events are recorded in HP SIM Event page with VC EVENT appearing at the beginning of the event. For virtual machine hosts that are managed by Virtual Machine Management Pack and not by VirtualCenter, ESX/VC appears at the beginning of the event.

### Setting up prefailure event handling

HP SIM can detect certain prefailure alerts and generate corresponding events. The Virtual Machine Management Pack uses VMotion to enable you to configure event handlers for these events so that the virtual machine can be moved to an alternate host before the system fails or is placed in maintenance mode.

The capability to detect prefailure alerts is only supported on VirtualCenter 2.x platforms and for VMware ESX hosts and virtual machines, which are on shared storage.
Automatic prefailure event handling

To create a new collection of VMware ESX systems:

1. From the HP SIM main page, select Customize. The Customize Collections screen appears.
2. From the Show collections of box, select System.
3. In the New Collection section, select one of the following collection types:
   - Choose members individually
   - Choose members by attributes
   - Choose members from the existing system and event collections
   If you select System collection, select Choose members individually, and then select the servers from the available list and save the collection.
   A predefined collection PreFailure Events appears on the Customize collections page in the Shared events category. You can edit this collection.
4. After the collection has been created, select Deploy>Virtual Machine>Handle VM Host Prefailure Events.
5. Select Select “Prefailure Test ESX Collection” itself, and then click Apply.
6. Click Add Event Filter.
7. Select the PreFailure Events collection that has already been created, click Apply, and then click Next. The Handle VM Host Prefailure Events screen appears.
8. To have the events automatically handled, click Schedule, select When new systems or events meet the list criteria, and then click Done. After you click Done, the new system or events that meet the criteria on the failed host are recovered to an alternate host (if one has been set up) or to place the host on maintenance mode.

Semiautomatic prefailure event handling

To configure alerts on the events to be delivered using e-mail:

1. To create system collections from the HP SIM main page, select Customize.
2. Select Options>Events>Automatic Event Handling>New Task to configure alerts for the events created. When the event occurs, an e-mail is automatically sent to the user.
3. Select Deploy>Virtual Machine>Handle VM Host Prefailure Events.
4. Verify the failed server host from the e-mail you receive, and then click Next.
5. To have the events manually handled now, click Run Now. When you click Run Now, the failed host is recovered to an alternate host (if one has already been set up) or the host is placed on maintenance mode.
Failed host recovery

Use the failed host recovery feature if you do not use the VMware VirtualCenter High Availability (HA) solution. The failed host recovery feature enables you to recover a failed VMware ESX Server host and leverage the ability of HP SIM to detect hardware failures. In a setup where both the failed host recovery feature and VMware VirtualCenter HA or VMware Distributed Resource Scheduler (DRS) are configured, the results might be unpredictable because both management tools try to control the same resource. Do not configure both the failed host recovery feature and the VMware HA or VMware DRS solution for the same VMware ESX hosts.

If the virtual machine being moved is already part of the VirtualCenter cluster, a warning message appears.

Setting up the recovery feature

To configure events to actions:

1. Create a CriticalVmHost collection based on the system health parameters.
2. Set your virtual machines so that you have appropriately-defined alternate hosts.
3. Schedule the recovery of failed hosts based on the collection and events.

Creating a CriticalVmHost collection

1. From the left pane of the HP SIM screen, click Customize, and then click New. The following screen appears.

2. Select Choose members by attributes.
3. Select the collection criteria as shown in the screen and then save the collection as CriticalVmHost.

Setting the alternate virtual machine host

To set alternate virtual machine hosts:

1. On the HP SIM All Systems page, select the VMware ESX Server virtual machine.
2. From the HP SIM toolbar, select Configure>Virtualization Management> Set Alternate Virtual Machine Host.
3. Verify the source virtual machine, and then click Next.
4. Select the recovery hosts from the list of authorized licensed hosts, and then click Run Now.

If some VMM menu options do not appear, then verify that at least one virtual machine guest has been properly discovered.
Scheduling the recovery of virtual machines of failed hosts feature

Recovery actions do not occur on virtual machine hosts or virtual machines without an alternate host set, even if those virtual machine hosts or virtual machines are included in the CriticalVmHost collection.

To schedule the recovery of virtual machines of failed hosts for any system that has turned critical and is part of the CriticalVmHost collection:

1. From the HP SIM toolbar, select Deploy>Virtual Machine>Recover Virtual Machines of Failed Host. The RecoverVMs screen appears.

2. From the Add targets by selecting from list, select CriticalVmHost.

3. Select Select “CriticalVmHost” itself as the target. Click Apply.

4. Verify the failed VMware ESX server host, and then click Next.
5. Confirm your choices, and then click **Schedule**.

6. You are prompted to schedule the task. Select **When new systems or events meet the list criteria**. The feature runs after the hardware status of a virtual machine host becomes critical.

7. Click **Done**.
Launching SCVMM

You can quickly access the System Center Virtual Machine Manager (SCVMM) client from the Virtual Machine Host or System Page within the Virtual Machine Management Pack instead of launching SCVMM separately.

Microsoft Virtual Server host system page

When using a Microsoft Virtual Server, from the host system page, click Launch SCVMM.
Microsoft Virtual Server guest system page

When using a Microsoft Virtual Server, from the guest system page, click **Launch SCVMM**.

Launching VirtualCenter

You can quickly access the VirtualCenter client from the Virtual Machine Host or System Page within the Virtual Machine Management Pack instead of launching VirtualCenter separately.

VMware ESX Server host system page

When using a VMware ESX Server, from the host system page, click **Launch VC**.
VMware ESX Server guest system page

When using a VMware ESX Server, from the guest system page, click Launch VC.

VirtualCenter information

The VirtualCenter information feature is only supported on VirtualCenter 2.x and on VMware ESX 2.x and 3.x hosts and virtual machines. To view information, VirtualCenter must be running and VirtualCenter URL credentials must be available in the Virtual Machine Management Pack.

You can import Virtual Center clusters and resource pool information from the VirtualCenter and view it on the System Page of the virtual machine host or guest within the Virtual Machine Management Pack, instead of logging into the Virtual Center separately.
To access VirtualCenter information, on the guest system page or host system page, click VirtualCenter Information.

Configuring Virtual Machine Management Pack on a Microsoft Cluster Server


Virtual machine hosts must be registered for at least one of the active node in the cluster. When the failover happens, the Virtual Machine Management Pack automatically establishes the trust between the VMM Agents and the active CMS node in the cluster by using the digital certificate on the cluster.

Virtual Machine Management Pack also ensures that after a failover occurs no data is lost within 5 hours of the CMS being powered up.
Multisystem aware tools available

A main feature within HP SIM is the possibility to run tools on multiple systems at once, or multisystem aware tools. The following Virtual Machine Management Pack tools can be multisystem aware:

- Starting virtual machine hosts
- Stopping virtual machine hosts
- Restarting virtual machine hosts
- Pausing virtual machine hosts
- Setting failover host
- Setting the performance threshold
- Recovering failed hosts of a virtual machine hosts
- Restarting an agent
- Deploying an agent
- Scheduling backups
- Restoring Last backup
- Performing moves, such as FastMove, VMotion, and regular
- Defining new virtual machine host collections for all VMware ESX virtual machines

For more information on multisystem aware tools, see the HP SIM User Guide at http://www.hp.com/go/hpsim.

Performance information

These sections list information that appears on the Performance tab of the System Page for virtual machine hosts and guests. Use the performance information to determine virtual machine host capacity and virtual machine workload characteristics. Use the threshold function to create alerts and log messages based on user-selectable performance values.

Virtual machine host

Click a virtual machine host in the HP SIM console, and then click the Performance tab to display the performance information for the host. You can choose to display activity for the most recent 1, 5, 15, 30, or 60 minutes. If the amount of time requested exceeds the amount available, all available information is reported.

Virtual machine host performance

The following performance information is provided for VMware ESX Server, VMware GSX Server, VMware Server and Microsoft Virtual Server 2005 hosts, except where noted.

- Processor utilization (x cpus)—The processor utilization on the host, including utilization by the virtual machines. The number of processor cores or threads on the virtual machine host is reported as x cpus.
- Virtual machine processor utilization—The processor consumption by all virtual machines on this host. Processor resources consumed by a virtual machine before powering down the virtual machine are not included.
- Reserved capacity (All running virtual machines)—The sum of the Reserved System Capacity values for all virtual machines currently powered up (Microsoft Virtual Server 2005 only).
- CPU min (All running virtual machines)—The sum of the CPU Min values for all virtual machines currently powered up, divided by the resources available on the host (VMware ESX Server only).
• Memory utilization—The total amount of memory currently in use on the host. The utilization bar indicates the memory utilization as a percentage of the physical memory configured.

• Virtual machine memory—The total amount of memory currently in use by virtual machines executing on the host. Memory consumed by a virtual machine before powering down the virtual machine is not included. The utilization bar indicates the virtual machine memory as a percentage of the physical memory configured (Microsoft Virtual Server 2005 and VMware ESX Server).

• Network throughput—Network traffic transmitted and received on this host. Virtual machine network throughput is included for VMware ESX Server.

• Network transmit throughput—Network traffic transmitted by this host. Virtual machine network transmission throughput is included for VMware ESX Server. The utilization bar represents the transmission percentage of the network throughput.

• Network receive throughput—Network traffic received by this host. Virtual machine network receive throughput is included for VMware ESX Server. The utilization bar represents the receive percentage of the network throughput.

• Storage throughput—Storage read and written by this host and all virtual machines on the host. This utilization bar is always completely filled.

• Storage read throughput—Storage read by this host and all virtual machines on the host. The utilization bar represents the read percentage of storage throughput.

• Storage write throughput—Storage written by this host and all virtual machines on the host. The utilization bar represents the write percentage of storage throughput.

Virtual machine performance

The value averages that appear in this section are relative to the duration of the virtual machine host activity. Resources consumed by a virtual machine before powering down the virtual machine are not included.

• CPU—The CPU percentage consumed by the virtual machine relative to the total processor capacity of the virtual machine host.

• vCPU—The CPU percentage consumed by the virtual machine relative to its resource allocation.

• Memory—Physical host memory consumed by the virtual machine (VMware ESX Server and Microsoft Virtual Server 2005).

• Network—Network throughput for the virtual machine. The utilization bar indicates the virtual machine network throughput as a percentage of the total network throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).

• Storage—Storage throughput for the virtual machine. The utilization bar indicates the virtual machine storage throughput as a percentage of the total storage throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).

• Threshold settings—A virtual machine host-specific threshold can be evaluated.

• Threshold interval—The number of minutes of utilization data that must be available before the threshold is evaluated.

• Threshold value—The maximum utilization value that provides a normal status.

• Measured interval—The number of minutes of utilization data averaged to calculate the measured value.
• Measured value—The average utilization over the most recent measured interval.
• State—The current state of this threshold. The state can be:
  o Unknown, indicating that the number of utilization samples available is less than the threshold interval
  o Normal, indicating that sufficient utilization samples are available, and the measured value is less than or equal to the threshold value
  o Exceeded, indicating that sufficient utilization samples are available, and the measured value is greater than the threshold value

Virtual machine guest

To display performance information for the guest, click a virtual machine guest in the HP SIM console, and then click the **Performance** tab. Select the appropriate time frame at the top of the screen for which to display information.

Virtual machine performance

The following performance information is provided for VMware ESX Server and Microsoft Virtual Server 2005 hosts.

• Virtual processor utilization (vCPU)—The CPU percentage consumed by the virtual machine relative to the resource allocation. The Host Processor Utilization on one CPU value is reported.
• Host processor utilization on x CPUs—The CPU percentage consumed by the virtual machine relative to the number of physical processors (x) on which the virtual machine can execute.
• Host processor utilization on all CPUs—The CPU consumed by this virtual machine, relative to the total virtual machine host processors.
• Memory utilization—The physical host memory used by this virtual machine. The utilization bar indicates the virtual machine memory utilization as a percentage of the physical memory configured on the virtual machine host.
• Network throughput—The network traffic transmitted and received by this virtual machine. The utilization bar indicates the virtual machine network throughput as a percentage of the total network throughput on the virtual machine host.
• Network transmit throughput—The network traffic transmitted by this virtual machine. The utilization bar indicates the virtual machine Network Transmit Throughput as a percentage of the total network throughput on the virtual machine host.
• Network receive throughput—The network traffic received by this virtual machine. The utilization bar indicates the virtual machine network receive throughput as a percentage of the total network throughput on the virtual machine host.
• Storage throughput—The storage read and written by this virtual machine. The utilization bar indicates the virtual machine storage throughput as a percentage of the total storage throughput on the virtual machine host.
• Storage read throughput—The storage read by this virtual machine. The utilization bar indicates the virtual machine storage read throughput as a percentage of the total storage throughput on the virtual machine host.
• Storage write throughput—The storage written by this virtual machine. The utilization bar indicates the virtual machine storage write throughput as a percentage of the total storage throughput on the virtual machine host.
Resource allocation

The bars indicate the virtual machine allocation relative to the capacity available on the virtual machine host.

- VMware ESX Server virtual machines
  - CPU min—The cpu.min value reported by VMware ESX Server
  - CPU max—The cpu.max value reported by VMware ESX Server
  - CPU shares—The cpu.shares value reported by VMware ESX Server
- Microsoft Virtual Server 2005 virtual machine
  - Reserved capacity—The reserved system capacity value reported by Microsoft Virtual Server 2005 relative to one CPU
  - Maximum capacity—The maximum system capacity value reported by Microsoft Virtual Server 2005 relative to one CPU
  - Relative weight—The relative weight value reported by Microsoft Virtual Server 2005
- Threshold settings—A virtual machine-specific threshold can be evaluated
- Threshold interval—The number of minutes of utilization data that must be available before the threshold is evaluated
- Threshold value—The maximum utilization value that provides a normal status
- Measured interval—The number of minutes of utilization data that was averaged when calculating the measured value
- Measured value—The average utilization over the most recent measured interval minutes
- State—The current state of this threshold, which can be:
  - Unknown, indicating that the number of utilization samples available is less than the threshold interval
  - Normal, indicating that sufficient utilization samples are available and the measured value is less than or equal to the threshold value
  - Exceeded, indicating that sufficient utilization samples are available and the measured value is greater than the threshold value

Performance color codes

The color codes on the Performance page indicate the percentage of a resource that has been consumed. The colors of the utilization bar indicate the following conditions:

- Blue—Indicates throughput
- Green—Indicates utilization is less than 70%
- Yellow—Indicates utilization is between 70% and 80%
- Red—Indicates utilization is greater than 80%
Virtual Machine Management Pack infrastructure

The Virtual Machine Management Pack is integrated completely within HP SIM to provide ease-of-use, installation, and maintenance. All requirements and practices for proper operation of HP SIM must be observed for Virtual Machine Management Pack. For more information about using HP SIM, see the appropriate version of the *HP Systems Insight Manager Installation and User Guide*.

The Virtual Machine Management Pack includes the following components, which are installed and set up during the software installation:

- The Virtual Machine Management (VMM) Pack—Resides on the HP SIM Central Management Server (CMS) and provides access to the virtual machine monitoring and control functions, accessible locally or remotely using industry-standard web browsers
- The Virtual Machine Management (VMM) Agent—Deployed to managed virtual machine hosts from the HP SIM toolbar


Virtualization and consolidation of servers   197
7 Reporting

This chapter describes the generating and printing of reports in HP SIM, and viewing patch installation status.

Reporting in HP SIM

This section describes the generating of reports in HP SIM and viewing software details.

Generating reports in HP SIM

The HP SIM System Information Reporting feature enables you to generate system information reports. In addition to generating reports, you can create customized report configurations and edit, copy, and delete report configurations. All users with login access to HP SIM can generate reports.

NOTE: To learn how to add a new report, see the appropriate version of the HP Systems Insight Manager Installation and Configuration Guide.

The System Information Reporting feature provides you with the following options:

- Managing Reports—Select Reports>Manage Reports. The Manage Reports page appears.
- Running Reports—Select Reports>Manage Reports. The Manage Reports page appears. Select the report that you want to run. Select the report format HTML, XML, or CSV. Click Run Report.
- Editing Reports—Select Reports>Manage Reports. The Manage Reports page appears. Select the report that you want to edit, and then click Edit. The Edit Report section appears.
- Copying Reports—Select Reports>Manage Reports. The Manage Reports page appears. Select the report that you want to copy, and then click Copy. The Copy Report section appears.
- Running Reports in HTML Format—Select Reports>Manage Reports. The Manage Reports page appears. Select the report you want to run in HTML format, and then select HTML>Run Report.
- Running Reports in XML Format—Select Reports>Manage Reports. The Manage Reports page appears. Select the report you want to run in XML format, and then select XML>Run Report.
- Running or Downloading Reports in CSV Format—Select Reports>Manage Reports. The Manage Reports page appears. Select the report you want to run or download the report in Comma Separated Value (CSV) format, and then select CSV>Run Report.
- Showing SQL Queries—Select Reports>Manage Reports. The Manage Reports page appears. Select the report for which you want to view the SQL details, and then select Run Report> Show SQL queries.
- Deleting Reports—Select Reports>Manage Reports. The Manage Reports page appears. Select the reports to be deleted, and then click Delete.
- Hardware and Operating System Reports—Several predefined reports are available for general information about server hardware and operating system information. To access these reports, select Reports>New Report or Reports>ManageReport. Categories exist for General, UNIX®, HP-UX only, Virtual Machines, and others. Expand the appropriate category and select the reports you want to review (such as Inventory, CPU, Operating System Information or HP-UX File System).

• **PMP Reports**—Three PMP reports are available through HP SIM:
  ○ **Status Analysis Report**—Displays configurations of server components, processors, memory, network connections, storage, and host buses. To access this report, select Reports>Performance Management Pack Reports>Static Analysis Report.
  ○ **System Summary Report**—Displays the percentage of time the server remains in a bottleneck state, the overall performance utilization of the server for each of its components, and the server configuration details. To access this report, select Reports>Performance Management Pack Reports>System Summary Report.
  ○ **CSV File Generator**—Displays the logged data from the PMP repository for all server components in a .csv file for import into desktop analysis or report tools. To access this report, select Reports>Performance Management Pack Reports>CSV File Generator.

---

### Software inventory details

A software inventory lists the HP software installed on a target system. HP SIM inventory retrieves and stores information from internal disk drives. HP Version Control Agent must be installed for HP SIM inventory to occur. HP Version Control Agent is an agent that is installed on a server to enable you to see the HP software installed on that server. The Version Control Agent can be configured to point to a Version Control Repository Manager agent, enabling easy version comparison and software updates from the repository.

For a complete description of other HP SIM components, see the HP SIM documentation.

---

### Printing reports in HP SIM

1. Select **Tasks & Logs>View Tasks Results**.
2. Click **View Printable Report**. A Print Report Question prompt appears, asking to generate a report containing only the currently selected target system or all target systems associated with the task instance.
3. Select which report to print.
4. To print the report, click **OK**.

---
Sample PMP CSV file

PMP enables you to generate many reports, and each user can have a different set of requirements. Therefore, PMP supplies all of the performance information gathered in a file that can be read by many desktop-reporting tools, including Microsoft Excel.

The following figure depicts a summary report generated in .csv file format and that appear in Microsoft Excel. This file format contains fully annotated performance data in a table, enabling information to be displayed and manipulated in a wide variety of data analysis and graphing applications.
### PMP measurement categories

The following is a list of the measurement categories for servers and subsystem components.

#### Servers

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample time</td>
<td>Page faults per second</td>
</tr>
<tr>
<td>Server performance</td>
<td>Page reads per second</td>
</tr>
<tr>
<td>Processor performance</td>
<td>Available Megabytes</td>
</tr>
<tr>
<td>Average processor busy</td>
<td>NIC performance</td>
</tr>
<tr>
<td>Processor busy</td>
<td>NIC Megabytes per second</td>
</tr>
<tr>
<td>Interrupts per second</td>
<td>Storage performance</td>
</tr>
<tr>
<td>Context switches per second</td>
<td>Storage transfers per second</td>
</tr>
<tr>
<td>Memory performance</td>
<td>Storage Megabytes per second</td>
</tr>
<tr>
<td>Hard page faults per second</td>
<td>PCI performance</td>
</tr>
<tr>
<td>Pages input per second</td>
<td>Host bus Megabytes per second</td>
</tr>
</tbody>
</table>

#### Servers with MSVS or VMware GSX (VM Host)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sample time</td>
<td>Page faults per second</td>
</tr>
<tr>
<td>Server performance</td>
<td>Page reads per second</td>
</tr>
<tr>
<td>Processor performance</td>
<td>Available Megabytes</td>
</tr>
<tr>
<td>Average processor busy</td>
<td>NIC performance</td>
</tr>
<tr>
<td>Processor busy</td>
<td>NIC Megabytes per second</td>
</tr>
<tr>
<td>Interrupts per second</td>
<td>Storage performance</td>
</tr>
<tr>
<td>Context switches per second</td>
<td>Storage transfers per second</td>
</tr>
<tr>
<td>Memory performance</td>
<td>Storage Megabytes per second</td>
</tr>
<tr>
<td>Hard page faults per second</td>
<td>PCI performance</td>
</tr>
<tr>
<td>Pages input per second</td>
<td>Host bus Megabytes per second</td>
</tr>
<tr>
<td>Average Physical Processor Busy</td>
<td>Average Virtual Processor busy</td>
</tr>
<tr>
<td>Available MB</td>
<td>Network Megabytes per second</td>
</tr>
<tr>
<td>Storage megabytes per second</td>
<td>—</td>
</tr>
</tbody>
</table>
### Servers with VMware ESX (VM Host)

| Sample time | Storage Read per second |
| Server performance | Storage Write per second |
| Processor performance | Host bus megabytes per second |
| Average processor busy | Average Physical Processor Busy |
| Available megabytes | Average Virtual Processor busy |
| NIC megabytes per second | Available megabytes |
| NIC Megabits Transmitted per second | Network megabytes per second |
| NIC Megabits Received per second | Storage megabytes per second (Consolidated value of the VM Guests on the host) |
| Storage megabytes per second (for the Physical Server) | |

**IMPORTANT:** The measurement categories are not applicable for the Server with VMware ESX Host

**NOTE:** Physical Processor Reserved and Physical Processor Limit are not applicable for the Guest configured on the VMware GSX Server

### VM Guest

| Sample time | Available megabytes |
| VM performance | Network megabytes per second |
| Processor performance | NIC Megabits transmitted per second |
| Average Physical Processor Busy | NIC Megabits received per second |
| Average Virtual Processor busy | Storage megabytes per second |
| Physical Processor Reserved | Storage Read megabytes per second |
| Physical processor Limit | Storage Write megabytes per second |

### Smart Array Controllers

| Controller ID | Transfers per second |
| Name | Megabytes per second |
| PCI slot | Millisecond per transfer |
| Sample time | Queue length |
| Performance | — |
## Smart Array Logical Drives

| Controller ID | Writes per second |
| Drive array   | Read Megabytes per second |
| Logical drive | Write Megabytes per second |
| Windows physical disk | Milliseconds per read |
| Drive ID      | Milliseconds per write |
| Sample time   | Queue length |
| Reads per second | -- |

## Smart Array Physical Arrays

| SCSI bus | Performance | Disk writes per second |
| Drive bay | Array reads per second | Disk read Megabytes per second |
| Disk type | Array writes per second | Disk write Megabytes per second |
| Controller ID | Array seconds per read | Disk seconds per read |
| Drive array | Array seconds per write | Disk seconds per write |
| Sample time | Disk reads per second | Disk queue length |

## SCSI buses attached to Smart Array Controllers

| Enclosure type | Performance |
| Controller ID | Transfers per second |
| SCSI bus | Megabytes per second |
| Sample time | SCSI bus utilization percent |

## Fibre Channel Host Bus Adapters

| PCI slot | Transfers per second |
| Controller model | Megabytes per second |
| HBA ID | Milliseconds per transfer |
| Sample time | Queue length |
| Performance | -- |
Fibre Channel Enclosures

<table>
<thead>
<tr>
<th>Model</th>
<th>Sample time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Transfers per second</td>
</tr>
<tr>
<td>Controller</td>
<td>Megabytes per second</td>
</tr>
<tr>
<td>Current role</td>
<td>Milliseconds per transfer</td>
</tr>
<tr>
<td>HBA</td>
<td>Enclosure queue</td>
</tr>
<tr>
<td>Enclosure</td>
<td>—</td>
</tr>
</tbody>
</table>

SCSI Adapters

<table>
<thead>
<tr>
<th>PCI Slot</th>
<th>Sample time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>Transfers per second</td>
</tr>
<tr>
<td>Adapter</td>
<td>Megabytes per second</td>
</tr>
</tbody>
</table>

SCSI buses attached to SCSI Adapters

<table>
<thead>
<tr>
<th>Model</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter</td>
<td>Transfers per second</td>
</tr>
<tr>
<td>Bus</td>
<td>Megabytes per second</td>
</tr>
<tr>
<td>Sample time</td>
<td>SCSI bus utilization percent</td>
</tr>
</tbody>
</table>

SCSI drives attached to SCSI Adapters

<table>
<thead>
<tr>
<th>Model</th>
<th>Writes per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter</td>
<td>Read Megabytes per second</td>
</tr>
<tr>
<td>Bus</td>
<td>Write Megabytes per second</td>
</tr>
<tr>
<td>Drive bay</td>
<td>Milliseconds per read</td>
</tr>
<tr>
<td>Sample time</td>
<td>Milliseconds per write</td>
</tr>
<tr>
<td>Performance</td>
<td>Queue length</td>
</tr>
<tr>
<td>Reads per second</td>
<td>—</td>
</tr>
</tbody>
</table>
### IDE Controllers

<table>
<thead>
<tr>
<th>Model</th>
<th>Megabytes per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller ID</td>
<td>Milliseconds per transfer</td>
</tr>
<tr>
<td>Sample time</td>
<td>Queue length</td>
</tr>
<tr>
<td>Transfers per second</td>
<td>—</td>
</tr>
</tbody>
</table>

### Network Adapters

<table>
<thead>
<tr>
<th>Model</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Slot</td>
<td>Megabits sent per second</td>
</tr>
<tr>
<td>Sample time</td>
<td>Megabits received per second</td>
</tr>
</tbody>
</table>

### Host Buses

<table>
<thead>
<tr>
<th>Device</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Megabytes per second</td>
</tr>
<tr>
<td>Sample time</td>
<td>Bus utilization percent</td>
</tr>
</tbody>
</table>
Sample PMP system summary report

System Summary reports are created in a browser window in a printable format. The report has two sections. The first section consists of a table showing what percentage of time each server subsystem was in a bottleneck state during the selected interval. This table provides a convenient method for gauging the performance health of a server.

The second section of the summary report includes a detailed system configuration listing. This is the same information available for each component in the Online Analysis. This section is not applicable to VM Guests.

System summary report for a server or MSVS/VMware GSX Host

Performance Management Pack Summary Report for 131.111.1.71
Hardware Configuration as on 03/16/2004 11:00:00 a.m.
Reporting from 03/16/2004 11:19:03 a.m. to 03/19/2004 12:41:04 p.m.

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>% Normal</th>
<th>% Minor</th>
<th>% Major</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>96.0</td>
<td>4.0</td>
<td>0</td>
</tr>
<tr>
<td>Memory</td>
<td>68.0</td>
<td>14.0</td>
<td>18.0</td>
</tr>
<tr>
<td>Network Connections</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NC3131 Dual Port 10/100 Fast Ethernet Base Adapter Port ID: 1</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NC3131 Dual Port 10/100 Fast Ethernet Base Adapter</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Storage</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Smart Array 4250ES</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Array: A</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Internal Drive Cage</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Storage Works Fibre Channel Host Bus Adapter/P</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Host Buses</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Primary Bus</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Secondary Bus</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Tertiary Bus</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Server Model: ProLiant ML750

Processors
Intel® Pentium® III Xeon 700 MHz with 2-MB L2 Cache
Pentium III Xeon 700 MHz with 2-MB L2 Cache
Pentium III Xeon 700 MHz with 2-MB L2 Cache
Pentium III Xeon 700 MHz with 2-MB L2 Cache

Memory
Total Memory: 4096 MB

Network Connections
NC3131 Dual Port 10/100 Fast Ethernet Base Adapter (PCI Slot #: 3)
  (Port Id #: 1) Compaq NC3131 Fast Ethernet NIC

Storage
Smart Array 4250ES (PCI Slot #: 10)
  Array A
    Logical Drive 1 (Windows Physical Disk: 0)
Internal Drive Cage
  Bus: 1,ID: 0 9.1-GB Pluggable Wide Ultra2 SCSI 10,000-rpm Hard Drive (1")
    (Part of Array: A)
  Bus: 1,ID: 1 9.1-GB Pluggable Wide Ultra2 SCSI 10,000-rpm Hard Drive (1")
    (Part of Array: A)
Storage Works Fibre Channel Host Bus Adapter/P (PCI Slot #: 7)
Storage Works RAID Array 4x00 by Compaq
  Logical Drive: 1 (Windows Physical Disk: 3)

Host Buses
Primary Bus
  (Empty) (Slot #: 1)
  (Empty) (Slot #: 2)
  Compaq NC3131 Fast Ethernet NIC (Slot #: 3)
  (Empty) (Slot #: 4)
Secondary Bus
  Compaq NC3131 Fast Ethernet NIC (Slot #: 5)
  (Empty) (Slot #: 6)
  Compaq Storage Works Fibre Channel Host Bus Adapter/P (Slot #: 7)
  (Empty) (Slot #: 8)
  Compaq Smart Array 4200 Controller (Slot #: 9)
Tertiary Bus
  Compaq Smart Array 4250ES Controller (Slot #: 10)
  (Empty) (Slot #: 11)
System summary report for a VMware ESX Host

Performance Management Pack Summary Report for 131.111.1.72
Hardware Configuration as on 03/16/2004 11:00:00 a.m.
Reporting from 03/16/2004 11:19:03 a.m. to 03/19/2004 12:41:04 p.m.

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>% Normal</th>
<th>% Minor</th>
<th>% Major</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>96.0</td>
<td>4.0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Server Model:** ProLiant ML750

**Processors**
- Intel Pentium III Xeon\textsuperscript{M} 700 MHz with 2-MB L2 Cache
- Pentium III Xeon 700 MHz with 2-MB L2 Cache
- Pentium III Xeon 700 MHz with 2-MB L2 Cache
- Pentium III Xeon 700 MHz with 2-MB L2 Cache

**Memory**
- Total Memory: 4096 MB

**Network Connections**
- NC3131 Dual Port 10/100 Fast Ethernet Base Adapter (PCI Slot #: 3)
  - (Port Id #: 1) Compaq NC3131 Fast Ethernet NIC

**Storage**
- Smart Array 4250ES (PCI Slot #: 10)
  - Array A
    - Logical Drive 1 (Windows Physical Disk: 0)
- Internal Drive Cage
  - Bus: 1,ID: 0 9.1-GB Pluggable Wide Ultra2 SCSI 10,000-rpm Hard Drive (1")
    - (Part of Array: A)
  - Bus: 1,ID: 1 9.1-GB Pluggable Wide Ultra2 SCSI 10,000-rpm Hard Drive (1")
    - (Part of Array: A)
- Storage Works Fibre Channel Host Bus Adapter/P (PCI Slot #: 7)
- Storage Works RAID Array 4x00 by Compaq
  - Logical Drive: 1 (Windows Physical Disk: 3)

**Host Buses**

**Primary Bus**
- (Empty) (Slot #: 1)
- (Empty) (Slot #: 2)
- Compaq NC3131 Fast Ethernet NIC (Slot #: 3)
- (Empty) (Slot #: 4)

**Secondary Bus**
- Compaq NC3131 Fast Ethernet NIC (Slot #: 5)
- (Empty) (Slot #: 6)
- Compaq Storage Works Fibre Channel Host Bus Adapter/P (Slot #: 7)
- (Empty) (Slot #: 8)
- Compaq Smart Array 4200 Controller (Slot #: 9)

**Tertiary Bus**
- Compaq Smart Array 4250ES Controller (Slot #: 10)
- (Empty) (Slot #: 11)
System summary report for a VM Guest

Performance Management Pack Summary Report for 131.111.1.73
Hardware Configuration as on 03/16/2004 11:00:00 a.m.
Reporting from 03/16/2004 11:19:03 a.m. to 03/19/2004 12:41:04 p.m.

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>% Normal</th>
<th>% Minor</th>
<th>% Major</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>96.0</td>
<td>4.0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Overall PMP performance**

The overall performance status for a system can be determined by referencing the following values shown in the first half of the summary report:

- %Normal—Percentage of overall performance that is satisfactory with no impending or existing bottleneck condition
- %Minor—Percentage of overall performance that might be approaching a bottleneck condition
- %Major—Percentage of overall performance that is in a bottleneck condition

The following table describes configuration details and performance status for components analyzed by PMP. The appropriate components are shown in the second section of the summary report.

**NOTE:** When PMP is unable to analyze and log data for a component, the values of %Normal, %Minor, and %Major might be 0.

**Table 20** PMP overall performance summary

<table>
<thead>
<tr>
<th>Components</th>
<th>Description and configuration details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Server models</td>
</tr>
<tr>
<td>Processors</td>
<td>All individual processor models</td>
</tr>
<tr>
<td>Memory</td>
<td>Total physical memory</td>
</tr>
<tr>
<td>Network Connections</td>
<td>Overall network connections</td>
</tr>
<tr>
<td>Network Card Base Adapter</td>
<td>Network card base adapter (PCI slot number)</td>
</tr>
<tr>
<td>Port ID</td>
<td>Port ID number belonging to the network card base adapter (NIC model)</td>
</tr>
<tr>
<td>Storage</td>
<td>Overall storage</td>
</tr>
<tr>
<td>Shared Storage</td>
<td>Overall shared storage</td>
</tr>
<tr>
<td>Smart Array controller</td>
<td>Smart Array controller model (PCI slot number)</td>
</tr>
<tr>
<td>• Array</td>
<td>Configured array</td>
</tr>
<tr>
<td>• External enclosure</td>
<td>• Logical drive number (Windows Physical Disk number)</td>
</tr>
<tr>
<td>• Internal drive cage</td>
<td>• External enclosure connected to the controller</td>
</tr>
<tr>
<td></td>
<td>• Bus number, Drive ID, Size, SCSI drive model</td>
</tr>
<tr>
<td></td>
<td>• Internal drive cage connected to the controller</td>
</tr>
<tr>
<td></td>
<td>• Bus number, Drive ID, Size, SCSI drive model</td>
</tr>
</tbody>
</table>
### Table 20  PMP overall performance summary

<table>
<thead>
<tr>
<th>Components</th>
<th>Description and configuration details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCSI adapter</td>
<td>- SCSI adapter model</td>
</tr>
<tr>
<td>Internal drive cage</td>
<td>- Internal drive cage connected to the adapter</td>
</tr>
<tr>
<td></td>
<td>- Bus number, Drive ID, Size, SCSI drive model</td>
</tr>
<tr>
<td>ATA/IDE RAID controller</td>
<td>- ATA or IDE RAID controller name</td>
</tr>
<tr>
<td>Fibre Channel Host Bus Adapter</td>
<td>- Individual Fibre Channel host bus adapter model (PCI slot number)</td>
</tr>
<tr>
<td></td>
<td>- External enclosure model</td>
</tr>
<tr>
<td></td>
<td>- Logical drive number (Windows Physical Disk number)</td>
</tr>
<tr>
<td>Host Buses</td>
<td>- Primary bus</td>
</tr>
<tr>
<td>- Primary Bus</td>
<td>- (Empty or component model) (Slot number)</td>
</tr>
<tr>
<td>- Secondary Bus</td>
<td>- Secondary bus</td>
</tr>
<tr>
<td>- Tertiary Bus</td>
<td>- (Empty or component model) (Slot number)</td>
</tr>
<tr>
<td>- Slot number</td>
<td>- Tertiary bus</td>
</tr>
<tr>
<td></td>
<td>- (Empty or component model) (Slot number)</td>
</tr>
<tr>
<td></td>
<td>- Bus slot number</td>
</tr>
<tr>
<td></td>
<td>- (Empty or component model) (Slot number)</td>
</tr>
</tbody>
</table>
# Sample PMP Static Analysis Report

A Static Analysis Report is an analysis of the hardware configuration for the server as a whole, identifying potential problem areas. A complete list of the configuration information analyzed to report the status of server subsystems is provided in the “PMP measurement categories” section of this guide.

<table>
<thead>
<tr>
<th>Static Analysis Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Static Analysis Report</strong> Generation Date/Time: Jun 16, 2005 6:46:33 PM</td>
</tr>
<tr>
<td><strong>Server Name</strong></td>
</tr>
<tr>
<td><strong>Server IP</strong></td>
</tr>
<tr>
<td><strong>Serial Number</strong></td>
</tr>
<tr>
<td><strong>Processors</strong></td>
</tr>
<tr>
<td><strong>Memory</strong></td>
</tr>
<tr>
<td><strong>Network Connections</strong></td>
</tr>
<tr>
<td><strong>Storage</strong></td>
</tr>
</tbody>
</table>
Sample PMP server availability report

Server Availability report is created in a browser window in a printable format. The report has one section, consisting of a table showing what percentage of time each server was in a bottleneck state during the selected interval, Accessible Duration of Server in hours, Inaccessible Duration of Server in hours and Average of the above Metrics for selected servers.

Viewing patch installation status

You can view consolidated reports showing patch installation status for all systems managed by the Vulnerability and Patch Management Pack. The VPM Patch Agent updates the patch database with a list of all applicable patches, including patches installed by methods other than Vulnerability and Patch Management Pack. Patch reports display the installation status of these patches for each system. HP recommends performing a vulnerability scan to determine which patches are required.

You can view reports by systems or patches. A search filter is also available to view the status of a particular patch on a particular system.

Information displayed in patch reports is obtained during the most recent patch deployment or validation task. Therefore, this information might not be current. The patch installation status can be updated by validating installed patches.
Viewing patch installation status by patch

1. Select **Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View by Patch.**

2. To view patch installation status, select either of the following options:
   - To filter the list of patches that appear, select the appropriate patch source from the list.
   - To view information about a specific patch, in the Advisory column, click the patch identification number.

---

### View Patch Status By Patch

View patch status for all or part of the repository

<table>
<thead>
<tr>
<th>Advisory</th>
<th>Description</th>
<th>Installed</th>
<th>Not Installed</th>
<th>Other</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS03-031</td>
<td>Cumulative Patch for Microsoft SQL Server (915485)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-034</td>
<td>ASP.NET Path Validation Vulnerability (997219)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-026</td>
<td>Vulnerability in HTML Help Could Allow Remote Code Execution (993550)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-027</td>
<td>Vulnerability in Server Message Block Could Allow Remote Code Execution (994422)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-032</td>
<td>Vulnerability in Microsoft Agent Could Allow Spoofing (990406)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-033</td>
<td>Vulnerability in Telnet Client Could Allow Information Disclosure (994120)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-036</td>
<td>Vulnerability in Microsoft Code Management Module Could Allow Remote Code Execution (987274)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-018</td>
<td>Cumulative Security Update for Internet Explorer (986277)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-039</td>
<td>Vulnerability in Reg andRex Could Allow Remote Code Execution and Elevation of Privilege (996566)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>MS05-040</td>
<td>Vulnerability in Windows Telephony Service Could Allow Remote Code Execution (997106)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

**Note:** Click on the numbers inside the table for additional information.
Viewing patch installation status by search filter

1. Select Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View by Search Filter.

2. Enter a search parameter in the appropriate box, and then click Search. You can view patches by advisory number, target system, or the status of patches. Advisory numbers are MS05-005 or RHSA-2005-05-850.

3. To view information about a specific patch, click the patch identification number in the Advisory column.
Viewing patch installation status by system

1. Select Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View by System.

2. Click the entry in the Installed, Not Installed, or Other column for a system to display additional information about patches for that system. An entry in the Other column indicates that the Vulnerability and Patch Management Pack cannot determine if the patch has been installed, possibly because adequate information was not provided by the patch vendor.

Viewing the patches installed by the Vulnerability and Patch Management Pack

A list of patches that have been applied by the Vulnerability and Patch Management Pack is maintained for each system. To view the list of patches for an individual system:

1. Select Diagnose>Vulnerability and Patch Management>View Patch Installation Status>View Patches Installed by VPM.

2. Select the system for which to view patches installed, and then click Apply.
3. Verify that the correct target systems appear in the lists.
4. To reselect target systems, click **Add Targets** or **Remove Targets**, and then click **Next**.

The list of patches installed on the system by the Vulnerability and Patch Management Pack appears. The Status column indicates one of the following states for each patch:

- **Install – Successful**—The patch installation completed successfully.
- **Install – Unsuccessful**—The patch installation did not complete successfully.
- **Install – Restore**—The patch was previously installed, removed, and restored.
- **Reboot Required**—The patch requires a reboot, which has not yet been performed.
- **Not Applicable**—The patch was not installed because it was not needed on this system.
This chapter identifies and provides solutions for commonly encountered issues, as well as answers to frequently asked questions. The following topics are included:

- ASP.NET 1.1 installation error
- Various installation issues
- Applying and assigning licenses
- IIS error appears during installation
- Verifying environment functionality with ICE Advisor
- Insight Control Management installation fails to accept username, password already accepted by HP SIM
- Removing IIS configuration in the RDP uninstaller

**NOTE:** For discussion of troubleshooting errors that pertain to specific Insight Control Management components, see the related component documentation referenced in “Technical support” in this guide.

### ASP.NET 1.1 installation error

ASP.NET 1.1 is an installation prerequisite for Insight Control Management. ASP.NET 1.1 is included with the Windows 2003 installation, but it is not installed in Microsoft Internet Information Server (IIS) by default. This omission can cause an installation error message to appear.

If ASP.NET is not installed, click **Start > Control Panel > Add or Remove Programs > Add Remove Windows Components > Application Server > Details > ASP.NET**, and then select the checkbox to add ASP.NET.

If issues remain after installing ASP.NET 1.1, other versions of ASP.NET might be installed already. Insight Control Management requires ASP.NET version 1.1 to be registered as a default IIS ASP.NET application handler. The execution of the additional command might be required to register ASP.NET 1.1 as the default handler in IIS:

```
"%windir%\Microsoft.NET\Framework\v1.1.4322\aspnet_regiis.exe" -i
```

For more information about this issue, see [http://support.microsoft.com/kb/306005](http://support.microsoft.com/kb/306005) and [http://support.microsoft.com/kb/816782](http://support.microsoft.com/kb/816782).
Installation issues

NOTE: To access installation log files, look in the logs directory at c:\hpic\logs directory. Identify these files before calling HP for installation troubleshooting assistance.

NOTE: Installation on domain controllers is not recommended.

- The Insight Control Management must be installed using an account password. Passwords must be alphanumeric characters or be in the following set: [] () _ - @ $, . ‘ *.
- When performing an installation on a Japanese operating system, Japanese characters cannot be used in the username, password, or installation boxes.
- When executed remotely using the Remote Desktop application, the remote desktop must be started using the /console switch.
- For installations from a network share, the share must be mapped to a network drive (installation directly from the share using UNC is not supported). Also, because a reboot is required in the middle of the installation, the network drive must be connected using the reconnect at logon option so the installation can proceed after the system is rebooted.
- When installing from a network drive, the Internet Explorer security level for the Trusted Sites zone must be set to Low. Select Tools>Internet Options>Trusted Sites, and then ensure that Security Level for this zone is set to Low. In addition, if using Windows Server 2003 SP2, the option Requires server verification (https:) for all sites in this zone option must be cleared in the Trusted Sites window.
- When installing with a remote Rapid Deployment Pack installation, the installer might display an error message stating that the Rapid Deployment Pack is not executing in that system. If this message appears, ensure that no firewall (either native Windows or third-party) is running on the Rapid Deployment Pack server.
- When using the Rapid Deployment Pack or database installations in remote platforms, ensure that the firewalls in the remote servers and the HP SIM CMS are configured in such a way that network traffic is permitted to the Rapid Deployment Pack and database ports.
- When reusing the Rapid Deployment Pack, the credentials must have administrator permissions in the local server. If the servers are not in a Windows domain, the Rapid Deployment Pack username must also exist in the local system, and both must have the same password.
- When reusing an existing Rapid Deployment Pack installation, the Rapid Deployment Pack Server and Web Console must be installed on the same server to enable Insight Control Management to correctly use the Rapid Deployment Pack.
- When selecting the option to create the virtual directory in IIS FTP service for Rapid Deployment Pack deployment, the IIS FTP service must already be installed and running in the system.
- To get the Rapid Deployment Pack product operational, install the files of at least one operating system for deployment. You can install the files at installation time from the Deployment Operating Systems screen, or at operation time, according to the instructions of Appendix C, Installing additional operating systems to be deployed by Rapid Deployment Pack.
- When uninstalling the product, if a warning message mentioning the PXE Configuration Utility appears, click OK.
- If the message w3wp.exe - Application Error appears during the VPM uninstallation process, click OK.
- In order to properly install VPM, be sure the supplied credentials correspond to an administrative user account and also that the logged on user has administrative rights.
- When reusing an existing database installation, the credentials used for database authentication must be the same as those of the currently logged-in user. If HP SIM is already installed, you must log in with the same credentials used for database authentication in HP SIM.
• When using database-named instances, you must have fixed port numbers, not dynamic port numbers.

• When installing MSDE in the CMS and the Web Based Enterprise Services application is already installed, verify that the Distributed Enterprise Service Tools Architecture (DESTA) is stopped. The MSDE installation might fail if DESTA is running.

• When upgrading Rapid Deployment Pack to version 3.70 in Japanese systems, Operating Systems previously used for Rapid Deployment Pack might not be available after the update.

• The installer requires a reboot in the middle of installation. To complete installation and remove automatic restart settings, the installation application must continue after this reboot. Therefore, do not remove the installation DVD from the drive until the installation process completes.

• The installer does not support operating systems loaded from a network shared drive.

• When using the auto-login feature after a reboot, the system uses the native screen resolution of the local operating system. This might cause changes in screen resolution after the reboot when accessing the CMS through Remote Desktop. To avoid these changes, verify that the Remote Desktop resolution is the same as the resolution of the CMS operating system.

Applying and assigning Insight Control suite licenses from HP SIM license manager

If you attempt to assign an Insight Control Environment, Insight Control Environment for BladeSystem, or Insight Control Data Center Edition key from the license manager, the following error message appears:

License Manager does not know how to assign licenses for this product. License Manager has no information about this product. Install the HP Systems Insight Manager plug-in that uses this license or Collect License Information from a system running this product first.

For more information about assigning licenses to Insight Control suites, see the “Adding and applying licenses to Insight Control Environment” section in this guide. For more information about assigning licenses to Insight Control Environment for BladeSystem suites, see the “Adding and applying licenses to Insight Control Environment for BladeSystem” section in this guide. For more information about assigning licenses to Insight Control Data Center Edition, see the “Adding and applying licenses to Insight Control Data Center Edition” section in this guide.
Insight Control licensing menus do not appear

Licenses for Insight Control suites must be applied from the Insight Control Management license menus. The following must be completed for the menus to appear and function:

- Use the Insight Control Management integrated installer to install or upgrade components. This installs Insight Control Management Services which includes the licensing menus.
- Discover one or more ProLiant ML or DL (300 or 500 series) for Insight Control Environment (ML/DL) menu to appear.
- Discover one or more HP ProLiant c-Class server blades, p-Class server blades, or xw460c blade workstation for Insight Control Environment (BL) and Insight Control Data Center Edition menus to appear.
- If 7.90 agents are installed, make sure HP SIM hotfix HOTFIX51_015.jar is applied to ensure correct HP SIM discovery of ProLiant servers and blade servers. This hotfix can be applied from the Insight Control Management 2.10 integrated installer.

Correct discovery of the appropriate system type is necessary.

IIS error message appears during installation

Microsoft Internet Information Services (IIS) 6.0 or higher, installed and running with FTP service, is a prerequisite for Insight Control Management installation. Otherwise, Insight Control Management installer blocks the installation process and an error message appears.

If this message appears during installation, perform either of the following steps as appropriate to identify and eliminate the error:

Verify the presence of IIS and DefaultAppPool by performing the following steps:

1. Click Start>Server Management to start the Server Management tool.
2. Expand Advanced Management, then expand Internet Information Services, and then expand ServerName, where ServerName is the name of the computer where you are installing Insight Control Management. Click Application Pools.
3. Verify that the DefaultAppPool is configured to run as a network service and the account credentials used by IIS to run the DefaultAppPool are valid and have enough privileges. If necessary, correct the credentials and start the Server Management tool as described in step 1.
4. If the message Service Unavailable still appears, remove and reinstall IIS. For more information about installing IIS, see the appropriate Microsoft documentation.

Verify DefaultAppPool is properly running by performing the following steps:

1. Open the Internet Explorer, enter http://localhost in the address box, and then click Enter. If the message Service Unavailable appears, perform the following steps.
2. Verify that the account credentials used by IIS to run the DefaultAppPool are valid and have enough privileges. If necessary, correct the credentials, then click Start>Server Management to start the Server Management tool.
3. If Service Unavailable still appears, install the latest Microsoft fixes, then click Start>Server Management to start the Server Management tool.
4. If Service Unavailable still appears, remove and reinstall IIS. For more information on installing IIS, see the appropriate Microsoft documentation.
Verifying environment functionality with ICE Advisor

The HP Insight Control Environment (ICE) Advisor tests and evaluates the hardware and software configuration of systems where HP SIM is installed or is being considered for installation. Test results can be used to identify issues or deficiencies with the target system that might hurt the performance of HP SIM and the associated components.

The ICE Advisor can run in either of the following methods:

- **Stand-alone**—The ICE Advisor is not installed on the target machine but runs from a local share or media. This ability to run from a local share or media enables the system without the need for installation. If you select to install the ICE Advisor, it is available from the Start>Program menu in Windows.
- **Installed**—If HP SIM is already installed, the ICE Advisor can be accessed from the HP SIM Tools menu. This accessibility enables you to run the ICE Advisor remotely. When starting the ICE Advisor from the Start>Programs menu in Windows, the main dialog box appears.

The ICE Advisor groups the various tests into two categories:

- **Pre-install**—Pre-install tests apply to conditions where HP SIM is not installed, but is being considered for installation. These tests include hardware configuration, disk space, and legacy software.
- **Post-install**—Post-install tests provide diagnostic information on conditions that might affect HP SIM or HP SIM plug-in performance.

To include pre-install items when running the ICE Advisor, perform either of the following steps:

- Select **Include Pre-Install Items**, and click **Run Now**.
- Click **Run Now** to begin the test.

Test results are provided in different ways depending on how the ICE Advisor is accessed. If you start the ICE Advisor by selecting **Start>Programs** from Windows, the results of each test appear next to the test in the main dialog box. If you access the ICE Advisor from within HP SIM, the test results appear within the HP SIM web interface.

Insight Control Management installation does not accept username, password already accepted by HP SIM

To change the username and password in this scenario:

1. If HP SIM was previously installed with a password that is not accepted by Rapid Deployment Pack or Insight Control Management, change the username and password by following the steps described in the white paper *Changing the HP SIM 5.x system name and password*, accessible at [http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00849542/c00849542.pdf?jumpid=reg_R1002_USEN](http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00849542/c00849542.pdf?jumpid=reg_R1002_USEN).

   Passwords must be alphanumeric characters or [, ], (,), !, @, -, _, $, *, comma, period, and space. Do not use a space as the last character in the account password.

   **NOTE:** If you install the Vulnerability and Patch Management Pack component before changing the CMS password, you must change the VPM password using the VPM user interface. For more information, see the *Vulnerability and Patch Management Pack User Guide*.
2. Run Insight Control Management, providing the new username and password.

Insight Control Management checks the password dynamically trying to log on in HP SIM, and the new password should be accepted.

Removing the IIS configuration in the RDP uninstaller

If you uninstall Rapid Deployment Pack, before you can reinstall it in a different path, you must manually remove some directories from IIS service that are left behind by the previous installation. To remove these directories, perform the following tasks in a command-prompt window:

1. Execute `C:`.
2. Execute `cd \WINDOWS\system32`.
3. Execute `C:\WINDOWS\system32>cscript iisftpdr.vbs /delete "MSFTPSVC/1/dslib"`.
4. Execute `C:\WINDOWS\system32>cscript isvdir.vbs /delete "w3svc/1/DSWeb"`.

PMP installation issues

This section identifies and provides solutions for commonly encountered setup and installation tasks. The following issues are included:

- PMP installation and uninstallation
- HP SIM integration
- PMP service
- PMP licensing and monitoring administration
- PMP component
- PMP database
- Windows Server 2003
## PMP installation and uninstallation

The following table describes issues and solutions that can be associated with performing an installation or uninstallation of PMP or its components.

### Table 21 Installation and uninstallation issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>During installation, the following error message appears:</td>
<td>The PMP installer cannot connect to the database server.</td>
<td>Restart the MSDE or SQL Server database processes. Perform a stand-alone PMP installation.</td>
</tr>
<tr>
<td>Failure to communicate with the database server. The installation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>was aborted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incorrect server details retrieved by PMP.</td>
<td>HP SIM and PMP are remotely installed on a system.</td>
<td>At remote MSSQL installation, ensure that the database instance that you mention is not used by any other PMP application.</td>
</tr>
<tr>
<td>The PF column is not present on the HP SIM console, yet there were</td>
<td>File system synchronization issues during installation prevent an update to</td>
<td>Manually enable the PF column by performing the following steps:</td>
</tr>
<tr>
<td>no errors during installation.</td>
<td>a HP SIM configuration file that enables the PF column to appear.</td>
<td>1. Manually stop the HP SIM and PMP services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Open <code>globalsettings.props</code> using Notepad by right-clicking <code>global-settings.props</code> (located by default in <code>C:\Program Files\Systems Insight Manager\config</code>) and selecting Open with&gt;Notepad.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Add the following two lines:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>PerformanceModuleURL=/PPA/IMPF.htm</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>PerformanceModuleInstalled=YES</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Save the file.</td>
</tr>
</tbody>
</table>
# HP SIM integration

The following table describes issues and solutions that can be associated with HP SIM integration.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When the icon in the PF column is clicked, the overall server performance status indicated in Online Analysis does not match the server performance status in the PF column.</td>
<td>The refresh interval of the Online Analysis page, which is based on sample rates, is different than the refresh interval of the PF column, which is fixed at 2 minutes. Thus, the performance status information does not match.</td>
<td>Refresh the HP SIM console and click the PF column.</td>
</tr>
</tbody>
</table>
| Clicking the icon in the PF column displays either a blank page or: Page cannot be displayed. | The Web server has entered an unrecoverable state caused by frequent restarts of applications. | Restart or close the following services and utilities and then reboot the middle-tier server.  
  - HP Foundation Agents for Servers  
  - Compaq Insight Manager XE (SNMP and DMI agents)  
  - HP WMI agent  
  - HP SIM  
  - HP Survey Utility (when installed as agent)  
  - HP Tape Storage Management Console  
  - HP Version Control Agent  
  - HP Version Control Repository Manager  
  - HP ROM Update Utility  
  - HP Insight Diagnostics  
  - Performance Management Pack  
  - System Healthcheck  
  - Enterprise Volume Manager/Business Copy  
  - Management Agents for Windows 2000  
  - HP StorageWorks Continuous Access-UI 1.0  
  - HP Storage Provisioner  
  - StorageWorks Management Appliance  
  - HP Array Configuration Utility XE  
### Table 22  HP SIM integration

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>A security alert in the Online Analysis and Offline Analysis pages displays: Security information: This page contains both secure and nonsecure items. Do you want to display the nonsecure items?</td>
<td>The Web server has entered an unrecoverable state caused by a timing problem with OpenSSL.</td>
<td>Close the window and perform a refresh of the browser to continue. For more information, see “Security Problems” in the <em>HP Systems Insight Manager Help Guide</em>.</td>
</tr>
<tr>
<td>After the PMP installation, the PMP menu might not appear on the HP SIM console.</td>
<td>The PMPTools.xml file is not executed properly during HP SIM and PMP integration.</td>
<td>To manually add the PMP menu 1  Perform either of the following procedures:   ○ From the command line, enter <code>mxtool -a -f &quot;&lt;PMP installation path&gt;:\Performance Management Pack 4\ToolsMenu\PMPTools.xml&quot;</code>   ○ Copy PMPTools.xml from &lt;PMP installation path&gt;:\Performance Management Pack 4\ToolsMenu to &lt;HP SIM installation path&gt;:\Systems Insight Manager\Setup. 2  Restart HP SIM.</td>
</tr>
<tr>
<td>The error message Page Not Found appears when launching PMP from the HP SIM menu.</td>
<td>HP SIM CMS name link is not resolved correctly on the network. Note the name used in the browser window.</td>
<td>Verify that the name resolves on the network and that it is not being affected by any proxy settings in the browser.</td>
</tr>
<tr>
<td>When HP SIM discovers systems, all Virtual Machines do not appear in the All Devices Not Available for Licensing table in the Licensing Setup page.</td>
<td>When the Tool Launch validation fails for all discovered Virtual Machines in the Verify Target Systems page.</td>
<td>To ensure that the Virtual Machines are listed in the table, perform the following steps: 1  Click the Virtual Machine listed in the All Systems page. The Systems Status page appears. 2  Click <strong>Tools and Links</strong>. 3  Click <strong>Edit System Properties</strong>. A new page appears. 4  In the Operating System Description Field, enter the name of the supported operating system. Remove unnecessary characters from the name. You must also remove the characters such registration marks. 5  Edit the Operating System Version field with the appropriate supported operating system version. 6  Click <strong>OK</strong>. 7  Select the Virtual Machine from the “All System Page” and view the details in the “All Devices Not Available for Licensing” table in the Licensing Setup page.</td>
</tr>
</tbody>
</table>
### Table 22  HP SIM integration

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When HP SIM discovers systems, all Windows and Linux Virtual Machines do not appear in the Monitoring Administration page.</td>
<td>When the System Sub Types are incorrect.</td>
<td>To resolve the issue:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click the Virtual Machine listed in the All Systems page. The Systems Status page appears.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Click <strong>Tools and Links</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click <strong>Edit System Properties</strong>. A new page appears.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Edit the System Subtype 1 field to Virtual Machine Guest.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Edit the System Subtype 2 field to MS Virtual Machine Guest. *</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. Select the Virtual Machine from the All Systems page and view the details in the Monitoring Administration page.</td>
</tr>
</tbody>
</table>

The Online Analysis page does not appear through the Diagnose menu for the monitored nodes. Occasionally

1. Go to `<HPSIM Install Path>/jboss/server/hpsim/work/jboss.web/localhost/_/org/apache/jsp/mxportal/PMP`
2. Find following files (Which ever present)
   a. `MxTmSetupLicensingConfig.jsp.class`
   b. `MxTmSetupLicensingConfig.jsp.java`
   c. `MxTmSetupLicensing.jsp.class`
   d. `MxTmSetupLicensing.jsp.java`
3. Delete all files.
4. Open Online Analysis page and then refresh the page.

* For MSVS – MS Virtual Machine Guest; For ESX – VMware ESX Guest; For GSX – VMware GSX Guest

---

### PMP service

The following table describes issues and solutions that can be associated with the PMP service.

### Table 23  PMP service issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clicking a normal, minor, or major icon in the PF column displays: HTTP Status 404, Not Found User: 01A4 Group: administrator Request: /PPA/IMPF.htm</td>
<td>PMP has terminated unexpectedly.</td>
<td>Restart PMP. The service can be restarted with the Services tool, accessed from Administrative Tools in Windows 2000, Windows XP, or Windows 2003.</td>
</tr>
<tr>
<td>The error message Bad Gateway. The proxy server received an invalid response from an upstream server appears on the Online Analysis page.</td>
<td>PMP has terminated unexpectedly.</td>
<td>Restart PMP. The service can be restarted with the Services tool, accessed from Administrative Tools in Windows 2000, Windows 2003, or Windows XP.</td>
</tr>
</tbody>
</table>
PMP licensing and monitoring administration

The following table describes issues and solutions that can be associated with licensing and monitoring administration.

**Table 24  PMP license administration issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>While logged on as Administrator, access to functions from the</td>
<td>The Unknown Performance status, Error Performance status, or Monitoring</td>
<td>To reactivate the appropriate Current User access level rights after a</td>
</tr>
<tr>
<td>Monitoring Administration page is lost and one of the following error</td>
<td>Administration page was left unattended and idle for 15 minutes or more.</td>
<td>session has expired:</td>
</tr>
<tr>
<td>messages appears:</td>
<td>The session has expired, and PMP set the Current User level to Anonymous as</td>
<td>1 Close the Unknown Performance status, Error Performance Status, or</td>
</tr>
<tr>
<td>• The Current User must have 'administrator' or 'operator' rights</td>
<td>a security precaution.</td>
<td>Monitoring Administration page.</td>
</tr>
<tr>
<td>enabled in order to access PMP administration functions.</td>
<td></td>
<td>2 Launch the page again by clicking the appropriate icon in the PF</td>
</tr>
<tr>
<td>• The Current User must have 'administrator' rights enabled in order</td>
<td></td>
<td>column of the HP SIM console or by selecting the page from the HP SIM</td>
</tr>
<tr>
<td>to access PMP licensing functions.</td>
<td></td>
<td>console toolbar.</td>
</tr>
<tr>
<td>A HP SIM-discovered server does not appear in the PMP Licensing</td>
<td>HP SIM does not discover the managed nodes using SNMP Protocol.</td>
<td>To resolve this issue:</td>
</tr>
<tr>
<td>Setup page.</td>
<td></td>
<td>1 Select “Global Protocol Settings”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Clear all the protocol settings (WBEM, SNMP, DMI, HTTP, and so on).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Run the Identify System task on the target system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 After successful completion of the task, enable only SNMP protocol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>settings from Global Protocol Settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 Rerun the Identify System task on the target system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 Perform Update server List in the License Administration page.</td>
</tr>
</tbody>
</table>
Table 24  PMP license administration issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>While attempting to license a virtual host, the following message</td>
<td>When the virtual host is not licensed by VMM.</td>
<td>To ensure that the Virtual Host is registered and licensed to VMM, complete the following procedure:</td>
</tr>
<tr>
<td>appears: Device is not licensed by VMM.</td>
<td></td>
<td>1 Select the host server on the All Systems page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Click Configure, and then select Virtual Machine Host Registration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Select Register VM Host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 Ensure that the entry of the selected virtual host appears in the Verify Target System page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 Click Next.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 Click Run Now on the Task Confirmation page. When the VM Host is registered, the following message appears:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent Registration Successful.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7 Click Deploy on the All Systems page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8 Select License Manager, and then click Virtual Machine Management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9 Click Manage License, and then select Paid license.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 Click Assign License tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 Select the Host server from Verify Target System table and then click Next.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 Select the Host server from Assigning Licenses table and then click Assign License Now.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13 The particular paid license is assigned to the selected Host server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14 Run Identify Systems (Options&gt; Identify Systems) for the selected Host server.</td>
</tr>
</tbody>
</table>
## PMP components

The following table describes issues and solutions that can be associated with PMP components.

<table>
<thead>
<tr>
<th>Table 25 PMP components</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Although monitoring has started and the proper number of samples for analysis has been collected, the Storage components icon for a monitored server remains “Unknown” in PMP Online Analysis.</td>
<td>The driver for the storage controller is not current.</td>
<td>Update the driver for the storage controller. You can get the latest driver from <a href="http://www.hp.com">http://www.hp.com</a> and the SmartStart CD.</td>
</tr>
<tr>
<td>Hardware configuration changes have been made, and the PMP session for this server has not been stopped and restarted.</td>
<td>If any hardware configuration changes are made to the monitored server, reboot the server and restart the PMP session from the middle-tier.</td>
<td></td>
</tr>
<tr>
<td>Storage Agents are not running on the monitored server.</td>
<td>Restart the Storage Agents on the monitored server with the Services tool, accessed from Administrative Tools in Windows 2000, Windows XP, and Windows 2003, or from the Control Panel in Microsoft Windows NT®.</td>
<td></td>
</tr>
</tbody>
</table>
| The Online Analysis graphical performance reports might not appear properly because of a known Internet Explorer issue. | The user attempts to review the Online Analysis graphical performance reports. | PMP has provided a utility to resolve this issue. To run the GraphFix utility from the HP SIM CMS: 1. Navigate to the PMP installation directory. The default installation directory is C:\Program Files\HP\Performance Management Pack 4, 2. Execute the following command from the command line:  

```bash
GraphFix remove
```

A message appears, confirming that the registry key has been successfully deleted. 3. Restart the HP SIM CMS when prompted. |

For more information, see the Microsoft support article at [http://support.Microsoft.com/default.aspx?scid=kb%3Ben-us%38323207](http://support.Microsoft.com/default.aspx?scid=kb%3Ben-us%38323207).

**NOTE:** Although this Microsoft article refers to Internet Explorer 5.5 SP2, this issue continues to occur with Internet Explorer 6 and later.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the PMP Online Analysis Status tab, the Storage components metrics</td>
<td>Physical and logical disk monitoring are not enabled on the monitored server.</td>
<td>Click Start&gt;Run, and then enter cmd in the dialog box. Enable physical and logical disk monitoring by entering the following at the command prompt: DISKPERF &lt; \COMPUTERNAME&gt; \Y Where \Y sets the system to start all disk performance counters when the system is restarted and &lt; \COMPUTERNAME&gt; is the name of the server on which to view or set the disk performance counters.</td>
</tr>
<tr>
<td>are all zero even though known I/O activity exists. The Windows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>physical disks cannot be traced to a logical drive. Storage component</td>
<td></td>
<td></td>
</tr>
<tr>
<td>icons appear as “Unknown” for affected components. *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No supported NICs are active.</td>
<td></td>
<td>Verify that the NIC card is supported. See the HP Insight Control</td>
</tr>
<tr>
<td>Although monitoring has been started and the proper number of</td>
<td></td>
<td>Management Support Matrix for a list of supported network adapters.</td>
</tr>
<tr>
<td>samples for analysis has been collected, the Network Connections</td>
<td></td>
<td></td>
</tr>
<tr>
<td>icon for a monitored server remains Unknown in PMP Online Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>page.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The NIC agents on the monitored server are not running.</td>
<td></td>
<td>Restart the NIC agents on the monitored server. Restart the agents</td>
</tr>
<tr>
<td>The NIC agents are running, but they collect and send invalid values</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to PMP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(PF) columns are always blue (unknown) and data cannot be logged</td>
<td></td>
<td></td>
</tr>
<tr>
<td>for that server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Even when a server is licensed and logging is started, the status</td>
<td>An internal logic error occurs on some systems.</td>
<td>Restart the session from the Monitoring Administration page.</td>
</tr>
<tr>
<td>that appear in the PF column is always blue (unknown) and data cannot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>be logged for that server.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Windows Server 2003 has physical and logical disk counters enabled by default.
PMP Database

The following table describes issues and solutions that can be associated with the PMP database.

<table>
<thead>
<tr>
<th>Table 26</th>
<th>PMP database components</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issue</strong></td>
<td><strong>Occurs when</strong></td>
</tr>
</tbody>
</table>
| When generating reports or deleting logged files, the following error message appears: | PMP is logging data, and the hard drive is out of space. | NOTE: You must be logged on as an administrator or a member of the administrators group.  
1. If no partition is available, insert another hard drive and create a new partition using the Disk Management utility. (See the Microsoft Windows Help entry on “Partition” for more information.)  
3. Select Start>Programs>Microsoft SQL Server. Click Query Analyzer to open a Query Analyzer page.  
4. Enter the login name and password.  
5. Enter the following queries and click Run:  
   Use Master  
   Go  
   Sp_detach_db 'PMP_V3_0'  
6. Copy SQL Default directory\data\PMP_V3_0'.mdf to the new partition.  
7. Copy SQL Default directory\data\PMP_V3_0_log.LDF to the new partition.  
8. Attach to the SQL server by using the following query statements in SQL Query Analyzer:  
   Sp_attach_db @dbname = N' PMP_V3_0'  
   @filename1=N'New Partition drive letter\PMP_V3_0.LDF',  
   @filename2=N'New Partition drive letter\PMP_V3_0_log.LDF'  
| PMP installation fails with a message stating that the PMP database could not be created. | The <SQL directory>\<MSDE directory>\Data folder might have .mdf and .ldf files present. This situation occurs when a database has been uninstalled.  
**NOTE:** Uninstalling the database software does not remove the user-created .mdf and .ldf files. | Manually delete the PMP .mdf and .ldf files in the <SQL directory>\<MSDE directory>\Data folder before installing the database software again. |
<p>| PMP status might be inconsistent with the mode of operation or some other unexpected behavior might occur. | When SQL server restarts. | Restart PMP. |</p>
<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No disk space is available to log PMP data in the SQL/Microsoft Date Engine (MSDE) database, and SQL events are generated in the event log.</td>
<td>This condition occurs with MSDE where a maximum database size limitation of 2 GB exists. PMP logs more information than previous versions of PMP.</td>
<td>Do not use MSDE to log PMP data.</td>
</tr>
<tr>
<td>PMP fails to establish remote Oracle® database connection and the installation fails.</td>
<td>PMP tries to connect to a database from a 64-bit Windows platform Analysis Server to PMP and HP SIM databases that is installed on a 32-bit operating system using programmatic interface (OLEDB).</td>
<td>Install PMP in Program Files\HP\ instead of the default location - Program Files (x86)\HP.</td>
</tr>
<tr>
<td>Shows blank, on the right pane of online page.</td>
<td>You can use Microsoft Internet Explore, and you keep the online analysis page open for a long duration.</td>
<td>Refresh the page or pane.</td>
</tr>
</tbody>
</table>
| Occasionally, PMP displays Unsupported Server for Integrity servers. | Occasionally | Complete the following procedure:  
1. Delete the server entry from HP SIM.  
2. Rediscover the server by enabling SNMP Protocol Settings from the Global Protocol Settings tab.  
3. Clear all other protocol settings.  
4. After discovery, click the PF column for the server or Update Server List in the Monitoring Administration page. |
The following table describes issues and solutions that can be associated with Windows Server 2003.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Occurs when</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When accessing HP SIM for the first time on a Windows Server 2003</td>
<td>The site is not accepted as a trusted site by the security settings.</td>
<td>Add the site to the trusted zone. Be aware that it lowers the security settings for all content on the HP SIM pages.</td>
</tr>
<tr>
<td>system, the following message appears:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content from Web site listed below is being blocked by Internet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explorer security configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>as a ProLiant server.</td>
<td>before HP SIM can collect and classify information about ProLiant servers</td>
<td>1 From Service, right-click <strong>SNMP service</strong>, and click <strong>Properties</strong>.</td>
</tr>
<tr>
<td></td>
<td>from the Management Agents.</td>
<td>2 Click the <strong>Traps</strong> tab, and be sure that public is entered as the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Community Name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Click the <strong>Security</strong> tab, be sure that Accept SNMP packets from any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hosts is selected, and then add the following Community Names:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Community</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Public</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Private</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Read Only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Read Create</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, see “SNMP Communities and ProLiant Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agents” section in the white paper at ftp://ftp.compaq.com/pub/</td>
</tr>
</tbody>
</table>
Vulnerability and Patch Management Pack troubleshooting

This section identifies and provides solutions for commonly encountered Vulnerability and Patch Management Pack issues, as well as answers to frequently asked questions. The following sections are included:

- Vulnerability and Patch Management Pack installation and configuration
- Uninstalling the Vulnerability and Patch Management Pack
- Vulnerability scans
- Patches and configuration fixes
- HP SIM integration

Vulnerability and Patch Management Pack installation and configuration

Viewing Vulnerability and Patch Management Pack installation logs

The Vulnerability and Patch Management Pack installation logs, which list the details of the installation of each Vulnerability and Patch Management Pack component, are located at %HOMEDRIVE%\vpmssetuplogs, where HOMEDRIVE is usually the C drive. You can view the following logs:

- vmpsetup.log—Contains log information from the main installer, including calls and result codes from the execution of component installers
- vmpsrvsetup.log—Contains log information about the creation of the Vulnerability and Patch Management Pack directories and menus in the VPM server
- vmpsimsetup.log—Contains log information from the HP SIM component installation
- RCS.log—Contains information about the installation of the Radia Configuration Server, which manages vulnerabilities based on policies established by HP SIM
- RPS.log—Contains information about the installation of the Radia Proxy Server, which is used as the central patch repository
- RMS.log—Contains information about the installation of the Radia Messaging Server, which is a messaging service used to communicate Vulnerability and Patch Management Pack status information
- RPM.log—Contains information about the installation of the Radia Patch Manager (Server), which acquires security patches from the Internet, loads them into the Radia Configuration Server, and synchronizes this information in the database
- RMP.log—Contains information about the installation of the Radia Management Portal, which is used to initiate the installation of the VPM Patch Agent and perform Vulnerability and Patch Management Pack actions on remote systems
- Radiawrp.log—Contains an installation summary of the previous five components

Vulnerability and Patch Management Pack installation updates MDAC and MSDE

If MSDE or files used by MSDE are not up-to-date, files are updated during the Vulnerability and Patch Management Pack installation. The server is rebooted after updated files are installed. In this situation, the Vulnerability and Patch Management Pack installation must be restarted.
An error occurs when installing MSDE files from a Remote Desktop session

Install Vulnerability and Patch Management Pack using the system console instead of a Remote Desktop session. For additional information, see http://support.microsoft.com/default.aspx?scid=kb;en-us;246694&sd=tech.

Vulnerability and Patch Management Pack installation fails with “There Are No Configuration Files” error

This error occurs because the metabase, the configuration files used for IIS, has been corrupted. To resolve:
3. Locate STATScanner at LM\W3SVC\1\ROOT, and then click Delete.

“STAT Scanner WSI Requires IWAM and IUSR” error occurs during Vulnerability and Patch Management Pack installation

This occurs when the server name has been changed after IIS was installed. IIS must be uninstalled and reinstalled before Vulnerability and Patch Management Pack can be installed.

Installation fails with “Product RMS not installed: Service RMS error. The specified service does not exist as an installed service (0x424)” message

If the password of the account used to install Vulnerability and Patch Management Pack contains curly braces, “{” or “},” the Radia component installation fails. To correct this, either complete the following steps to temporarily change the install account password or create a new local account with administrator privileges to use to perform the installation.
1. Change the password to remove the invalid characters.
3. Right-click HP Systems Insight Manager, and then select Properties.
4. Click the Log On tab, and then update with the new password.
5. Click the General tab, and then click Stop>Start to restart the HP SIM service.
6. Right-click IIS Admin Service, and then select Restart. To confirm, click Yes.

Proceed with the Vulnerability and Patch Management Pack installation. If necessary, the installation account credentials can be changed back after the installation completes. Repeat steps 2 through 6 after the password has been changed, and then to update the VPM password, see the “Updating VPM credentials using the Change VPM Credentials Utility” section in this guide.
Vulnerability and Patch Management Pack installation fails

- Be sure the VPM server can effectively communicate with other networking components, such as the database and HP SIM server (if separate).
- If the VPM server has multiple IP addresses, be sure Name Resolution is used for both.
- If IPv6 is enabled, uninstall from the network interface card being utilized for Vulnerability and Patch Management Pack communication.
- If the Vulnerability and Patch Management Pack installation was attempted multiple times, reboot before attempting the installation again.

Cannot modify VPM acquisition settings to acquire updates from a local repository

A patch acquisition must have already been run using the VPM Acquisition Utility and saved to the designated directory before VPM acquisition settings can be modified to acquire updates from a local repository. For information about acquiring patches using the VPM Acquisition Utility, see the “Performing additional Vulnerability and Patch Management Pack post-installation configuration tasks” section.

Required open ports

The following ports must be open on target systems to allow successful scanning with Vulnerability and Patch Management Pack:

- **TCP 22**—SSH
- TCP 135, 137, 138, 139, 443, and 445—NetBIOS and SSL, used by the Vulnerability and Patch Management Pack scanning components
- TCP 2301 and 49400—HP Management Agents
- TCP 3463, 3464, 3466, and 3465—Used by Vulnerability and Patch Management Pack patching components

The following ports must be open on the VPM server:

- TCP 80—HTTP Web server, if an HTTP connection is used between the VPM and HP SIM servers (TCP 443 must be open if an HTTPS connection is used)
- TCP 445—MSDE named pipes communications
- UDP 1433, 1434—MSDE Shared Instance Support
- TCP (variable)—MSDE TCP/IP communications. This port, assigned at random by MSDE during installation, can be identified by selecting Start>Run, entering `svrnetcn.exe`, and clicking OK. From the Server Instances menu, select `Computername\Dovico`. In the Enabled Protocols list, select `TCP/IP>Properties`. The port number appears. The port number can be changed at this time, if necessary.
The following ports are used by HP SIM and must be open:

- TCP 22—SSH
- UDP 161—SNMP
- UDP 162—SNMP trap
- TCP 280—HTTP
- TCP 5989—WBEM/WMI Mapper secure
- TCP 50000—HTTPS
- TCP 50001—Secure SOAP
- TCP and UDP 53—DNS

The following ports are used by the Virtual Machine Management Pack and must be open:

- 1125
- 1126
- 40420

**Modifying firewall configuration settings**

To ensure that Vulnerability and Patch Management Pack can obtain updates, be sure that your firewall is configured for access to ftp://ftp.hp.com/pub/essentials/vpm/.

**Configuring a DNS server**

If no DNS server exists in the server network, update the host files on both the HP SIM and VPM servers (if separate) with the IP and Network Naming. These files are located at C:\Windows\system32\Drivers\etc. The target systems must be able to resolve the VPM server name to an IP address.

The server host name where HP SIM and VPM are installed must be correctly configured for name resolution and reverse lookup. To determine if DNS is properly configured, use the nslookup command, passing both the host IP address and the fully qualified hostname.
If using DHCP, verify the following configurations in the advanced TCP/IP properties:

Be sure that the DNS suffix for this connection field has the correct DNS suffix and that both the Register this connection’s addressees in DNS and Use this connection’s DNS suffix in DNS registration checkboxes are selected.

**All target systems do not have the same administrator credentials**

For target systems that have individual administrator credentials, configure WBEM credentials individually to enable access to these target systems.

1. From within HP SIM, select Options>Protocol Settings>System Protocol Settings.
2. Select the system to configure, and then click Apply.
3. Enter the appropriate WBEM credentials, and then click Run Now.

**Multiple VPM servers**

Target systems cannot be scanned and patched by multiple VPM servers. The deployed VPM Patch Agent is set up to respond to only one VPM server.

**Administrator credentials have been changed**

If the administrator credentials have been changed for target systems, the WBEM credentials must be reconfigured. To reconfigure Global Protocol Setting, select Options>Protocol Settings>Global Protocol Settings.
Changing the IIS IWAM user name and password

HP recommends that the IWAM_hostname and IUSR_hostname accounts not be modified after they are installed by IIS. Modifying these accounts corrupts the rights and security privileges of Vulnerability and Patch Management Pack and IIS components.

For information about backing up and restoring the ISS Metabase, see http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/131b609d-ff3a-488f-a8dd-13044fa623a1.mspx.

The IIS Certificate has expired and the Vulnerability and Patch Management Pack connection must be reconfigured to use an HTTP connection

HP recommends using a secure HTTPS connection between the HP SIM server and the VPM server, when these components are installed on separate servers. However, if you currently have an HTTPS connection that must be reconfigured to HTTP, then perform the following steps:

1. Remove the SSL certificate from IIS.
2. Change the IIS configuration to accept both HTTP and HTTPS connections:
   a. Open Internet Information Services Manager.
   b. Locate STATScanner under Default Web Site on the local computer.
   c. Right-click STATScanner, and then select Properties.
   d. Click the Directory Security tab.
e. In the Secure Communications field, click **Edit**.

f. Clear the **Require secure channel (SSL)** option, and then click **OK>OK**.
Radia uses installation account instead of local account

To accommodate a security modification contained in Windows 2003 SP1, the Vulnerability and Patch Management Pack installer modifies the Windows service running httpd (Radia Integration Server) to use the installation account rather than the Local System account. In addition, the installation account is modified to run as a service.

Uninstalling Vulnerability and Patch Management Pack

Use either of the following methods to uninstall Vulnerability and Patch Management Pack. The Vulnerability and Patch Management Pack uninstallation must be performed from the VPM server.

Vulnerability and Patch Management Pack scan results can be retained after uninstallation. The last scan performed can be accessed from the VPM column. If you choose to delete scan results, the VPM column is set to an initialized state.

**IMPORTANT:** Be sure that no vulnerability scans, patch deployments, or patch acquisitions are running. Close all browsers before attempting to uninstall Vulnerability and Patch Management Pack.

**IMPORTANT:** Vulnerability and Patch Management Pack licenses are not removed from target systems when Vulnerability and Patch Management Pack is uninstalled.

To uninstall with the Vulnerability and Patch Management Pack uninstaller:

1. Select **Start>Programs>HP ProLiant Essentials Vulnerability and Patch Management>Uninstall Vulnerability and Patch Management.**
2. When prompted, select whether to remove the Vulnerability and Patch Management Pack data stored on the HP SIM server, such as scan reports and Vulnerability and Patch Management Pack tasks. If data is removed, then it is cleared from the HP SIM systems list.
3. When prompted, select whether to remove the patch database.
4. When uninstall is complete, the HP SIM service is automatically restarted.
5. Delete the VPM directory. The default location is: C:\Program Files\HP\VPM.

To uninstall VPM from the Control Panel:

1. Select **Add or Remove Programs.**
2. Select **HP Vulnerability and Patch Management>Change/Remove.**
3. When prompted, select whether to remove the Vulnerability and Patch Management Pack data stored on the HP SIM server, such as scan reports and Vulnerability and Patch Management Pack tasks. Data that appears in the HP SIM systems list is cleared if data is removed.
4. When prompted, select whether to remove the patch database.
5. When uninstall is complete, the HP SIM service is automatically restarted.
6. Delete the VPM directory. The default installation location is: C:\Program Files\HP\VPM.
Remaining Vulnerability and Patch Management Pack files

A Vulnerability and Patch Management Pack uninstallation does not remove all Vulnerability and Patch Management Pack files from the server. The following files remain after uninstallation:

- C:\Novadigm\ManagementAgent\nvdkit.exe
- C:\Novadigm\ManagementAgent\rma.tkd
- C:\Novadigm\ManagementAgent\rma.log
- C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\VPM\column\vpmcolmain.jsp
- C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\VPM\column\vpmbase.html
- C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\home\STATScanner ¹
- C:\Program Files\Microsoft SQL Server\MSSQL$VPMMSSQL\Data\radiadb.mdf ²
- C:\Program Files\Microsoft SQL Server\MSSQL$VPMMSSQL\Data\radiolog.ldf ²

¹ The VPM Results directory only remains if you select to retain Vulnerability and Patch Management Pack data during the uninstallation.
² These files only remain if you select to retain the patch database during uninstallation.

Reinstalling Vulnerability and Patch Management Pack

If an updated version of Vulnerability and Patch Management Pack is installed after a previous version has been uninstalled, the entitlement list could be lost for all managed target systems. To prevent this, be sure that you uninstall and reinstall the updated VPM Patch Agent to all target systems.

Vulnerability scans

Vulnerability and Patch Management Pack cannot access target systems

If Vulnerability and Patch Management Pack cannot perform accurate scanning on a target system because of access problems, verify the following information depending on the target operating system.

Windows

- The account used to scan the target system is a member of the Administrator group or Domain Administrator group for that system.
- Client for Microsoft Networks is installed and enabled.
- Vulnerability and Patch Management Pack has share-level access to all target systems.
- Remote Registry Service is started.
- File and Printer Sharing protocol is installed and enabled.
- Default Administrative Shares are enabled.
- Server Service is started.
- Simple File Sharing is disabled.
- The Internet Connection Firewall is configured correctly or disabled, and the target system is configured to respond to ping commands.
- The Computer Name/Domain network component is defined.
**Windows XP**

Verify that Simple File Sharing is disabled on Windows XP Professional machines that are not part of a domain. Simple File Sharing is enabled by default, disabling network access to Administrative shares on the machine.

**Windows VPM server**

STAT scanner cannot connect to HP SIM if the file, msxml3.dll, is not registered on the Windows XP system.

1. Execute the following command at the command prompt to verify the existence of the file:
   ```cmd
   dir %SystemRoot%\system32\msxml3.dll.
   ```

2. If the file is not registered, execute the following command at the command prompt to force the registration:
   ```cmd
   regsvr32 %SystemRoot%\system32\msxml3.dll
   ```

The following message appears after successful registration:

```
RegSvr32

DllRegisterServer in C:\WINDOWS\system32\msxml3.dll succeeded.

OK
```

Also, ensure that the IWAM_xxx account has adequate privileges to function properly. Appropriate file permissions and Microsoft Windows NT registry permissions must exist for the resources to function properly. For examples, see the following screen.
Configure file permissions on all necessary DLLs. Configure Windows NT Registry permissions on the following:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\STAT Scanner
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\STAT Scanner WSI

Linux target systems

- TCP/IP network protocol is enabled.
- SSH is enabled and listening on the default port 22.
- Vulnerability and Patch Management Pack includes PuTTY SSH client and uses the plink session command and PSCP secure copy, as well as SFTP secure file transfer commands. Both protocols 1.5 and 2.0 are supported if they are correctly installed and functioning on the target system. To determine which protocol is running, telnet to port 22 on the target system, read the return banner, and then press Enter.
  - SSH-1.5—Only protocol 1.5 is supported.
  - SSH-1.9—Protocol 1.5 and 2.0 are supported. Protocol 1.5 is attempted first.
  - SSH-2.0—Only protocol 2.0 is supported, the newest and preferred session protocol.

Scan reports cannot be viewed

If scan reports cannot be viewed in .pdf format because Adobe Acrobat cannot be launched, perform the following procedure:

1. From Internet Explorer, select Tools>Internet Options.
2. Click the Advanced tab, and then scroll to Security.
3. Clear the Do not save encrypted pages to disk option, and then click OK.

For more information, see http://support.microsoft.com/default.aspx?scid=kb;en-us;812935&Product=ie600.

A scan was submitted but never started

All target systems scanned by Vulnerability and Patch Management Pack must have an IP address that appears in the HP SIM console. If a scan is requested for a target system with no IP address, the scan does not run and an internal error is generated. Be sure that all target systems being scanned have IP addresses that appear in the HP SIM console.

Scan results are inaccurate because of overlapping tasks

When scheduling vulnerability scans and patches, be sure the two processes do not overlap. Allow adequate time for a vulnerability scan to complete before starting a patch. If a patch deployment runs during a vulnerability scan, the scan results might be inaccurate or the target systems might reboot during the scan.

Do not schedule patch acquisition tasks to run while vulnerability scans are running. Patch acquisition tasks cause vulnerability scans to abort.
Current patch information is not displayed in scan reports

Scan definition updates are available a few days after the release of patches. You might have a patch in your patch repository that does not appear in your scan results. You can apply the patch without a scan. The VPM Patch Agent will not apply patches that are not appropriate. With the new patch reports, you can also use the Validate VPM Patch Agent operation to determine where patches are needed. This operation applies to patches only. The VPM Patch Agent does not report on non-patch security vulnerabilities.

Patches and configuration fixes

VPM Patch Agent installation fails

The VPM Patch Agent is automatically deployed when systems are licensed to allow patches to be applied to the systems. If a server type is identified as Unknown or Unmanaged with no identified operating system in the HP SIM console, Vulnerability and Patch Management Pack automatically attempts to deploy the VPM Patch Agent for Windows systems. The VPM Patch Agent deployment fails on Linux systems, and event details display an error.

To deploy the VPM Patch Agent to target systems, see the “Deploying the VPM Patch Agent” section. Be sure that the Red Hat library, compat-libstdc++, is installed on Red Hat target systems.

The VPM Patch Agent installation can also fail because the WBEM credentials are not configured properly to allow Vulnerability and Patch Management Pack to access target systems. For information about configuring WBEM credentials, see the “Performing an Insight Control Management integrated installation” section.
A patch acquisition was started, but no patches are seen

A patch acquisition can take quite a bit of time the first time it is run. It is not unusual for the acquisition to take more than four hours, depending on how many operating systems are selected for download and the speed of the Internet connection.

Progress of the acquisition can be monitored at:
C:\Program Files\HP\VPM\Radia\IntegrationServer\logs\patch-acquire.log.

If the log file indicates that no patches are being acquired and there is a proxy server in the environment, be sure you have properly configured Vulnerability and Patch Management Pack to access the proxy server by selecting Options>Vulnerability and Patch Management>Settings. In addition, the proxy server must be configured to allow both HTTP and FTP traffic.

If the patch-acquire.log is not being updated, the acquisition process might be hung. Search the patch-acquire.log for the start of the last logged process id. Stop the nvdkit.exe with that process id running on your VPM server. This action terminates the current acquisition and allows the next acquisition to run.

HTTP 300 errors received during patch acquisition

Patch acquisition can generate events containing HTTP 300 errors for some older Microsoft patches, such as:

Error downloading patch data for Bulletin MS02-050 at URL http://www.microsoft.com/ntserver/terminalserver/downloads/critical/q329115/default.asp error code 300

This message occurs because the Microsoft information pertaining to the patch location is incorrect and the patch cannot be downloaded. HP is working to correct the metadata at the HP/Radia website for these older patches, however this is ongoing maintenance. These corrections will automatically be downloaded each time a patch acquisition is run. No updates are needed to Vulnerability and Patch Management Pack.

Patches appear in a scan report but are not successfully deployed

This can occur in the following situations:

- A vulnerability scan has identified vulnerabilities, patches were selected for deployment based on the scan, and one or more of the selected patches were not located in the patch repository. Generally, some of the patches will install successfully, while others do not install for an extended time. Patches might not be available in the patch repository because all of the necessary operating systems were not selected for patch acquisition or only some of the patches have been acquired.
- The VPM Patch Agent has not been successfully installed on the system being patched.
- A patch deployment is attempted on a system for which the patch is not applicable. Vulnerability and Patch Management Pack applies patches to target systems based on the operating system characteristics and patch vulnerabilities. For example, a patch cannot be deployed when a Red Hat patch is selected for deployment on a Windows target system.

Check for missing patches

Be sure that a patch acquisition has been selected for all operating systems in the server environment. Different Microsoft patches can exist for each operating system associated with an advisory. To validate if a patch has been acquired, click the advisory link to the operating system vendor. The patches for each operating system are listed. Check the C:\Program Files\HP\VPM\Radia\IntegrationServer\Data\Patch\Microsoft\<bulletin number> directory to see if each patch has been acquired.
Check the file `C:\Program Files\HP\VPM\Radia\IntegrationServer\Logs\patch-acquire.log` for a history of the last patch acquisition, including any errors. Patches downloaded through HTTP might have been acquired successfully, but those requiring FTP are failing. If this occurs, validate the proxy and firewall settings to be sure they are configured properly to enable FTP traffic.

**Validating VPM Patch Agent installation**

Check the VPM events to see if a successful Installed VPM Patch Agent event exists for the system to be patched. If no event is present or if a Failed VPM Patch Agent Install event exists, select `Deploy>Vulnerability and Patch Manager>VPM Patch Agent` to deploy the agent.

After the VPM Patch Agent installation and patch acquisition have been verified, reinitiate the patch installation by selecting `Deploy>Vulnerability and Patch Manager>Validate Installed Patches`.

**Patch installation status reports are not current or do not match information that appears in scan reports**

Information that appears in patch reports is obtained during the most recent patch deployment task. If this information is not current, update the patch installation status by validating installed patches. For information, see the “Validating installed patches” section in this guide.

**Other tools report that a Windows system is patched, but Vulnerability and Patch Management Pack reports patches needed**

Many other tools read the registry to determine if a patch is installed. In many cases, when a patch installation fails, the registry is updated while the files remain unchanged. Vulnerability and Patch Management Pack verifies that both the files and registry keys have been updated.

**Patch source for vendor patches is Microsoft* or Red Hat* **

To determine patch applicability, Vulnerability and Patch Management Pack might enhance patch detection criteria to be more precise than vendor information. These patches appear with an asterisk in the Patch Source column. HP does not support itself.

**Multiple events listed in HP SIM for patch deployments**

Patch deployments create multiple events in HP SIM. There is a start event, a completion event, and a patch current status event. The patch current status event evaluates the status of the patches after the reboot has been completed.

**STAT Scanner update error listed in the HP SIM event log**

If STAT Scanner cannot access certain necessary files during a patch acquisition scanner update, a 3010 error appears in the HP SIM event log. The file update will be completed the next time a reboot is performed.

**Radia internal error listed in the HP SIM event log**

A generic Radia internal error appears in the HP SIM event log if the patch repository is viewed before a patch acquisition had been performed.
“Abuse of Service” error occurs when attempting to acquire Red Hat patches

The Red Hat network might be disabled if the network determines that patches have been acquired too frequently. To resolve this issue, delete the registered system from the Red Hat network Web interface at https://rhn.redhat.com. Recreate the Red Hat credentials on the Red Hat server, and then copy to the VPM server.

Validate Installed Patches event does not complete

Certain Vulnerability and Patch Management Pack events cannot complete successfully until after a system has been scanned and patched at least one time. Be sure a system has been scanned and patched before attempting to validate installed patches.

HP SIM integration

The tool menus might not appear after a Vulnerability and Patch Management Pack installation for any of the following reasons:

• The HP SIM user does not have appropriate privileges to access the menus. If a new HP SIM user cannot view the Vulnerability and Patch Management Pack menus, be sure that the user is authorized for All Tools or VPM Tools in Options>Security>Users and Authentication.

• A successful installation of Vulnerability and Patch Management Pack requires the user to have CMS administrative privileges because changes are made to the HP SIM core and the tool menus.

• When installing Vulnerability and Patch Management Pack, you must use the credentials previously used when installing HP SIM. Failure to do so results in an incorrect installation. Also, the user name will not have appropriate privileges. Be sure the CMS user has privileges (toolbox and authorizations) to use Vulnerability and Patch Management Pack. If the authorization is not correct, the menus do not appear. To correct this issue, uninstall Vulnerability and Patch Management Pack and reinstall using the correct credentials. Be sure the CMS user that will be using Vulnerability and Patch Management Pack has appropriate privileges. This can include having authorization for a toolbox containing the Vulnerability and Patch Management Pack tools.

• The Vulnerability and Patch Management Pack installation failed. Installation errors appear during installation and in the log files.
9 Technical support

HP offers a number of software support services, many of which are provided to our customers at no additional charge.

- **Software Technical Support and Update Service**—Insight Control suites and select ProLiant Essentials software products include one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems. The service also provides access to software updates and reference manuals either in electronic form or on physical media as they are made available from HP. (Customers who purchase an electronic license to use are eligible for electronic updates only.) With this service, Insight Control and ProLiant Essentials customers will benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see [http://www.hp.com/services/insight](http://www.hp.com/services/insight).

Registration for Software Technical Support and Update Service:

There are two methods for registering:

- If you received a license entitlement certificate, automated registration for this service will take place upon online redemption of the license certificate/key.
- If the license information you received for your product instructs you to register for Software Technical Support and Update Service, follow the instructions so that you will be eligible for telephone support and product updates.

How to Use Your Software Technical Support and Update Service:

Once registered, you will receive a service contract in the mail containing the Customer Service phone number and your Service Agreement Identifier (SAID). You will need your SAID when calling for technical support. Using your SAID, you can also go to the Software Update Manager (SUM) web page to view your contract online and elect electronic delivery for product updates.

- **Warranty**—HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight Control Management, HP Systems Insight Manager, and ProLiant Essentials products.

- **Join the discussion**—The HP Support Forum is a community-based, user-supported tool for HP customers to participate in discussions amongst the customer community about HP products. For discussions related to Insight Control and ProLiant Essentials software, see the “Management Software and System Tools” area.

- **Software and Drivers download pages**—These pages provide the latest software and drivers for your ProLiant products.

- **Management Security** ([http://www.hp.com/servers/manage/security](http://www.hp.com/servers/manage/security))—HP is proactive in its approach to the quality and security of all its management software. Be sure to check this website often for the latest downloadable security updates.

- **Obtain the latest SmartStart Release** ([http://www.hp.com/servers/smartstart](http://www.hp.com/servers/smartstart))—The SmartStart, Management, and Firmware CDs are now freely available for download following a simple registration from the SmartStart website. If you wish to receive physical kits with each release, you can order single release kits from the SmartStart website. To receive proactive notification when SmartStart releases are available, subscribe to Subscriber’s Choice at [http://www.hp.com/go/subscriberschoice](http://www.hp.com/go/subscriberschoice).

HP Installation and Startup Service for
HP BladeSystem infrastructure

For initial installation and setup, HP offers HP Installation and Startup Service for HP BladeSystem infrastructure. This service provides the installation and configuration of an HP BladeSystem implementation, including installation of the HP BladeSystem enclosure and server hardware, software deployment, and manageability enablement.

This service meets the needs of most HP BladeSystem customers, and requires two days for completion. For more advanced requirements, customized installation is available.

For more information about this service, see ftp://ftp.hp.com/pub/services/servers/info/hp_bladesystem_install_startup_datasheet.pdf.

HP also offers ProLiant Essentials Installation and Startup Services. For more information, see http://h20219.www2.hp.com/services/cache/43768-0-0-225-121.aspx.

Where to go for additional help

In addition to this guide, the following resources are available:

- http://www.hp.com/go/insightcontrol
- HP Insight Control Management Installation Checklist
- HP Insight Control Management Quick Setup Poster
- HP Insight Control Management Release Notes
- HP Insight Control Management Support Matrix
- The Documentation tab on the Insight Control Management DVD for individual documentation for each component

For more information about HP SIM, see the following resources:

- http://www.hp.com/go/hpsim
- HP Systems Insight Manager Installation and Configuration Guide for HP-UX
- HP Systems Insight Manager Installation and Configuration Guide for Linux
- HP Systems Insight Manager Installation and Configuration Guide for Microsoft Windows
- HP SIM User Guide

For more information about Extensions for HP SIM on Microsoft Windows, see the following resources:


For more information about HP BladeSystem and appropriate firmware and software, see http://www.hp.com/go/bladesystemupdates.

For more information about HP Insight Power Manager, see the following resources:

- [http://www.hp.com/go/ipm](http://www.hp.com/go/ipm)
- **HP Insight Power Manager User Guide**

For more information about HP iLO 2 Advanced Pack and Select Pack, see the following resources:

- [http://www.hp.com/go/ilo](http://www.hp.com/go/ilo)
- **HP Integrated Lights-Out 2 User Guide**

For more information about HP Rapid Deployment Pack, see the following resources:

- [http://www.hp.com/go/rdp](http://www.hp.com/go/rdp)
- **HP ProLiant Essentials Rapid Deployment Pack Installation Guide**
- **HP ProLiant Essentials Rapid Deployment Pack Planning Guide**
- **HP ProLiant Essentials Rapid Deployment Pack User Guide**
- **HP Rapid Deployment Pack Knowledge Base at [http://www.hp.com/servers/rdp/kb](http://www.hp.com/servers/rdp/kb)** (Regularly updated troubleshooting information, frequently asked questions, and specific how-to procedures are available on this site.)

For more information about HP Performance Management Pack, see [http://www.hp.com/go/pmp](http://www.hp.com/go/pmp)

For more information about HP Vulnerability and Patch Management Pack, see [http://www.hp.com/go/vpm](http://www.hp.com/go/vpm)

For more information about HP Virtual Machine Management Pack, see the following resources:

- **HP ProLiant Essentials Virtual Machine Management Pack Support Matrix**

For more information about Integrity Essentials for HP-UX and Linux, see the following resources:

- [http://www.hp.com/go/integrityessentials](http://www.hp.com/go/integrityessentials)
- [http://www.hp.com/go/managehpux11i](http://www.hp.com/go/managehpux11i)
- [http://www.hp.com/go/integritylinux](http://www.hp.com/go/integritylinux)

For more information about managing the HP BladeSystem Integrity BL860c blade, see the following resources:

- [http://www.hp.com/go/BL860c](http://www.hp.com/go/BL860c)

**NOTE:** Beginning with this release, Performance Management Pack and Vulnerability and Patch Management Pack documentation are incorporated into Insight Control Management documentation.
HP contact information

For the name of the nearest HP authorized reseller:

- In the United States, see the HP U.S. service locator at http://www.hp.com/service_locator.
- In other locations, see Contact HP Worldwide at http://welcome.hp.com/country/us/en/wwcontact.html.

For HP technical support:

- In the United States, for contact options see Contact HP United States at http://welcome.hp.com/country/us/en/contact_us.html. To contact HP by phone, call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored. When prompted, say “Insight Manager.”
- In other locations, see Contact HP Worldwide at http://welcome.hp.com/country/us/en/wwcontact.html.
Appendix A Performance Management Pack reference matrix

This appendix details the measurement parameters evaluated by the performance management component for the various components of a system configuration. A brief description of each parameter that appears, in both the Status and Inventory view is provided.

Static analysis

The following configuration information is gathered by hardware discovery and analyzed by PMP to display the performance status of server components:

- Processors—For example, a mix of processors with different cache sizes
- Memory
- Network connections—For example, the ability to detect a NIC running at reduced speed or in half duplex mode
- Storage—For example:
  - A fast physical disk drive plugged into an enclosure that cannot support the maximum I/O capabilities of the drive
  - A slow physical drive plugged into a fast enclosure
  - A RAID consisting of a mix of drive speeds
  - A RAID consisting of a mix of drive capacities
- Host buses—For example:
  - Bus overloading
  - Too many I/O resources plugged into the same bus on a multi-bus server
**ATA disk array**

The following information is provided for an ATA disk array.

**ATA Disk Array Status**

- **Reads/Sec**—The number of reads from this ATA disk array each second
- **Writes/Sec**—The number of writes to this ATA disk array each second
- **Read MBytes/Sec**—The average number of megabytes read from the ATA disk array each second
- **Write MBytes/Sec**—The average number of megabytes written to the ATA disk array each second
- **Millisec/Read**—The average time for each read to complete
- **Millisec/Write**—The average time for each write to complete
- **Queue Length**—The average number of concurrent requests between the server and this ATA disk array, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (disk or IDE controller)

ATA disk array performance is not evaluated because the performance of an array is determined by the performance of the disks in the array.

**ATA Disk Array Inventory**

- **Array configuration**
  - Displays the total capacity of the disk array
  - Displays where the disk array is defined (which IDE controller)
  - Displays the RAID level and striping factor (if applicable) for the array
- **Hard Drives**—Lists the ATA disks that constitute the disk array
- **Spare Drives**—Lists the ATA disks that are designated as spares

**ATA disk**

The following information is provided for an ATA disk.

**ATA Disk Status**

- **Reads/Sec**—The number of reads from this ATA disk each second
- **Writes/Sec**—The number of writes to this ATA disk each second
- **Read MBytes/Sec**—The average number of megabytes read from the ATA disk each second
- **Write MBytes/Sec**—The average number of megabytes written to the ATA disk each second
- **Millisec/Read**—The average time for each read to complete
- **Millisec/Write**—The average time for each write to complete
- **Queue Length**—The average number of concurrent requests between the server and this ATA disk (Queue Length is the primary indicator of ATA disk performance, whether the disk is part of an array)
ATA Disk Inventory

- Disk Information—Displays a description of the drive, including the hard drive model number
- Configuration Information
  - Provides a summary of the drive configuration
  - Displays the name of the IDE controller to which it is attached
  - Indicates to which disk array the disk belongs (if applicable)

Drive array

The following information is provided for a drive array.

Drive Array Status

- Reads/Sec—The number of reads from each drive in the drive array each second
- Writes/Sec—The number of writes to each drive in the drive array each second
- Read MBytes/Sec—The average number of megabytes read from each drive in the drive array each second
- Write MBytes/Sec—The average number of megabytes written to each drive in the drive array each second
- Millisec/Read—The average time for each read to complete
- Millisec/Write—The average time for each write to complete
- Queue Length—The average number of concurrent requests between the server and each drive in the drive array, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (drive or controller)

Drive Array Inventory

- Array Configuration—Displays on which Smart controller the drive array is defined and the number of array logical drives implemented on the array
- Hard Drives—Lists the SCSI drives constituting the disk array
- Spare Drives—Lists the SCSI drives designated as spares
External storage enclosure

The following information is provided for an external storage enclosure.

External Storage Enclosure Status

- Transfers/Sec—The average number of transfers (reads and writes) on this external storage enclosure each second
- MBBytes/Sec—The average number of megabytes transferred on this external storage enclosure each second
- Millisec/Transfer—The average time to complete a transfer to and from the selected external storage enclosure
- Enclosure Queue—The average number of transfer requests (reads and writes) waiting to be serviced by the external channel storage enclosure

PMP does not evaluate the performance of external storage enclosures

External Storage Enclosure Inventory

- Enclosure Configuration—Displays the type or model, name, and serial number of the external storage enclosure.
- Controller—Displays the name and model of the enclosure and whether it is operating with redundant controllers. If a redundant controller is configured, then both standby and active controllers are listed (if redundancy is not configured, only active controllers are listed).
- Host Bus Adapters (HBAs)—Lists the HBAs used to attach the enclosure to the server.
- Windows/Linux Physical Disks—Lists the logical volumes defined in the storage enclosure.

Fibre Channel host bus adapter

The following information is provided for a Fibre Channel HBA.

Fibre Channel Host Bus Adapter Status

- Transfers/Sec—The average number of transfers on the selected HBA each second
- MBBytes/Sec—The average number of megabytes transferred on the selected HBA each second
- Millisec/Transfer—The average time to complete a data transfer between the server and the storage attached to the selected HBA
- Queue Length—The average number of concurrent requests between the server and this HBA, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting
- Port Utilization %—The average utilization of the Fibre Channel port on this adapter.

Performance is determined by comparing the MBBytes/Sec with the theoretical throughput (1 or 2 GB/s) of the HBA.
Fibre Channel Host Bus Adapter Inventory

- **Host Bus Adapter Configuration**—Displays the name of the HBA and the supported and negotiated PCI protocol (bus speed) of the HBA
- **Fibre Channel Enclosures**—Displays all enclosures assigned to the HBA, the names of the enclosures, and the enclosure models
- **Windows/Linux Physical Disks**—Displays all physical disks traced from the server to the logical drives on the accessible enclosures

**Host buses**

The following information is provided for host buses.

**Host Buses Status**

- **Host Bus MBytes/Sec**—The average number of megabytes transferred over the host buses each second

**Host Buses Inventory**

- **Bus Configuration**—Displays a summary of each PCI or PCI-X bus on the server with the PCI/PCI-X slots and the I/O expansion boards installed in each slot

**IDE channel**

The following information is provided for an IDE channel.

**IDE Channel Status**

- **MBytes/Sec**—The average number of megabytes transferred on this IDE channel each second (the sum of the MBytes/Sec for all ATA disks on this channel)
- **Transfers/Sec**—The average number of transfers on this IDE channel each second (the sum of the Transfers/Sec for all ATA disks on this channel)
- **Channel Queue**—The average number of transfer requests (reads and writes) waiting to be serviced by ATA disks on the IDE channel

**IDE Channel Inventory**

- **Channel Configuration**
  - Identifies the IDE controller to which this IDE channel is connected
  - The number of ATA disks attached to the channel
IDE controller

The following information is provided for an IDE controller.

IDE Controller Status

- Transfers/Sec—The number of requests between the server and this IDE controller each second
- MBytes/Sec—The sum of all megabytes transferred (read and written) between the server and this IDE controller each second
- Millisec/Transfer—The average time for each request to complete
- Queue Length—The average number of concurrent requests between the server and this IDE controller, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (disk or controller)

IDE controller status is determined by the performance status of the ATA disks attached to the controller and the IDE channels connecting the ATA disks to the controller.

IDE Controller Inventory

- Controller Configuration
  - The controller identification, including controller model and PCI slot (if applicable)
  - Number of disk arrays on the controller (if applicable)
  - Number of ATA disks attached to the controller
- Windows/Linux Physical Disks—Lists each Microsoft Windows and Linux physical disk defined on this IDE controller and whether the physical disk is defined on a single ATA disk or an array of ATA disks

Logical drive

The following information is provided for a logical drive.

Logical Drive Status

- Reads/Sec—The number of reads from this logical drive each second
- Writes/Sec—The number of writes to this logical drive each second
- Read MBytes/Sec—The number of megabytes read from the logical drive each second
- Write MBytes/Sec—The number of megabytes written to the logical drive each second
- Millisec/Read—The average time for each read to complete
- Millisec/Write—The average time for each write to complete
- Queue Length—The average number of concurrent requests between the server and this logical drive, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (disk or controller)
Logical Drive Inventory

Logical Drive Configuration
- The controller on which the logical drive is defined
- The array label (such as A, B, or C) as shown by the Array Configuration Utility (ACU)
- The logical drive number as assigned by the ACU and the physical disk mapping
- Logical drive size in megabytes
- The RAID level for this logical drive
- The logical drive striping factor
- Whether caching is enabled for this logical drive

Memory

The following information is provided for memory.

Memory Status
- Available MBytes—The amount of memory that is not currently allocated to any process or is unused. A low Available MBytes value can indicate memory allocation bottlenecks.
- Page Reads/Sec—The number of times the disk was read to retrieve pages of virtual memory necessary to resolve page faults each second. Multiple pages can be read during a single disk read operation.
- Pages Input/Sec—The number of pages read from the disk to resolve memory references to pages that were not in memory at the time of the reference. This counter includes paging traffic on behalf of the system cache to access file data for applications. It is important to observe this counter if you are concerned about excessive memory usage, or thrashing, and the excessive paging that can result.
- Page Faults/Sec—The average number of page faults each second. A page fault occurs when a process refers to a virtual memory page that is not in its working set in main memory. A page fault does not cause the page to be fetched from disk if that page is on the standby list and is already in main memory or if it is in use by another process with which the page is shared. There are two types of page faults:
  - Hard Page Fault—The most expensive in terms of system resource usage, occurring when a missing page must be retrieved from the disk
  - Soft Page Fault—Generally not considered a source of memory bottlenecks, occurring when the missing page is not in the current working set but is located elsewhere in memory and easily brought into the working set
- Hard Page Faults %—The ratio of page faults per second to pages input per second. This value is a primary indication of memory bottlenecks.

Memory performance is determined primarily by the rate at which memory is swapped out to disk. Page Reads/Sec is the primary factor in determining memory performance issues, but the Hard Page Faults % and Available MBytes are also considered.
Memory Inventory

- System Memory
  - Displays the physical memory installed in the server
  - Displays the amount of memory that can be addressed by the operating system
  - Displays any server-specific memory technology or configurations
- Memory Board—Describes the configuration of the memory boards and lists the number of DIMMs configured in each particular DIMM socket and any empty sockets

Network adapter

The following information is provided for a network adapter.

Network Adapter Status

- MBits TX/Sec—The average number of megabits transmitted from the selected adapter each second
- MBits RX/Sec—The average number of megabits received by the selected adapter each second
- MBytes/Sec—The average number of megabytes transferred (transmitted or received) over the network adapter each second

NIC port performance on the adapter determines network adapter performance.

Network Adapter Inventory

- NIC Configuration
  - Displays the name and location of the network adapter
  - Displays the supported and negotiated PCI protocol (bus speed) of the network adapter
  - Lists the number of ports on the NIC adapter, including any upgrade modules installed on the network adapter
- NIC Ports—Displays all IP addresses assigned to the network ports
- Network Teams—The state of all the ports on all network adapters

Network connections

The following information is provided for network connections.

Network Connections Status

- Network MBytes/Sec—The average number of megabytes transferred (transmitted or received) over the network subsystem each second
- MBits TX/Sec—The average number of megabits transmitted over the network each second
- MBits RX/Sec—The average number of megabits received over the network each second

Network connection performance is determined by the performance of the network adapters.
Network Connection Inventory

- Network Connections Configuration—Displays the number of adapters and ports installed and available on the server, including any that are disabled
- IP Addresses—Displays all IP addresses assigned to the ports

Network Port

The following information is provided for a network port.

Network Port Status

- MBytes/Sec—The average number of megabytes transferred (transmitted or received) over the NIC port each second.
- MBits TX/Sec—The average number of megabits transmitted from the selected NIC port each second.
- MBits RX/Sec—The average number of megabits received by the selected NIC port each second.
- TX Utilization %—The percentage of data that is transmitted from the selected NIC port. This value is calculated from the TX MBits/Sec and the operating speed of the NIC port.
- RX Utilization %—The percentage of data that is received from the selected NIC port. This value is calculated from the RX MBits/Sec and the operating speed of the NIC port.
- Port Utilization %—The percentage of data that is transferred (transmitted over the NIC port). If the port is running in full duplex mode, Port Utilization % is the higher of TX Utilization % and RX Utilization %. If the port is running in half duplex mode, Port Utilization % is the sum of TX Utilization % and RX Utilization %.

Network Port Inventory

- Port Configuration
  - Displays the name of the NIC adapter
  - Displays the name of the port (on the base board or upgrade module)
  - Displays the media access control (MAC) address of the NIC port
  - Displays the IP address of the NIC port
  - Displays the maximum speed (in MB/s) of the NIC port
  - Provides the NIC teaming configuration if the server is configured with NIC teaming
Network storage array

The following information is provided for a network storage array.

Network Storage Array Status

- Server Transfers/Sec—The average number of transfer requests (read and written) between the monitored servers and the array each second
- Server MBytes/Sec—The average number of megabytes transferred (read and written) between the monitored servers and this array each second
- Server Millisec/Transfer—The average time for each request between the monitored servers and the array to complete
- Server Queue Length—The average number of transfer requests (read and written) from the monitored servers that are waiting to be serviced by this array
- Array MBytes/Sec—The average number of megabytes transferred (read and written) to all the disks in the array each second
- Disk Queue Length—The average number of transfer requests (read and written) waiting to be serviced by each disk in the array

Network Storage Array Inventory

- Array Configuration—Displays the number of logical drives implemented on the array
- Hard Drives—Lists the drives that constitute the array

Network storage controller

The following information is provided for a network storage controller.

Network Storage Controller Status

- Transfer/Sec—The average number of transfers (reads and writes) on this network storage controller each second
- MBytes/Sec—The average number of megabytes transferred on this network storage controller each second
- Millisec/Transfer—The average time to complete a transfer to and from the selected network storage controller
- Queue Length—The average number of transfer requests (reads and writes) waiting to be serviced by the network storage controller
- Port Utilization%—The average utilization of the Fibre Channel port on this controller

Network Storage Controller Inventory

Controller Configuration

- The controller identification, including controller model
- The supported and negotiated PCI protocols (bus speed)
Network storage enclosure

The following information is provided for a network storage enclosure.

Network Storage Enclosure Status

- Transfers/Sec—The average number of transfers (reads and writes) on this network storage enclosure each second
- MB/Sec—The average number of megabytes transferred on this network storage enclosure each second
- Milliseconds/Transfer—The average time to complete a transfer to and from the selected network storage enclosure
- Queue Length—The average number of transfer requests (reads and writes) waiting to be serviced by the network storage enclosure

Network Storage Enclosure Inventory

- Enclosure Configuration—Displays the type or model, name, and serial number of the network storage enclosure.
- Controllers—Displays the name and model of the enclosure and whether it is operating with redundant controllers.
  - If a redundant controller is configured, then both standby and active controllers are listed.
  - If redundancy is not configured, only active controllers are listed.
- Detected Servers—Displays a list of servers sharing the enclosure.

Network storage logical drives

The following information is provided for logical drives located in the network storage.

Network Share Status

- Reads/Sec—The average number of reads from the selected logical drive each second
- Writes/Sec—The average number of writes to the selected logical drive each second
- Read MB/Sec—The average number of megabytes read from the selected logical drive each second
- Write MB/Sec—The average number of megabytes written to the selected logical drive each second
- Milliseconds/Read—The average time required to complete a read operation
- Milliseconds/Write—The average time required to complete a write operation
- Queue Length—The average number of transfer requests (reads and writes) that are waiting to be serviced by the logical drive
Network Share Inventory

Logical Drive Configuration
- Displays the total capacity of the drive
- Displays the network storage enclosure in which the selected logical drive is located
- Displays the RAID level for this logical drive

PCI bus

The following information is provided for a PCI bus.

PCI Bus Status
- MBytes/Sec—The average number of megabytes transferred on the selected PCI bus each second.
- PCI Utilization %—The PCI utilization for the selected PCI bus. A 32-bit PCI and 64-bit PCI can operate simultaneously on the same PCI bus. The utilization is primarily dependent on the MBytes/Sec rate and the negotiated PCI bus protocol:
  - 32-bit PCI—Operates at 33 MHz, resulting in a maximum throughput of 132 MB/s
  - 64-bit PCI—Operates at 33 MHz, resulting in a maximum throughput of 264 MB/s
  - 64-bit/50-MHz PCI-X—Provides a maximum throughput of 400 MB/s
  - 64-bit/66-MHz PCI or PCI-X—Provides a maximum throughput of 528 MB/s
  - 64-bit/100-MHz PCI-X—Provides a maximum throughput of 800 MB/s
  - 64-bit/133-MHz PCI-X—Provides a maximum throughput of 1064 MB/s
  - PCI Express X1—Provides a maximum throughput of 500 MB/s
  - PCI Express X2—Provides a maximum throughput of 1000 MB/s
  - PCI Express X4—Provides a maximum throughput of 2 GB/s
  - PCI Express X8—Provides a maximum throughput of 4 GB/s
  - PCI Express X12—Provides a maximum throughput of 6 GB/s
  - PCI Express X16—Provides a maximum throughput of 8 GB/s

PCI bus performance is evaluated using the Bus Utilization %.

**NOTE:** PMP does not accurately report the negotiated PCI bus protocol when unknown PCI devices with slower transfer rates than the controller are configured on the same bus.

PCI Bus Inventory
- PCI Support—Displays the supported and negotiated PCI protocol (bus and speed)
- PCI Devices—Lists the PCI bus slots and any I/O expansion boards installed in the slots
Processors

The following information is provided for processors.

Processors Status

- **Average Processor Utilization %**—The average percentage of time that all the processors on the system are busy executing non-idle threads. On a multiprocessor system, if all processors are always busy, the metric reads 100%; if all processors are 50% busy, the metric reads 50%; if one-fourth of the processors are busy, the metric reads 25%. Average Processor Busy % can be viewed as the fraction of the time spent doing useful work.

  Each processor is assigned an idle thread in the idle process consuming unproductive processor cycles not used by another thread. Some processors might be more heavily loaded than other processors. In this case, the total processor time percentage is the average of the loads on each processor.

- **Busiest Processor Utilization %**—The average utilization of the logical processor with the highest utilization. This value is equal to the Average Processor Utilization % if the server is using one processor core.

- **Processor Busy %**—The percentage of time that the processor is executing a non-idle thread.

- **Context Switches/Sec**—The number of thread context switches at which all processors on the server are switched from one thread to another each second. Context switches occur when a running thread voluntarily relinquishes the processor, is preempted by a higher-priority ready thread, or switches between user mode and privileged (kernel) mode to use a subsystem service.

- **Interrupts/Sec**—The average number of hardware interrupts the processor is receiving and servicing each second.

Average Processor Utilization % and Highest Processor Utilization % are used to determine processor performance.

Processors Inventory

- **Processor Support**—Lists the number of processors supported by the server

- **Processors**—Displays the number of processors installed on the server and a summary of the processors (type, speed, and cache size)
SCSI adapter

The following information is provided for a SCSI adapter.

SCSI Adapter Status

- Transfers/Sec—The number of requests between the server and this SCSI adapter each second
- MBytes/Sec—The average number of megabytes transferred (read and written) between the server and this SCSI adapter each second
- Millisecond/Transfer—The average time for each request to complete
- Queue Length—The average number of concurrent requests between the server and this SCSI adapter, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (drive or adapter)

SCSI adapter performance is based on the performance of the SCSI disks attached to the adapter and the SCSI buses used to attach the disks to the adapter.

SCSI Adapter Inventory/Controller Configuration

- Identifies the supported and negotiated PCI protocol (bus speed) used by the SCSI adapter
- Provides the number of SCSI drives configured on the adapter
- Provides the number of SCSI ports used
- Windows/Linux Physical Disks—Lists the physical disk drives and identifies each drive SCSI ID, drive letter, and associated SCSI adapter
SCSI storage enclosure

The following information is provided for a SCSI storage enclosure.

SCSI Storage Enclosure Status

- Transfers/Sec—The average number of transfers on this SCSI bus each second (the sum of the Disk Transfers/Sec for all hard drives on this bus).
- MBBytes/Sec—The average number of megabytes transferred on this SCSI bus each second (the sum of the Disk MBBytes/Sec for all SCSI drives on this bus).
- SCSI Utilization %—The average SCSI utilization for this SCSI bus, which is primarily dependent on the MBBytes/Sec, and the SCSI protocol negotiated between the controller and each drive on the bus. The negotiated SCSI protocol is reported in the hard drive inventory. The valid SCSI protocols include:
  - SCSI-1—5 MB/s with 8-bit transfers at 5 MHz (5,000,000 bytes/s)
  - Fast SCSI-2—10 MB/s with 8-bit transfers at 10 MHz (10,000,000 bytes/s)
  - Fast-Wide SCSI-2—20 MB/s with 16-bit transfers at 10 MHz
  - Ultra SCSI-3—20 MB/s with 8-bit transfers at 20 MHz
  - Wide-Ultra SCSI-3—40 MB/s with 16-bit transfers at 20 MHz
  - Wide Ultra2 SCSI—80 MB/s with 16-bit transfers at 40 MHz
  - Wide Ultra3 SCSI—160 MB/s with 16-bit transfers at 80 MHz
  - Ultra320 SCSI—320 MB/s with 16-bit transfers at 160 MHz

SCSI storage enclosure performance is determined by the SCSI Utilization %.

SCSI Storage Enclosure Inventory

- Enclosure Configuration
  - The type or model of the storage enclosure
  - Which SCSI protocol is supported by the storage enclosure
  - The number of drive bays provided by the storage enclosure
  - The number of SCSI drives installed in the storage enclosure
  - The SCSI adapter attached to the storage enclosure and the port on the adapter
**SCSI drive**

The following information is provided for a SCSI drive.

**SCSI Drive Status**

- Disk Reads/Sec—The average number of reads from the selected SCSI drive each second
- Disk Writes/Sec—The average number of writes to the selected SCSI drive each second
- Disk Read MBytes/Sec—The average number of megabytes read from the selected SCSI drive each second
- Disk Write MBytes/Sec—The average number of megabytes written to the selected SCSI drive each second
- Disk Millisec/Read—The average time required to complete a read
- Disk Millisec/Write—The average time required to complete a write
- Disk Queue Length—The average number of transfer requests (reads and writes) waiting to be serviced by the SCSI drive, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (drive or controller)

PMP uses a set of algorithms to determine SCSI drive status. In general, the Disk Queue Length is a primary parameter. When the value of the Disk Queue Length exceeds an acceptable value, the Disk Reads/Sec and Writes/Sec are examined to determine whether read or write operations are requiring most of the drive throughput. When combined with Disk Millisec/Read or Write, PMP can determine if the number of requests for the drive is exceeding the capabilities of the drive.

**SCSI Drive Inventory**

- Drive Information
  - Displays a description of the drive, including the size
  - Displays the hard drive model number
  - Displays the exact size of the drive as seen by the operating system
- Configuration Information
  - Provides a summary of the drive configuration
  - Displays the name of the Smart Array controller to which it is attached
  - Displays the location of the hard drive in its enclosure
  - Displays the array in which the drive is configured
  - Provides the SCSI protocol negotiated for transfers between this drive and the disk controller
Server metrics

The following information is provided for server metrics.

Server status

- Average Processor Utilization %—The percentage of time that the processor is executing a non-idle thread, averaged for the number of processors in the server
- Available MBytes—The amount of memory not currently allocated to any process (unused). A low Available MBytes value might indicate memory allocation bottlenecks.
- Page Faults/Sec—The number of faulted pages handled by the processor each second
- Network MBytes/Sec—The sum of megabytes transferred (transmitted and received) over the subsystem each second
- Storage MBytes/Sec—The sum of megabytes transferred (read and written) over the storage subsystem each second
- Host Bus MBytes/Sec—The sum of megabytes transferred over the host buses each second

Server inventory

- Server model
  - Processor quantity and description
  - Amount of memory
  - Network adapters and ports
  - Storage controllers/SCSI adapters
  - Host buses
- Operating system
  - Server operating system and version information
  - Summary of the file systems defined on the operating system
  - Number of processors in use
  - Windows and Linux physical disks

Smart Array controller

The following information is provided for a Smart Array controller.

Smart Array Controller Status

- Transfers/Sec—The number of requests between the server and this IDE Smart Array controller each second
- MBytes/Sec—The sum of all megabytes transferred (read and written) between the server and this Smart Array controller each second
- Millisec/Transfer—The average time for each request to complete
- Queue Length—The average number of concurrent requests between the server and this Smart Array controller, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (drive or controller)

Smart Array controller performance is based on the performance of the SCSI disks attached to the controller and the SCSI buses used to attach the drives to the controller.
Smart Array Controller Inventory

- Controller Configuration
  - The controller identification, including controller model and PCI slot (if applicable)
  - The supported and negotiated PCI protocols (bus speed)
  - The controller cache configuration
  - Number of hard disks attached to the controller
  - Number of SCSI ports currently in use on the controller
  - Number of arrays on the controller
  - Number of array logical drives defined on the controller
- Windows/Linux Physical Disks—Lists the physical disk drives and identifies each drive SCSI ID, drive letter, and associated Smart Array controller

Smart Array SCSI drive

The following information is provided for a Smart Array SCSI drive.

Smart Array SCSI Drive Status

- Disk Reads/Sec—The number of reads from the drive each second
- Disk Writes/Sec—The number of writes to the drive each second
- Disk Read MBytes/Sec—The number of megabytes read from the drive each second
- Disk Write MBytes/Sec—The number of megabytes written to the drive each second
- Disk Millisec/Read—The average time for each read to complete
- Disk Millisec/Write—The average time for each write to complete
- Disk Queue Length—The average number of concurrent requests between the server and the drive

Smart SCSI Drive Inventory

- Drive Information
  - Displays a description of the drive, including the size
  - Displays the hard drive model number
  - Displays the exact size of the drive as seen by the operating system
- Configuration Information
  - Provides a summary of the drive configuration
  - Displays the name of the Smart Array controller to which it is attached
  - Displays the location of the hard drive in its enclosure
  - Displays the array in which the drive is configured
  - Provides the SCSI protocol negotiated for transfers between this drive and the disk controller
SATA Drives

The following information is provided for a SATA drive.

SATA Drive Status

- Disk Read/Sec—The average number of reads from the selected SATA drive each second
- Disk Write/Sec—The average number of writes to the selected SATA drive each second
- Disk Read Mbytes/Sec—The average number of Megabytes of data read from the selected SATA drive each second
- Disk Write Mbytes/Sec—The average number of Megabytes of data written to the selected SATA drive each second
- Disk Millisec/Read—The average time required to complete a read operation
- Disk Millisec/Write—The average time required to complete a write operation
- Disk Queue Length—The average number of transfer requests (reads and writes) waiting to be serviced by the SATA drive, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (drive or controller)

PMP uses a set of algorithms to determine the SATA drive status. The Disk Queue Length is a primary parameter. However, when the value of the Disk Queue Length exceeds the acceptable value, the Disk Reads/Sec and Writes/Sec are examined to determine whether read or write operations require most of the drive throughput. When combined with Disk Millisec/Read or Write, PMP can determine if the number of requests for the drive will exceed the capabilities of the drive.

SATA Drive Inventory

- Drive Information
  - Displays description of the drive, including size
  - Displays the hard drive model number
  - Displays the exact size of the drive as seen by the operating system
- Configuration Information
  - Provides a summary of the drive configuration
  - Displays the name of the Smart Array controller to which it is attached
  - Displays the location of the hard drive in its enclosure
  - Displays the array in which the drive is configured
  - Provides the SATA protocol negotiated for transfers between this drive and the disk controller
SAS Drives

The following information is provided for a SAS Drive.

SAS Drive Status

- Disk Read/Sec—The average number of reads from the selected SAS drive each second
- Disk Write/Sec—The average number of writes to the selected SAS drive each second
- Disk Read Mbytes/Sec—The average number of Megabytes of data read from the selected SAS drive each second
- Disk Write Mbytes/Sec—The average number of Megabytes of data written to the selected SAS drive each second
- Disk Millisecond/Read—The average time required to complete a read operation
- Disk Millisecond/Write—The average time required to complete a write operation
- Disk Queue Length—The average number of transfer requests (reads and writes) waiting to be serviced by the SAS drive, including transfers currently being serviced and transfers waiting for service, regardless of where the request is waiting (drive or controller)

PMP uses a set of algorithms to determine the SAS drive status. The Disk Queue Length is a primary parameter. However, when the value of the Disk Queue Length exceeds the acceptable value, the Disk Reads/Sec and Writes/Sec are examined to determine whether read or write operations require most of the drive throughput. When combined with Disk Millisecond/Read or Write, PMP can determine if the number of requests for the drive will exceed the capabilities of the drive.

SAS Drive Inventory

- Drive Information
  - Displays description of the drive, including size
  - Displays the hard drive model number
  - Displays the exact size of the drive as seen by the operating system
- Configuration Information
  - Provides a summary of the drive configuration
  - Displays the name of the Smart Array controller to which it is attached
  - Displays the location of the hard drive in its enclosure
  - Displays the array in which the drive is configured
  - Provides the SAS protocol negotiated for transfers between this drive and the disk controller
Storage components

Storage components differ depending on the server environment. PMP is designed to monitor a variety of storage components, including:

- Storage enclosures
- Fibre Channel HBAs
- SCSI arrays and logical and physical disk drives
- Smart arrays

Storage Status

- Storage Transfers/Sec—The number of PCI bus transfers to and from storage each second
- Storage MBytes/Sec—The average number of megabytes transferred (read and written) on the storage each second

Storage Inventory

- Windows/Linux Logical Disks—Lists all of the logical disks in the storage subsystem and identifies their associated drive letter, file system, disk drive size (in MB), and percentage of space used
- Windows/Linux Physical Disks—Lists all of the physical disks in the storage subsystem and identifies their associated SCSI ID, drive letter, and array controller
Appendix B Vulnerability and Patch Management Pack additional information

Infrastructure

A server environment using the Vulnerability and Patch Management Pack consists of the following components:

- Vulnerability and Patch Management Pack
- HP SIM
- Target systems
- VPM Acquisition Utility (installed on a separate system, optional)

You can install the Vulnerability and Patch Management Pack and HP SIM together on a single server (referred to as a shared configuration), or install each component on a separate server (referred to as a distributed configuration). For this release, both the Vulnerability and Patch Management Pack and HP SIM must operate on a Windows server.
Shared server configuration

In a shared server configuration, Vulnerability and Patch Management Pack and HP SIM are installed on the same server. The following figure depicts a shared server configuration in which the VPM server has Internet access to obtain patch and vulnerability updates.
The following figure depicts a shared server configuration in which the VPM Acquisition Utility is used to obtain patch and vulnerability updates from the patch update sources.
Vulnerability and Patch Management Pack hardware requirements

The VPM server, the server on which the Vulnerability and Patch Management Pack software is installed, must meet the following hardware requirements. Requirements listed for the VPM server are independent of requirements for HP SIM and any other applications that coexist on the VPM server. For specific hardware requirements for the HP SIM server, see the HP Systems Insight Manager Installation and Configuration Guide.

Table 28 Hardware requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any HP x86 server</td>
<td>—</td>
</tr>
<tr>
<td>Memory</td>
<td>At least 512 MB RAM</td>
</tr>
<tr>
<td>Processor</td>
<td>1.5 GHz or faster</td>
</tr>
<tr>
<td>Disk space</td>
<td>At least 1 GB for Vulnerability and Patch Management Pack (150 MB in the TEMP directory for installation)</td>
</tr>
<tr>
<td></td>
<td>Additional space for scan reports and patches</td>
</tr>
<tr>
<td>File structure</td>
<td>New Technology File System (NTFS)</td>
</tr>
<tr>
<td>DVD-ROM drive</td>
<td>—</td>
</tr>
</tbody>
</table>
Vulnerability and Patch Management Pack software requirements

The VPM server, the server on which the Vulnerability and Patch Management Pack software is installed, must meet the following software requirements. Requirements listed for the VPM server are independent of requirements for HP SIM and any other applications that coexist on the VPM server. For specific software requirements for the HP SIM server, see the *HP Systems Insight Manager Installation and Configuration Guide*.

**Table 29** Software requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows 2000 Server SP4</td>
</tr>
<tr>
<td></td>
<td>Windows 2000 Advanced Server SP4</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2003, Standard Edition SP1</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003, Enterprise Edition SP1</td>
</tr>
<tr>
<td>Services</td>
<td>Microsoft Internet Information Services (IIS) 5.0 or later, installed and running**</td>
</tr>
<tr>
<td></td>
<td>TCP/IP with DNS properly configured so that system names can be resolved to IP addresses</td>
</tr>
<tr>
<td>Database</td>
<td>An existing Microsoft SQL Server database can be used, or Microsoft Data Engine (MSDE) will be installed on the VPM server with the Vulnerability and Patch Management Pack installation. When changing databases during an upgrade, patch data from the previous database is not migrated. A full patch acquisition must be performed to repopulate the patch repository.</td>
</tr>
<tr>
<td>Applications</td>
<td>HP SIM 5.1 or later, installed on a Windows server with Windows Management Interface (WMI) Mapper</td>
</tr>
<tr>
<td></td>
<td>Mozilla Firefox 2.0 or Microsoft Internet Explorer 6.0 or 7.0</td>
</tr>
<tr>
<td></td>
<td>Adobe Acrobat Reader 3.x or later (to view scan results)</td>
</tr>
</tbody>
</table>

*HP SIM might have additional restrictions for supported service pack levels.

**HP strongly recommends enabling HTTPS if HP SIM and Vulnerability and Patch Management Pack are installed on separate servers. For information about configuring HTTPS service in IIS, see [http://support.microsoft.com/?kbid=324069](http://support.microsoft.com/?kbid=324069).
**VPM Acquisition Utility (optional)**

The VPM Acquisition Utility can be installed on a system with Internet access to acquire patch information and patch files from selected vendor websites. This utility allows patch acquisitions and vulnerability updates without requiring the VPM server to be directly connected to the Internet, thereby reducing potential security risks. No other Vulnerability and Patch Management Pack components or database software is required to be installed on the system to download vulnerability and patch updates.

The table below lists the minimum requirements for the system on which you can install the VPM Acquisition Utility.

**Table 30  VPM Acquisition Utility requirements**

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>256 MB RAM</td>
</tr>
<tr>
<td>Processor</td>
<td>1.5 GHz or faster</td>
</tr>
<tr>
<td>Disk space</td>
<td>At least 1 GB</td>
</tr>
<tr>
<td></td>
<td>Available space for downloading vulnerability patches</td>
</tr>
<tr>
<td>Internet access for downloading vulnerability patches</td>
<td>Windows 2000 Server SP4</td>
</tr>
<tr>
<td></td>
<td>Windows 2000 Advanced Server SP4</td>
</tr>
<tr>
<td>Operating system (32-bit versions only)</td>
<td>Windows 2000 Professional</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003, Standard Edition SP1 or SP2 (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003, Enterprise Edition SP1 or SP2 (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2, Standard Edition (32-bit only)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2, Enterprise Edition (32-bit only)</td>
</tr>
</tbody>
</table>

**Target systems**

Target systems are managed by Vulnerability and Patch Management Pack. HP recommends installing HP Management Agents on ProLiant target systems to allow HP SIM to better identify the target systems. Enable WMI or Web-Based Enterprise Management (WBEM) for other target systems. The VPM Patch Agent is automatically deployed when target systems are licensed to allow patches to be applied to the systems.

Secure Shell (SSH) must be installed on Linux target systems.

For a list of supported target systems, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Support Matrix*. 
Provided scans

The following table lists the provided scan definitions that are provided with Vulnerability and Patch Management Pack and a brief description of each.

**NOTE:** Custom scans can be created from the default system scans. When default system scans are updated, the custom scans are updated with corresponding vulnerability updates also.

<table>
<thead>
<tr>
<th>Scan definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4_0*</td>
<td>Windows NT 4.0 vulnerabilities</td>
</tr>
<tr>
<td>Advisory</td>
<td>Microsoft Advisories</td>
</tr>
<tr>
<td>AutoFix</td>
<td>Autofixable vulnerabilities</td>
</tr>
<tr>
<td>CrossPlatform</td>
<td>Windows and Linux vulnerabilities</td>
</tr>
<tr>
<td>FileChecks</td>
<td>Known and unknown locations file checks</td>
</tr>
<tr>
<td>FileCheck_KnownLocation</td>
<td>Known location file checks</td>
</tr>
<tr>
<td>FileCheck_UknownLocation</td>
<td>Unknown location file checks</td>
</tr>
<tr>
<td>IE</td>
<td>Internet Explorer vulnerabilities</td>
</tr>
<tr>
<td>IIS</td>
<td>IIS vulnerabilities</td>
</tr>
<tr>
<td>Linux</td>
<td>Linux vulnerabilities</td>
</tr>
<tr>
<td>Malware</td>
<td>Malware checks</td>
</tr>
<tr>
<td>Password</td>
<td>Password policy check</td>
</tr>
<tr>
<td>PasswordChecker</td>
<td>Windows NT password policy</td>
</tr>
<tr>
<td>Policy</td>
<td>All policy check</td>
</tr>
<tr>
<td>SqlServer</td>
<td>SQL Server vulnerabilities</td>
</tr>
<tr>
<td>W2K</td>
<td>Windows 2000 vulnerabilities</td>
</tr>
<tr>
<td>W2K3</td>
<td>Windows 2003 vulnerabilities</td>
</tr>
<tr>
<td>XP</td>
<td>Windows XP vulnerabilities</td>
</tr>
</tbody>
</table>

* This scan definition is not included with the current version of Vulnerability and Patch Management Pack and only exists if previous versions of the software have been installed.
Updating VPM credentials using the Change VPM Credentials Utility

You can use the Change VPM Credentials Utility to update Vulnerability and Patch Management Pack:

- When the credentials or IP address of the HP SIM server have been changed
- When the credentials of the account used to install Vulnerability and Patch Management Pack have been changed
- To turn on or off the secure connection between the HP SIM and VPM server:

To update the Vulnerability and Patch Management Pack credentials:

1. From the VPM server, click **Start > HP Vulnerability and Patch Management Pack > Change VPM Credentials**.
2. Select whether to change Vulnerability and Patch Management Pack or database credentials, and then click **OK**.
3. If changing Vulnerability and Patch Management Pack credentials enter your current user credentials and IP address, select whether to a secure connection to the VPM server, and then click **Change**.
4. If changing database credentials, enter your current database credentials, and then click **Change**.

Backing up and restoring the Vulnerability and Patch Management Pack

Vulnerability and Patch Management Pack application files are tightly coupled to HP SIM and its components. There are also Vulnerability and Patch Management Pack subcomponents, which can place files in other locations. A number of tables exist in databases, which require special tools to back up effectively.

Use the following guidelines to preserve the history of previous scan results and the list of patches installed on each target system.

The Vulnerability and Patch Management Pack plug-in for HP SIM can be installed in a shared or distributed configuration. Backup and restore can be done by preserving individual components. Before beginning:

- Understand the HP SIM file/directory structure and database layout
- Understand the Vulnerability and Patch Management Pack file and directory structure

Component backup

HP SIM must be offline to back up components. To back up individual components:

1. Back up the Vulnerability and Patch Management Pack files under the HP SIM directory:
   - C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\home\ STATConfigurations
   - C:\Program Files\HP\Systems Insight Manager\hpwebadmin\webapps\ROOT\mxportal\home\ STATScanner
2. Back up HP SIM directory tree and the HP SIM database. For instructions, see the *HP Systems Insight Manager Help Guide*. This procedure might be different depending on the operating system.
Component restoration

1. Restore HP SIM and the HP SIM database from the backup files.
3. Restore the Vulnerability and Patch Management Pack files from the backup.

This procedure restores the Vulnerability and Patch Management Pack historical scan and patch data to the point where it was backed up. HP recommends running a scan to restore current Vulnerability and Patch Management Pack status.

Reinstalling VPM to a new host

This process removes the patch and vulnerability database, save the historical files, and reinstalls VPM to a new host. After completing the process you must reload the patch and vulnerability database.

1. Connect to the system housing the remote VPM server (not the HP SIM server).
2. Uninstall VPM using either the Start menu or the Add or Remove Programs option in the Control Panel.
3. When prompted to remove the data files, select NO to keep the historical files.
4. Connect to the system housing the HP SIM Server.
5. Install the VPM package, using the HP SIM server as the host for VPM.
6. After the entire installation process is complete, reboot the system, to make sure all files are released and installed correctly.

**NOTE:** You must redeploy the patch agents to direct them to the new VPM server before patching.

**NOTE:** Before acquiring Linux Patches you must re-apply the Red Hat network SID files to the new VPM server.

7. Using HP SIM, request a Patch Acquisition. The entire patch database must be reloaded.
8. Rescan your servers to update Vulnerability status.

Vulnerability and Patch Management Pack events

Vulnerability and Patch Management Pack creates events in HP SIM. These events can be viewed with all HP SIM events in the Events list, or independently in the VPM Events list.
Scan events

The following table lists the events created by the Vulnerability and Patch Management Pack scanning components.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitted VPM Scan</td>
<td>A vulnerability scan has been submitted</td>
<td>When a scan is submitted. If another scan is already running, this scan is queued.</td>
</tr>
<tr>
<td>Started VPM Scan</td>
<td>A group vulnerability scan has started</td>
<td>When a scan is started for all systems selected in the scan operation. Each individual system also has a scan start event. Individual machines are scanned one at a time.</td>
</tr>
<tr>
<td>Started VPM Scan for System</td>
<td>A vulnerability scan has started on a system</td>
<td>At the start of the scan for each individual system.</td>
</tr>
<tr>
<td>Completed VPM Scan</td>
<td>A group vulnerability scan has completed</td>
<td>When a scan is completed for all systems selected in the scan operation. Each individual system also has a scan completion event. Individual machines are scanned one at a time.</td>
</tr>
<tr>
<td>Completed VPM Scan for System</td>
<td>A vulnerability scan has completed on a system</td>
<td>At the completion of the scan for each individual system.</td>
</tr>
<tr>
<td>Failed VPM Scan</td>
<td>A failure has occurred during a VPM scan</td>
<td>When an entire scan fails to complete because of an internal error. Check the system event log for more information.</td>
</tr>
</tbody>
</table>
## Patch and fix events

The following table lists the events created by the Vulnerability and Patch Management Pack patching components.

**Table 33** VPM patch and fix events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submitted VPM Patch and Fix</td>
<td>A VPM patch and fix has been submitted.</td>
<td>When one or more patches and fixes have been submitted.</td>
</tr>
<tr>
<td>Started VPM Patch and Fix</td>
<td>A group VPM patch and fix has started.</td>
<td>When one or more patches or fixes have been started for all systems selected in the patch-fix operation. Each individual system also has a start event.</td>
</tr>
<tr>
<td>Started VPM Patch and Fix for System</td>
<td>A VPM patch and fix has started on a system.</td>
<td>When one or more patches or fixes have been started for an individual system.</td>
</tr>
<tr>
<td>Completed VPM Patch and Fix</td>
<td>A group VPM patch and fix has completed.</td>
<td>When all patches and fixes have been completed for all systems selected in the patch-fix operation. Each individual system also has a completion event.</td>
</tr>
<tr>
<td>VPM Patch Start</td>
<td>A vulnerability patch installation has begun on the target system.</td>
<td>When a vulnerability patch installation has been started on the target system. A software update or bulletin is being applied to the target system.</td>
</tr>
<tr>
<td>Completed VPM Patch and Fix for System</td>
<td>A VPM patch and fix has completed on a system.</td>
<td>When all patches and fixes have been completed for an individual system.</td>
</tr>
<tr>
<td>VPM Patch Ended with Success</td>
<td>A vulnerability patch installation has ended on the target system with the status of successful.</td>
<td>When a vulnerability patch installation has ended on the target system with the status of successful.</td>
</tr>
<tr>
<td>VPM Patch Ended with Failure</td>
<td>A vulnerability patch installation has ended on the target system with the status of failure. Follow up might be required to determine the actual cause and remedy to the failure. It might be useful to examine any patch event details related to this patch.</td>
<td>When a vulnerability patch installation has ended on the target system with the status of failure.</td>
</tr>
<tr>
<td>VPM Patch Current Status</td>
<td>VPM Patch Agent is reporting the current status of a patch on the target device.</td>
<td>The status is reported after the reboot. When VPM Patch Agent reports the current status of a patch on the target device because of a patch requiring a reboot.</td>
</tr>
<tr>
<td>VPM Patch Not Applicable</td>
<td>The selected patch is not applicable to the selected system and therefore is not applied.</td>
<td>When the selected patch is not applicable to the selected system.</td>
</tr>
<tr>
<td>Failed VPM Patch and Fix</td>
<td>A failure has occurred during a VPM patch or fix operation.</td>
<td>When one or more patches fails to complete because of an internal error. Check the system event log for more information.</td>
</tr>
<tr>
<td>Failed VPM Patch and Fix for a System</td>
<td>A failure has occurred during a VPM patch or fix operation for a particular system.</td>
<td>When an individual system fix fails to complete because of an internal error. Check the system event log for more information.</td>
</tr>
</tbody>
</table>
### Acquisition events

The following table lists the events created by the Vulnerability and Patch Management Pack patch acquisition.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started VPM Acquisition</td>
<td>Acquisition of vulnerability updates and patches has started</td>
<td>When acquisition of scan definitions, patches and fixes for selected operating systems and applications has started. This operation might take a few minutes depending on the number of items being downloaded.</td>
</tr>
<tr>
<td>VPM has been Updated</td>
<td>The VPM product has been updated</td>
<td>When patches for selected operating systems and applications have been downloaded successfully as part of an acquisition.</td>
</tr>
<tr>
<td>VPM Scan Definitions Updated</td>
<td>Successfully updated vulnerability scan definitions</td>
<td>When scan definition files have been updated successfully as part of an acquisition.</td>
</tr>
<tr>
<td>VPM / STAT Updated</td>
<td>Successfully updated the vulnerability scanner component of VPM</td>
<td>When code that scans and fixes configuration issues has been updated successfully as part of an acquisition.</td>
</tr>
<tr>
<td>VPM Scan Definitions Up-to-date</td>
<td>No updates required for the vulnerability scan definitions, already up to date</td>
<td>When scan definition files do not need to be updated as part of an acquisition.</td>
</tr>
<tr>
<td>VPM / STAT Up-to-date</td>
<td>No updates required for the vulnerability scanner component of VPM</td>
<td>When code that scans and fixes configuration issues does not need to be updated as part of an acquisition.</td>
</tr>
<tr>
<td>Completed VPM Acquisition</td>
<td>Acquisition of vulnerability updates and patches has completed</td>
<td>When acquisition of scan definitions, patches, and fixes for selected operating systems and applications is complete.</td>
</tr>
<tr>
<td>Failed VPM Acquisition</td>
<td>A failure has occurred during a VPM patch acquisition</td>
<td>When acquisition of scan definitions, patches, and fixes for selected operating systems and applications has failed.</td>
</tr>
<tr>
<td>Failed VPM Scan Definitions Update</td>
<td>Updates for the vulnerability scan definitions failed</td>
<td>When acquisition of scan definitions has failed.</td>
</tr>
<tr>
<td>Failed VPM / STAT Update</td>
<td>Updates for the vulnerability scanner component of VPM failed</td>
<td>When acquisition of updated code that scans and fixes configuration issues has failed.</td>
</tr>
</tbody>
</table>
## Miscellaneous events

The following lists the miscellaneous events created by Vulnerability and Patch Management Pack.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed VPM</td>
<td>VPM has been installed</td>
<td>When installation of VPM successfully completes.</td>
</tr>
<tr>
<td>Removed VPM</td>
<td>The VPM product has been removed from this HP SIM Server</td>
<td>When uninstallation of VPM successfully completes.</td>
</tr>
<tr>
<td>VPM Product License</td>
<td>VPM license applied</td>
<td>When a license for VPM is successfully applied to HP SIM.</td>
</tr>
<tr>
<td>VPM Product License Failure</td>
<td>VPM license not applied</td>
<td>When a license for VPM is not successfully applied to HP SIM.</td>
</tr>
<tr>
<td>VPM Security Access Violation</td>
<td>VPM is reporting a security violation</td>
<td>When the VPM plug-in (on the HP SIM server) does not have the right credentials to access the STAT Scanner service (on the VPM server).</td>
</tr>
<tr>
<td>VPM Scan Definition Creation Failure</td>
<td>VPM could not write a new vulnerability scan definition file</td>
<td>When a custom scan definition cannot be created. This event can indicate a lack of disk space or permission problems.</td>
</tr>
<tr>
<td>VPM Scan Definition Removal Failure</td>
<td>VPM could not remove a vulnerability scan definition file</td>
<td>When one or more custom scan definitions are not removed as a part of the delete operation from the Customize Scan operation.</td>
</tr>
<tr>
<td>VPM Scanner Service Unreachable</td>
<td>VPM could not make a connection to the vulnerability scanner service</td>
<td>When VPM has found a problem trying to contact the STAT Scanner service either because of a network problem or because STAT Scanner service is not operational (for example, IIS service is not running on the VPM server).</td>
</tr>
<tr>
<td>VPM Results Structure Creation Failure</td>
<td>VPM could not create its results directory</td>
<td>When VPM cannot create the directory structure required to receive the scan results.</td>
</tr>
<tr>
<td>VPM Results Creation Failure</td>
<td>VPM could not write a results file</td>
<td>When a custom scan definition cannot be created. This event can indicate a lack of disk space or permission problems.</td>
</tr>
<tr>
<td>VPM Results Removal Failure</td>
<td>VPM failed to remove a results file from the VPM results area</td>
<td>When one or more reports are not removed as a part of the delete operation from the View Results by System or View Results by Scan Name process.</td>
</tr>
<tr>
<td>Installed VPM Patch Agent</td>
<td>The VPM Patch Agent has been installed</td>
<td>When the VPM Patch Agent deploys successfully to a system as part of a licensing operation or the Deploy VPM Patch Agent operation.</td>
</tr>
<tr>
<td>Failed VPM Patch Agent Install</td>
<td>A failure has occurred in the VPM Patch Agent installation</td>
<td>When the VPM Patch Agent fails to deploy to a system as part of a licensing operation or the Deploy VPM Patch Agent operation. VPM might not have permission to access the system. If the system type is Unknown or Unmanaged, the VPM Patch Agent must be deployed from the Deploy VPM Patch Agent menu so the operating system type can be manually selected.</td>
</tr>
</tbody>
</table>
### Table 35  Miscellaneous VPM events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
<th>Occurs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started VPM Patch Removal</td>
<td>A patch removal operation has been started</td>
<td>When removal of a patch starts.</td>
</tr>
<tr>
<td>Completed VPM Patch Removal</td>
<td>A patch removal operation has completed</td>
<td>When a patch is successfully removed from a system.</td>
</tr>
<tr>
<td>VPM Generic Radia Error</td>
<td>An error has been detected in the Radia Patch Manager component of VPM</td>
<td>When an error occurs while attempting to apply a patch. See the event details for more information.</td>
</tr>
</tbody>
</table>
Appendix C Installing additional operating systems to be deployed by Rapid Deployment Pack

If you want to install the Windows, VMware, or Linux operating system CDs/DVDs after installation, you must run the ProLiant Integration Module (PIM) or the Integrity Integration Module (IIM) to properly copy the operating system media and RDP jobs to their appropriate locations. You must have your operating system media available so that you can use them during installation.

To run the PIM:
1. Insert your Insight Control Management DVD into the CMS.
2. Run \rdp\eng\pim\setup.exe
3. On the Prerequisites screen, click Verify to check the prerequisites, and then click Next.
4. On the Installation Options screen, select the operating systems to be copied, and then click Next.
5. On the Configuration Options screen, click Next.
7. On the Installation and Configuration screen, to begin copying the operating systems media, click Install.
8. Provide media for each operating system when prompted.
9. To complete the procedure, click Finish.

To run the IIM:
1. Insert your Insight Control Management DVD into the CMS.
2. Run \rdp\eng\iim\setup.exe.
3. On the Prerequisites screen, to check the prerequisites, click Verify, and then click Next.
4. On the Installation Options screen, select the operating systems to be copied, and then click Next.
5. On the Configuration Options screen, click Next.
7. On the Installation and Configuration screen, to begin copying the operating systems media, click Install.
8. Provide media for each operating system when prompted.
9. To complete the procedure, click Finish.
The following table lists RDP operating system directory names from the location "/lib/osdist/yyyyy where yyyy is the directory name of the operating system.

Table 36  RDP operating system directory names

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Directory name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000 Server</td>
<td>w50s</td>
</tr>
<tr>
<td>Windows 2000 Advanced Server</td>
<td>w50as</td>
</tr>
<tr>
<td>Windows Server 2003, Standard Edition</td>
<td>w52s</td>
</tr>
<tr>
<td>Windows Server 2003, Enterprise Edition</td>
<td>w52e</td>
</tr>
<tr>
<td>Windows Server 2003, Web Edition</td>
<td>w52w</td>
</tr>
<tr>
<td>Windows Server 2003, Standard x64 Edition</td>
<td>w52s.64</td>
</tr>
<tr>
<td>Windows Server 2003, Enterprise x64 Edition</td>
<td>w52e.64</td>
</tr>
<tr>
<td>Windows Server 2003 IA64, Enterprise Edition</td>
<td>w52e.ia64</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux AS 4 Update 4 for x86</td>
<td>rhas4u4</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux ES 4 Update 4 for x86</td>
<td>rhes4u4</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux AS 4 Update 4 for AMD64 and Intel EM64T</td>
<td>rhas4u4.64</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux ES 4 Update 4 for AMD64 and Intel EM64T</td>
<td>rhes4u4.64</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux AS 4 Update 4 for Intel Integrity</td>
<td>rhas4u4.ia64</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux ES 4 Update 4 for Intel Integrity</td>
<td>rhes4u4.ia64</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5 for x86</td>
<td>rhel5</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 5 for AMD64 and Intel EM64T</td>
<td>rhel5.64</td>
</tr>
<tr>
<td>VMware ESX Server 2.5.3</td>
<td>vmesx253</td>
</tr>
<tr>
<td>VMware ESX Server 3.0.1</td>
<td>vmesx301</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 10 for x86</td>
<td>sles10</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server 10 for AMD64 and Intel EM64T</td>
<td>sles10.64</td>
</tr>
</tbody>
</table>
accessing Insight Control Management component interfaces in HP SIM, 71
acquiring
  HP Vulnerability and Patch Management Pack updates, 60
acquisitions
  from VPM server, 61
  using VPM Acquisition Utility, 61
adding
  iLO 2 license keys, 69
  users to CMS, 55
adding and applying licenses
  error message, 220
  Insight Control Data Center Edition, 67
  Insight Control Environment, 66
  Insight Control Environment for BladeSystem, 66
  Virtual Machine Management Pack licenses, 72
additional information, 251
addressing PMP performance issues with no hardware upgrade recommendation, 113
administration
  issues, 228
  monitoring, 126
agents
  deploying VMM Agent, 49
  upgrading VMM Agent, 52
Altiris Product Licensing Utility, 67
application requirements for installation, 21
applying
  licenses, 221
  RDP license file, 67
array, displaying status, 106
ASP.NET 1.1 installation error, 218
ATA disk
  inventory, 256
  status, 255
ATA Disk Array
  inventory, 255
  status, 255
Auto Refresh, 90
automatic system discovery, 53
B
Backing up and restoring VPM, 282
bay properties rule configuration, 147
benefits of HP Insight Control Management, 12
Boot from SAN installation, 148
Boot from SAN scripted install jobs, 139
bottlenecks, debugging, 93, 101
C
canceling scheduled tasks, 154
change rule setting, 147
CMS
  adding users, 55
  creating users, 55
color codes, performance, 197
comma-separated-value file. See CSV File Generator
components
  backup, 282
  delivered and licensed with Insight Control Management suites, 13
  restoration, 283
configuration
  mxagentconfig, 50
  OpenSSH, 50
  post-upgrade, 52
  VirtualCenter, 51
configuration fix
  deploying based on scan, 157
  scheduling deployment, 157
  troubleshooting, 246
  viewing deployment results, 157
configured virtual machine hosts, 170
configuring
  DNS server, 238
  domain accounts for Rapid Deployment Pack, 63
e-mail settings, 56
HP BladeSystem server blades, 140
HP Vulnerability and Patch Management Pack acquisition for Red Hat, 60
image installs, 137
parameters for HP Insight Control Management suites, 23
polling frequency for virtual machine status checks, 184
ports, 237
predeployment steps, 136
protocol settings, 57
rip-and-replace, 147
scripted installs, 138
troubleshooting, 235
virtual machine guest, 64
VPM, 276
console, HP Systems Insight Manager, 92
contact information, 253
controller, displaying graph, 97
controlling servers, 81
controls, using in Virtual Machine Management Pack, 171
copying
  operating systems to be deployed by Rapid Deployment Pack, 289
  virtual machine guests, 174
creating
  critical VM host collection, 187
  image, 142
  reference server, 142
  virtual machine guest backups, 177
  virtual machine guest templates, 176
CSV File Generator, 123
CSV File sample, 201
customized vulnerability scan
  definitions, 155
  deleting, 155
  deleting results by system, 156
  deleting scan results, 155
  deleting scan results by scan name, 155
customizing
  firewall, 238
  vulnerability scan definitions, 155
D
database
  configuration parameters, 23
  issues with PMP components, 232
  requirements for installation, 21
debugging
  server bottleneck, 93
  storage bottleneck, 101
  virtual machine host and guest bottleneck condition, 107
default PMP settings, 85
definition provided scan, 275
deleting
  customized vulnerability scan, 155
  customized vulnerability scan results, 155
  customized vulnerability scan results by name, 155
  customized vulnerability scan results by system, 156
  users, 56
deploying
  fixes, 149, 156
  HP SIM certificate on Virtual Machine Management Pack, 184
  imaging, 144, 145
  patches, 149, 156
  patches based on a scan, 157
  patches without a scan, 159
  scheduling VPM patch agent deployment, 162
  setting change rule, 147
  virtual machine guests, 176
  virtual machine hosts manually, 49
  VMM Agent from HP SIM, 50
  VMM Agent from the HP SIM menu, 50
  VPM Patch Agent, 162
deploying hardware configuration, 144, 145
deploying servers, 136
discovery, HP Systems Insight Manager, 63
disk space requirements for installation, 20
displaying
  array, 106
  hard disk status, 107
  logical drive under network storage, 104
  memory graph, 95
  memory status, 94
  network storage enclosure, 105
  network storage status, 103
  storage status, 102
  the controller, 97
  the drive, 99
  the inventory, 100
  the port, 98
DNS server, 238
domain accounts configuring for Rapid Deployment Pack, 63
drive array
  inventory, 256
  status, 256
drives
displaying graph, 99
displaying inventory, 100
displaying status, 107
unassigned, 116
DVD drive requirements for installation, 20
E
editing users, 56
e-mail settings, configuring, 56
enabling
automatic system discovery, 53
network storage logging, 127
enabling rip-and-replace, 147
Enclosure view, 77
enclosures
displaying status, 105
managing, 75
error when trying to apply license from License Manager, 220, 221
establishing security, 70
events
automatic handling of, 186
handling, 185
scan, 284
semiautomatic handling of, 186
setting up prefailure, 185
viewing patch deployment, 157
viewing patch removal, 163
viewing patch validation results, 161
viewing VPM Patch Agent deployment, 162
Vulnerability and Patch Management, 283
Events tab, 76
expanding the local storage, 96
Extensions for HP SIM on Microsoft Windows
additional information, 251
configuration parameters, 23
HP-UX Configuration Tools, 79
HP-UX Workload Manager, 80
Ignite-UX, 79
installation time, 32
OpenView GlancePlus, 79
overview, 77
Process Resource Manager, 80
Software Distributor-UX, 79
System Management Homepage, 79
upgrading, 19
external storage enclosure
inventory, 257
status, 257
F
failed host recovery, 187
features
HP iLO Power Management Pack, 12
HP iLO Power Management Pack for BladeSystem, 12
HP Insight Control Data Center Edition, 11
HP Insight Control Environment (ProLiant ML/DL servers), 11
HP Insight Control Environment for BladeSystem, 11
HP Insight Control Management, 10
Fibre Channel host bus adapter
inventory, 258
status, 257
file structure requirements for installation, 20
firewall settings, 238
fixes, 156
deploying, 149, 156
deploying based on a vulnerability scan, 157
frames, 87
functionality, 86
G
generating a CSV file, 123
generating reports in HP SIM, 199
graph, using, 96
guest, setting up, 64
H
half-duplex port, 115
handling events
automatic, 186
semiautomatic, 186
hardware installation requirements, 20
hardware requirements, Vulnerability and Patch Management Pack, 278
help resources, 250, 251
host buses
balancing, 117
inventory, 258
status, 258
host licensing virtual machine, 72
HP BladeSystem infrastructure, 251
HP BladeSystem Integrated Manager
  additional information, 251
  Enclosure view, 77
  Events tab, 76
  installation time, 32
  managing racks and enclosures, 75
  rack view, 76
  System(s) tab, 76
  upgrading, 19
  using, 75
  working with the System page, 77
HP BladeSystem server blades
  configuring, 140
  deploying, 144
  enabling rip-and-replace, 147
HP BladeSystem servers
  deploying, 145
HP iLO Power Management Pack (ProLiant ML/DL servers)
  adding and applying licenses, 68
  components, 13
  features, 12
  overview, 12
HP iLO Power Management Pack for BladeSystem
  components, 13
  features, 12
  overview, 12
HP Insight Control Data Center Edition
  adding licenses, 67
  components, 13
  features, 11
  licensing preparation, 66
  overview, 11
HP Insight Control Environment
  adding and applying licenses, 66
  features, 11
  licensing preparation, 66
HP Insight Control Environment (ProLiant ML/DL servers)
  components, 13
  overview, 11
HP Insight Control Environment Advisor, 23
  installation time, 32
  upgrading, 19
HP Insight Control Environment for BladeSystem
  adding and applying licenses, 66
  components, 13
  features, 11
  licensing preparation, 66
  overview, 11
HP Insight Control Management
  introduction, 10
HP Insight Power Manager
  additional information, 251
  configuring options, 81
  licensing managed systems, 68
  managing license keys, 68
  post-installation configuration tasks, 62
  upgrading, 19
HP Installation and Startup Service for HP BladeSystem
  infrastructure, 251
HP Open Service Event Manager (OSEM), 13
HP OpenView GlancePlus, 79
HP Performance Management Pack
  additional information, 251
  default PMP settings, 85
  installation time, 32
  monitoring PMP parameters, 85
  number of samples, 85
  Offline Analysis, 86
  Online Analysis, 86
  reference matrix, 254
  sample rate, 85
  upgrading, 19
  using, 86
HP Rapid Deployment Pack
  additional information, 251
  configuration parameters, 23
  configuring domain accounts, 63
  connecting the server blades, 140
  licensing, 67
  predeployment configuration, 136
  upgrading, 19
  using, 139
HP Rapid Deployment Pack installation time, 32
HP Rapid Deployment Pack SIM Integration Module, installation time, 32
HP Service Essentials Remote Support Pack installation time, 32
HP Service Essentials Remote Support Pack Setup, 58
HP Service Essentials Remote Support Software Pack
  configuring, 57
HP SIM. See HP Systems Insight Manager
HP Systems Insight Manager
accessing target systems, 63
additional information, 251
configuration parameters, 23
console, 92
discovery, 63
generating reports, 120, 199
initial setup tasks, 52
installation time, 32
integration, 249
integration issues, 225
managing server blades, 75
printing reports, 200
reports, 199
troubleshooting, 249
upgrade version, 19
HP Systems Insight Manager initial setup tasks
adding users to CMS, 55
configuring e-mail settings, 56
configuring protocol settings, 57
creating users for CMS, 55
enabling automatic system discovery, 53
setting up managed systems, 56
HP Virtual Machine Management Pack
adding licenses, 72
additional information, 251
infrastructure, 198
installation time, 32
licensing, 72
overview, 166
setting up virtual machine hosts, 63
upgrading, 19
HP Vulnerability and Patch Management Pack
acquiring updates, 60
additional information, 251
configuring acquisition for Red Hat, 60
customizing vulnerability scan definitions, 155
deleting a customized vulnerability scan, 155
deleting vulnerability scan results, 155
deploying patches and fixes, 156
deploying patches and fixes based on a vulnerability scan, 157
deploying patches without a vulnerability scan, 159
deploying the VPM Patch Agent, 162
installation time, 32
modifying, 59
overview, 149
performing post-installation configuration tasks, 59
provided scan definitions, 153
removing patches, 163
scanning for vulnerabilities, 153
target systems, 62
upgrading, 19
validating installed patches, 161
viewing the patch reboot status, 159
viewing vulnerability scan results, 154
HP Workload Management Pack, 13
HP-UX
HP-UX Workload Manager, 80
IDE channel
inventory, 258
status, 258
IDE controller
inventory, 259
status, 259
Identity tab
virtual machine guest, 168
virtual machine host, 167
Ignite-UX, 79
ignore change option, 147
IIS configuration in RDP uninstaller, 223
IIS issue, 221
iLO browser
interface, 83
Remote Console tab, 84
System Status tab, 83
Virtual Devices tab, 85
imaging
creating, 142
deploying, 144, 145
imaging jobs, 137
initial deployment job, 147
initial setup tasks in HP SIM, 52
Insight Control Environment (ICE) Advisor, 222
Insight Control Management installation does not accept username, password already accepted by HP SIM, 222
Insight Control Management Services, installation time, 32
installation issues, 219, 224
logs, 235
OpenSSH on HP SIM CMS, 50
OpenSSH on Windows-based virtual machine hosts, 50
post-upgrade configuration, 52
reinstalling Vulnerability and Patch Management, 243
requirements, 20
scripted, 138
troubleshooting, 235
uninstalling, 242
upgrading with HP Insight Control Management
Integrated Installer components, 19
installation process
HP Insight Control Management software, 18
installation times for HP Insight Control Management
components, 32
installed patches
validating, 161
viewing, 216
installing
HP Insight Control Management software, 18
Microsoft Virtual Server Additions, 64
ProLiant or Integrity Support Pack on Linux system, 57
ProLiant Support Pack on Windows systems, 56
required software on HP-UX system, 57
VMware tools, 64
VMware Tools, 64
installing HP Insight Control Management, 33
integrated installer components, 18
Integrated Lights-Out (iLO)
adding iLO 2 license keys, 69
additional information, 251
integration, HP Systems Insight Manager, 225, 249
Internet Information Services
scan definition, 275
troubleshooting, 240
introduction, 10
IP address, 87
L
launching
remote access, 180
Remote Console, 180
Remote Desktop, 181
System Center Virtual Machine Manager, 190
virtual network computing, 182
VirtualCenter, 191
License Manager
error appears when trying to apply license, 221
License Manager error appears when trying to apply
license, 220
licenses
adding, 67
applying, 221
free licenses for Virtual Machine Management Pack, 72
issues, 228
preparing for licensing Virtual Machine Management
Pack, 72
purchased, 67
virtual machine host, 72
Virtual Machine Management Pack, 72
licensing
HP Insight Control Management, 13
HP Insight Control Management suites, 65
HP Insight Power Manager managed systems, 68
HP Rapid Deployment Pack, 67
HP Virtual Machine Migration Pack, 72
Integrity and Storage Systems, 124
virtual machine guests, 125
virtual machine hosts, 125
log days, 130
logged files, deleting, 91, 135
logical drive
inventory, 260
status, 259
logs, installation, 235
M
managed systems, setting up, 56
Management Agents, modifying, 131
managing
enclosures, 75
racks, 75
managing Insight Power Manager license keys, 68
manual log purge, 91
Manual Log Purge, 91, 135
measurement categories
Fibre Channel enclosures, 205
Fibre Channel host bus adapters, 204
host buses, 206
IDE controllers, 206
network adapters, 206, 207, 210
SCSI adapters, 205
SCSI buses attached to SCSI adapters, 205
SCSI buses attached to smart array controllers, 204
SCSI drives attached to SCSI adapters, 205
servers, 202, 203
smart array controllers, 203
smart array logical drives, 204
smart array physical arrays, 204
VM Guest, 203
memory
displaying graph, 95
displaying status, 94
inventory, 261
memory status, 260
memory requirements for installation, 20
Microsoft Data Engine (MSDE)
troubleshooting, 236
updating, 235
Microsoft Virtual Server
Additions, 64
guest system page, 191
host system page, 190
Microsoft Virtual Server Additions
installing, 64
modes, 87, 90, 129
modifying
HP Vulnerability and Patch Management Pack, 59
log days, 130
Management Agents, 131
Management Agents from Internet Explorer, 132
monitoring status, 126
number of samples, 130
performance threshold settings, 130
sample rate, 130
scheduled tasks, 154
monitoring
administration, 126
issues, 228
parameters, 129
servers, 81
status, 87, 126
moving virtual machine guests, 175
multisystem aware tools, 194
mxagentconfig, 50
N
network adapter
inventory, 261
status, 261
network connections
inventory, 262
status, 261
network port
inventory, 262
status, 262
network share
inventory, 265
status, 264
network storage
debugging bottleneck, 101
displaying logical drive, 104
Network Storage Analysis, 88
network storage array, 263
inventory, 263
status, 263
network storage controller
inventory, 263
status, 263
network storage enclosure
inventory, 264
status, 264
network storage logical drives, 264
network, displaying storage status, 103
number of samples, 87
number of samples, modifying, 130
O
Offline Analysis
manual mode, 90
Performance Management Pack tool, 86
performing, 118
Online Analysis
Performance Management Pack screen, 93
Performance Management Pack tool, 86
performing, 118
screen, 101
OpenSSH
configuration, 50
installing on HP SIM CMS, 50
installing on Windows-based virtual machine hosts, 50
operating system
deploying, 144, 145
requirements for installation, 21
operation, modes, 129
overview
HP iLO Power Management Pack (ProLiant ML/DL servers), 12
HP iLO Power Management Pack for BladeSystem, 12
HP Insight Control Data Center Edition, 11
HP Insight Control Environment (ProLiant ML/DL servers), 11
HP Insight Control Environment for BladeSystem, 11
HP Insight Control Management, 10
Virtual Machine Management Pack, 72, 166
Virtual Machine Management Pack infrastructure, 198

parameters, monitoring, 129

patch
deploying, 149, 156
deploying agent, 162
deploying based on a vulnerability scan, 157
deploying without a scan, 159
reboot status, 159
reinstallation, 161
removing, 163
scheduling deployment, 157
scheduling validation, 161
scheduling VPM Patch Agent deployment, 162
troubleshooting, 246
validating installed, 161
viewing deployment results, 157
viewing installed, 216
viewing removal results, 163
viewing repository, 159
viewing validation results, 161
patch acquisition, 247
patch acquisition errors, 247
patch deployments, 248
patch detection, 248
patch installation fails, 248
patch installation status
viewing, 213
viewing by search filter, 215
viewing by system, 216
patch installation status reports, 248
patches in scan report, 247
patches missing, 247
PCI bus
inventory, 265
status, 265
performance information, 194
Performance Management Pack
compact issues, 230
graph, 96
issues, 227
Performance Management reference matrix
ATA disk, 255
ATA disk array, 255
drive array, 256
external storage enclosure, 257
Fibre Channel host bus adapter, 257
host buses, 258
IDE channel, 258
IDE controller, 259
memory, 260
network adapter, 261
network connections, 261
network port, 262
network share status, 264
network storage array, 263
network storage controller, 263
network storage enclosure, 264
PCI bus, 265
processors, 266
SAS drive, 273
SATA drives, 272
SCSI adapter, 267
SCSI drive, 269
SCSI storage enclosure, 268
Smart Array controller, 270
Smart Array SCSI drive, 271
static analysis, 254, 259, 270, 271
storage components, 274
performance threshold settings, 130, 183
performing
post-installation tasks for Insight Power Manager, 62
post-installation tasks for Vulnerability and Patch
Management Pack, 59
static analysis, 114
performing an integrated installation, 33
PF column refresh interval, 225
platform support, 13
PMP default settings, 85
PMP reports, 88
polling frequency, 184
port
displaying graph, 98
Linux requirements, 245
required, 237
port, half-duplex, 115
post-installation configuration tasks
configuring domain accounts for Rapid Deployment Pack, 63
configuring HP Service Essentials Remote Support Software Pack, 57
performing additional Vulnerability and Patch post-installation configuration tasks, 59
performing HP SIM initial setup tasks, 52
performing Insight Power Manager post-installation configuration tasks, 62
procedures, 48
setting up virtual machine guests for Virtual Machine Management Pack, 64
setting up virtual machine hosts for Virtual Machine Management Pack, 63
prefailure events
automatic, 186
overview, 185
seмаutomatic, 186
printing reports in HP SIM, 200
Process Resource Manager, 80
processor requirements for installation, 20
processors
inventory, 266
status, 266
product configuration, installation time, 32
product installation, 33
product installation time, 32
product troubleshooting, 218
protocol settings, configuring, 57
protocol, community string, and discovery range configuration parameters, 23
proxy configuration parameters, 23
R
Rack view, 76
racks, managing, 75
radia uses installation account instead of local account, 242
Reboot for install/upgrade, installation time, 32
reboot status, 159
recovering, virtual machines of a failed host, 179
recovery
failed hosts, 187
scheduling for virtual machine of failed hosts, 188
setting up, 187
Red Hat Linux troubleshooting, 249
redeployment options, 147
reference server, creating, 142
refresh mode, 90
registering for Software Technical Support and Update Service, 69
registering virtual machine hosts from HP SIM, 183
using the CLI, 184
reinstalling VPM to a new host, 283
remote access, launching, 180
Remote Console, launching, 180
Remote Desktop, launching, 181
removing IIS configuration in RDP uninstaller, 223
removing patches, 163
removing, alternate virtual machine hosts, 179
reports
CSV file, 123, 201
generating, 120
generating in HP SIM, 199
HP SIM, 199
overall PMP performance, 210
PMP measurement categories, 202
sample PMP server availability report, 213
sample PMP static analysis report, 212
sample PMP system summary report, 207
sample PSP CSV file, 201
server availability, 124
Static Analysis Report, 114, 121, 212
System Summary Report, 122, 207, 213
repository, patch, 159
requirements
configuration, 136
resetting virtual machine guests, 173
resource allocation, 197
restarting
virtual machine guests, 173
VMM Agent, 182
restoring
last virtual machine guest backups, 178
virtual machine guest backups, 178
Restoring and backing up VMP, 282
Results frame, 87
resuming virtual machine guests, 172
rip-and-replace, 147
Root installation directory and existing Rapid Deployment Pack configuration parameters, 23
run job option, 147

S
sample navigation, 90
sample rate, modifying, 130
SAN-attached scripted install jobs, 138
SAS drive
inventory, 273
status, 273
SATA drive
inventory, 272
status, 272
scan
provided, 275
required ports, 237
troubleshooting, 243
scan definition
Internet Information Services, 275
provided scans, 281
Vulnerability and Patch Management Pack definitions, 153
scanning vulnerabilities, 153
scheduled tasks
canceling, 154
modifying, 154
viewing, 154
scheduling recovery of virtual machine hosts, 188
scripted installation, 138
SCSI adapter
inventory, 267
status, 267
SCSI drive
inventory, 269
status, 269
SCSI speed, 117
SCSI storage enclosure
inventory, 268
status, 268
SCVMM. See System Center Virtual Machine Manager
security, establishing, 70
server
debugging bottleneck, 93
requirements for installation, 20
Server Information frame, 87
server name, 87
Server Tree frame, 87
services requirements for installation, 21
setting performance thresholds, 133
setting up
alternate virtual machine hosts, 179, 187
managed systems, 56
performance thresholds, 183
prefailure events, 185
recovery feature, 187
virtual machine hosts, 63
setting up managed systems
installing an HP ProLiant or Integrity Support Pack on a Linux system for the first time, 57
installing ProLiant Support Pack on Windows systems for the first time, 56
installing the required software on an HP-UX system, 57
shutting down virtual machine guests, 172
Smart Array controller
inventory, 271
status, 270
Smart Array SCSI drive status, 271
Smart SCSI drive inventory, 271
SMH. See System Management Homepage
software
installation requirements, 21
inventory details, 200
Vulnerability and Patch Management Pack, 279
Software Distributor-UX, 79
Software Technical Support and Update Service, 69
software update utility, 46
software updates for Insight Control Management Software, 46
SQL queries list, generating, 121, 122, 123, 124
starting virtual machine guests, 172
static analysis, 254, 259, 270
Static Analysis Report
generating, 114, 121
performing, 114
sample, 212
scenarios of servers running with VMware ESX operating systems, 121
status
monitoring, 126
reboot, 159
stopping virtual machine guests, 172
storage components
displaying status, 102
inventory, 274
status, 274
suite icons, 17
supported configurations, 73
supported suites, 18
suspending virtual machine guests, 173
System Center Virtual Machine Manager, launching, 190
System Management Homepage, 79
System Summary Report
  sample, 207, 213
system summary report for a VMware ESX Host, 209
System Summary Report, generating, 122
System(s) tab, 76
systems accessing, 243
T
target systems
  identifying, 280
Linux requirements, 245
  managed by the Vulnerability and Patch Management Pack, 62
  required ports, 237
task
  scheduling patch deployment, 157
  scheduling patch validation, 161
  scheduling VPM Patch Agent deployment, 162
task execution process, 170
technical support, 250
threshold
  settings, 197
  values, 134
tools, using in Virtual Machine Management Pack, 171
troubleshooting, 218
  administrator credentials have been changed, 239
  all target systems do not have same administrator credentials, 239
  applying licenses, 220, 221
ASP.NET 1.1 installation error, 218
cannot modify VPM acquisition settings to acquire updates from a local repository, 237
changing the IIS IWAM user name and password, 240
configuration, 235
configuration fix, 246
current patch information is not displayed in scan reports, 246
database, 232
HP Systems Insight Manager, 225
HP Systems Insight Manager integration, 249
IIS issue, 221
Insight Control Management installation does not accept
  username, password already accepted by HP SIM, 222
installation, 224, 235
installation fails with Product RMS not installed, 236
installation issues, 219
Internet Information Services, 240
licensing, 228
monitoring, 228
multiple VPM servers, 239
patches, 246
Performance Management Pack, 227, 230
PMP installation issues, 223
Radia internal error listed in HP SIM event log, 248
remaining VPM files, 243
removing IIS configuration in RDP uninstaller, 223
scan reports cannot be viewed, 245
scan results are inaccurate because of overlapping tasks, 245
scan was submitted but never started, 245
STAT Scanner update error listed in HP SIM event log, 248
uninstallation, 224
validate installed patches event does not complete, 249
verifying environment functionality with ICE Advisor, 222
VPM installation fails, 237
VPM Patch Agent installation fails, 246
Vulnerability and Patch Management Pack, 235
Vulnerability and Patch Management Pack installation fails with, 236
vulnerability scan, 243
vulnerability scan for Windows, 243
vulnerability scan for Windows VPM server, 244
vulnerability scan for Windows XP, 244
Windows Server 2003, 234
U
unconfigured virtual machine hosts, 170
uninstalling HP Insight Control Management, 19
uninstalling Vulnerability and Patch Management Pack, 242
unregistering virtual machine hosts, 184
unsupported configurations, 74
Updating VPM credentials, 282
upgrading
  Insight Control Management, 19
  Microsoft Data Engine, 235
upgrading with HP Insight Control Management Integrated Installer components, 19
usage scenario, 86
users
  adding to CMS, 55
  creating for CMS, 55
  deleting, 56
  editing, 56
using PMP, 92
V
validation
  installed patches, 161
  scheduling, 161
  viewing results, 161
VC. See VirtualCenter
viewing
  patch installation status, 214
  scheduled tasks, 154
  vulnerability scan guidelines, 154
  vulnerability scan results, 154
  vulnerability scan results by scan name, 154
  vulnerability scan results by system, 155
virtual machine guests
  copying, 174
  creating backups, 177
  creating templates, 176
  debugging a bottleneck condition, 107
  deploying, 176
  discovery, 63
  displaying the virtual machine guest, 111
  displaying the virtual machine guests page, 110
  displaying the virtual machine guests processor status, 112
  enabling logging, 128
  Identity tab, 168
  installing Microsoft Virtual Server Additions, 64
  installing VMware tools, 64
  moving, 175
  performance, 196
  recovering from a failed host, 179
  resetting, 173
  restarting, 173
  restoring backups, 178
restoring last backup, 178
resuming, 172
setting up, 64
shutting down, 172
starting, 172
stopping, 172
suspending, 173
viewing performance, 196
virtual machine hosts
  debugging a bottleneck condition, 107
  deploying VMM Agent, 49
  discovery, 63
  displaying, 109
  enabling logging, 128
  Identity tab, 167
  licensing, 72
  performance, 194, 195
  recovering when failed, 187
  registering from HP SIM, 183
  registering using the CLI, 184
  removing alternate, 179
  scheduling recovery, 188
  selection, 108
  setting alternate, 179, 187
  setting up for Virtual Machine Management Pack, 63
unregistering, 184
Virtual Machine Management Pack
  configuring on a Microsoft Cluster Server, 193
  controls, 171
  deploying HP SIM certificate, 184
  tools, 171
  virtual machines polling frequency, 184
virtual network computing, launching, 182
VirtualCenter
  information, 192
  launching, 191
  viewing, 192
virtualization and consolidation of servers, 166
VMM Agent
  deploying, 49
  deploying from HP SIM, 50
  deploying manually, 49
  registering to Microsoft Windows virtual machine hosts, 49
  registering VMware ESX hosts, 49
  restarting, 182
upgrading, 52
VMware
copying operating systems to be deployed by Rapid Deployment Pack, 289
tools, 64
VirtualCenter settings, 51
VMware ESX Server
guest system page, 192
host system page, 191
VMware Tools, installing, 64
VNC. See virtual network computing
VPM Acquisition Utility, 280
acquisitions, 61
VPM Patch Agent
deploying, 162
installation, 248
viewing deployment results, 162
VPM server
acquisitions, 61
vulnerability
scanning, 153
Vulnerability and Patch Management Pack
acquisition events, 286
components, 275
events, 283
hardware requirements, 278
installation logs, 235
interface, 152
miscellaneous events, 287
patch and fix events, 285
reinstalling, 243
reinstalling to a new host, 283
scan events, 284
software requirements, 279
troubleshooting, 235
uninstalling, 242
vulnerability scan
customizing definitions, 155
deleting, 155
deleting results by scan name, 155
deleting results by system, 156
provided, 275
required ports, 237
results by scan name, 154
results by system, 155
results guidelines, 154
troubleshooting, 243
viewing results, 154
vulnerability scan definitions, customizing, 155
vulnerability scan results, viewing, 154
W
wait option, 147
Windows copying operating systems to be deployed by Rapid Deployment Pack, 289
Windows operating system entering domain name, 55
Windows Server 2003 issues, 234
Windows Sysprep images, 137
Windows Sysprep jobs, 137