HP Systems Insight Manager 7.4 Installation and Configuration Guide for Linux

HP Part Number: 418811-404
Published: September 2014
Edition: 1

Legal Notices

Acknowledgments

Warranty

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight Management products.

Contents

1 Installation overview and requirements....5
First time install process overview....5
Upgrade overview....5
System requirements....5
Support for Adobe Flash player....5
Part 1: Linux Central Management Server....5
Part 2: Managed system requirements and recommendations....8
Installing Red Hat Enterprise Linux (RHEL) version 6.0....17
Managed storage system....18
SSH requirements....18
Foreign language support....18
HP CloudSystem Integrated Manager requirements....18
System support....18
Hardware support....19
2 Installing HP SIM on the CMS for the first time....26
Preparing the system....26
Installing and configuring the software....27
Automatically installing HP SIM....27
Manually installing HP SIM....28
After installing HP SIM....29
Enabling Linux VCRM features....33
Next steps....34
3 Setting up managed systems....35
Installing the ProLiant or Integrity Support Pack on a Linux system for the first time....35
Setting up managed storage systems....35
Installing SMI-S providers....35
Verifying SSL....35
Configuring SMI-S providers....36
Configuring HP SIM to discover storage systems....36
RHEL 6.3 installation instructions....36
4 Configuring HP SIM....38
Configuring HP Systems Insight Manager using the First Time Wizard....38
Configuring HP SIM using the Options menu....39
Setting up Linux managed systems manually....40
5 Upgrading from HP SIM....42
Upgrading HP SIM in Linux....42
6 Uninstalling HP SIM....45
Uninstalling HP SIM from a Linux system....45
7 Configuration options....46
CPU utilization during data collection....46
Overview....46
Implementation....46
GUI time-out policy....46
Overview....46
Implementation....47
Systems Insight Manager audit log configuration....47
Overview....47
Implementation....48

Configuring task results....48
8 Troubleshooting....50
9 Support and other resources....53
Information to collect before contacting HP....53
How to contact HP....53
Security bulletin and alert policy for non-HP owned software components....53
Subscription service....53
Registering for software technical support and update service....54
How to use your software technical support and update service....54
HP authorized resellers....54
Related information....54
Documents....54
Websites....55
Typographic conventions....55
10 Documentation feedback....56
Glossary....57
Index....70

1 Installation overview and requirements

This chapter provides an overview of the HP Systems Insight Manager installation process, and it identifies the system requirements for a Linux CMS, a managed system, and a network client.

First time install process overview

Perform these steps for a first time install of HP Systems Insight Manager on your CMS:

1. Install and configure the CMS. For details, see "Installing HP SIM on the CMS for the first time" (page 26).
2. Install and configure the required Insight Management Agents on the systems that will be managed by the CMS. For more information, see "Setting up managed systems" (page 35).
3. Configure HP SIM for your environment. For more information, see "Configuring HP SIM" (page 38).

Upgrade overview

If HP SIM has previously been installed on your CMS proceed to the upgrade instructions in "Upgrading from HP SIM" (page 42).

System requirements

This section identifies the hardware and software requirements and recommendations for HP SIM. These requirements are broken into sections by the CMS, managed system, and network client.

Support for Adobe Flash player

HP recommends that the version of Adobe Flash player must atleast be 10.3.183.11. This is a patched version of Adobe Flash player 10. Use the link http://www.adobe.com/support/security/bulletins/apsb11-28.html to download the latest patched version.

Part 1: Linux Central Management Server

Operating systems

- Red Hat Enterprise Linux 6.5 AMD64/EM64T
- Red Hat Enterprise Linux 6.5 x86
- Red Hat Enterprise Linux 6.4 x86
- Red Hat Enterprise Linux 6.4 AMD64/EM64T
- Kernel-Based Virtual Machine on Red Hat Enterprise Linux 6.4
- Red Hat Enterprise Linux 6.3 x86
- Red Hat Enterprise Linux 6.3 AMD64/EM64T
- Red Hat Enterprise Linux 5.10 x86
- Red Hat Enterprise Linux 5.10 AMD64/EMT64T
- Red Hat Enterprise Linux 5.9 x86
- Red Hat Enterprise Linux 5.9 AMD64/EM64T
- SUSE Linux Enterprise Server 11 x86, SP2
- SUSE Linux Enterprise Server 11 AMD64/EM64T, SP2

Supported 64-bit Linux operating systems running as guest on the following VMware systems:

- VMware Vsphere 5.5 Update 2 running guest Linux
- VMware Vsphere 5.5 Update 1 running guest Linux
- VMware ESXi 5.0 Update 3 running guest Linux
- VMware ESXi 5.0 Update 2 running guest Linux
- VMware ESXi 5.1 Update 2 running guest Linux
- VMware ESXi 5.1 Update 1 running guest Linux
- VMware ESXi 5.5 running guest Linux
- VMWare ESX 4.0/ESXi 4.0 Update 4 running guest Linux
- VMware ESXi 4.1 Update 3 running guest Linux
- VMware ESX 4.1 Update 3 running guest Linux

NOTE: HP SIM can run on a Linux Virtual Machine (VM) provided the following requirements are met. The VM must be hosted on ESX/ESXi 4.0 U4, ESX/ESXi 4.1 U3, ESXi 5.0 U2/U3, ESXi 5.1 U1 release through U2, ESXi 5.5 intial release through U2 or later server. The VM configuration must meet HP SIM hardware requirements and the CPU and Memory resources allocated to this VM must be always available to this VM (by reserving CPU and Memory resources).

NOTE: Installing a HP SIM on Linux Itanium Processor Family (IPF) is not supported. If you see the following error message, it is because you are attempting to manually install on an unsupported IPF system:

- `error: %pre(hpsim-C.06.x.00.00-1.i386) scriptlet failed, exit status 255`
- `error: install: %pre scriptlet failed (2), skipping hpsim-C.6.x.00.00-1`

Hardware

- Any HP IA-32 AMD64 or EM64T system with the following configuration:
  - Minimum: 1.5-GHz processor and 1 GB RAM
  - Recommended: 2.4-GHz processor and 2 GB RAM
- Free disk space:
  - 2 MB for CMS (/)
  - 400 MB for the CMS and DTF agent (/opt)
  - 500 MB minimum recommended for data (/var/opt)

Software

- General:
  - OpenSSH version 1.0 or later
  - ProLiant Support Pack for Linux 7.00 or later
  - Service Pack for ProLiant 2014.09.0 Gen9 Snap 1 updates
  - Oracle 11g R2 Enterprise

    NOTE: Oracle supports up to 5,000 systems and 50,000 events.

    NOTE: You must install the Oracle JDBC driver, version 11.2.0.4. You can download this driver from the Oracle website at _http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html.

    NOTE: The Oracle database must be created with Unicode character set of AL32UTF8 and national character set of AL16UTF16 before installing HP SIM. The NLS Length must be set to BYTE. You must also specify the thin client .jar file location. HP SIM requires Oracle database and Transparent Network Substrate (TNS) listener services to be up and running when system is restarted. Oracle by itself does not start the Oracle database and TNS listener automatically. An Oracle database administrator (DBA) must set these services to be restarted when the server is reset. See the Oracle documentation for details on how to auto start these services at http://docs.oracle.com/html/A96167_01/post-inst.htm. Access to this link requires registration. The Oracle DBA who manages the Oracle installation must perform this task.

  - PostgresSQL 8.2.1 (hpsmdb)

    NOTE: The hpsmdb version supports up to 500 systems and 5,000 events.

Browser software:

- Mozilla Firefox 3.x
- Mozilla Firefox 6.x
- Mozilla Firefox 9.x
- Mozilla Firefox 10.x
- Mozilla Firefox 24.0

Networking

- Static or dynamic host name resolution

NOTE: On Linux, look for the entry 127.0.0.1 localhost, the local system IP address, and the system name in the `/etc/hosts` file. If they are not present, add the entries manually.

- SNMP

Part 2: Managed system requirements and recommendations

Operating systems

- **Windows managed systems**
  - Windows Server 2008 R2 Standard, Server Core, SP1
  - Windows Server 2008 R2 Enterprise, Server Core, SP1
  - Windows Server 2008 Standard, Server Core, SP2
  - Windows Server 2008 Enterprise, Server Core, SP2
  - Windows Storage Server 2008 R2 Standard, SP1
  - Windows Storage Server 2008 R2 Enterprise, SP1
  - Windows Storage Server 2008 R2 Standard
  - Windows Storage Server 2008 R2 Enterprise
  - Windows Server 2008 Standard
  - Windows Server 2008 Enterprise
  - Windows Server 2008 Datacenter
  - Windows Server 2008 Small Business Server
  - Windows Server 2008 Web Ed
  - Windows Server 2008 Itanium-based
  - Windows Storage Server 2012 Standard R2
  - Windows Storage Server 2012 Standard
  - Windows Storage Server 2008 Standard (x64)
  - Windows Storage Server 2008 Enterprise (x64)
  - Windows Server 2008 R2 Standard, SP1
  - Windows Server 2008 R2 Enterprise, SP1
  - Windows Server 2008 R2 Datacenter, SP1
  - Windows Server 2008 R2 Web Server, SP1
  - Windows HPC Server 2008 R2
  - Windows Server 2008 R2 Standard
  - Windows Server 2008 R2 Enterprise
  - Windows Server 2008 R2 Datacenter

- Windows Server 2008 R2 Small Business Server
- Windows Server 2008 R2 Web Server
- Windows Server 2008 R2 Itanium
- Windows Server 2008 Standard, SP2
- Windows Server 2008 Standard (x64), SP2
- Windows Server 2008 Standard (x64)
- Windows Server 2008 Enterprise, SP2
- Windows Server 2008 Enterprise (x64), SP2
- Windows Server 2008 Enterprise (x64)
- Windows Server 2008 Datacenter, SP2
- Windows Server 2008 Small Business Server, SP2
- Windows Server 2008 Web Ed, SP2
- Windows Server 2008 Itanium-based, SP2
- Windows Storage Server 2008
- Windows 2003 R2 Standard
- Windows 2003 R2 Standard (x64)
- Windows 2003 R2 Standard, SP2
- Windows 2003 R2 Standard (x64), SP2
- Windows 2003 R2 Enterprise
- Windows 2003 R2 Enterprise (x64)
- Windows 2003 R2 Enterprise, SP2
- Windows 2003 R2 Enterprise (x64), SP2
- Windows 2003 R2 Datacenter
- Windows 2003 R2 Datacenter, SP2
- Windows 2003 Standard, SP1
- Windows 2003 Standard (x64), SP1
- Windows 2003 Standard, SP2
- Windows 2003 Standard (x64), SP2
- Windows 2003 Enterprise, SP1
- Windows 2003 Enterprise (x64) SP1
- Windows 2003 Enterprise (IA64) SP1
- Windows 2003 Enterprise, SP2

- Windows 2003 Enterprise (x64), SP2
- Windows 2003 Enterprise (IA64) SP2
- Windows 2003 Datacenter, SP1
- Windows 2003 Datacenter (x64), SP1
- Windows 2003 Datacenter (IA64), SP1
- Windows 2003 Datacenter, SP2
- Windows 2003 Datacenter (x64), SP2
- Windows 2003 Datacenter (IA64), SP2
- Windows 2003 Web Edition SP1
- Windows 2003 Web Edition SP2
- Windows Small Business Server 2011 Standard
- Windows Small Business Server 2011 Essentials
- Windows 7 SP1 (Professional/Enterprise) (x86)
- Windows 7 SP1 (Professional/Enterprise) (x64)
- Windows Vista (Business/Enterprise) SP2
- Windows Vista (Business/Enterprise) (x64) SP2
- Windows Vista (Business/Enterprise) (x86) SP2
- Windows Server 2012 Foundation
- Windows Server 2012 Essentials
- Windows Server 2012 Standard
- Windows Server 2012 R2 Standard
- Windows Server 2012 Datacenter
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V

- **HP-UX and HP NonStop Kernel managed systems**
  - HP-UX 11i v1 (11.11)
  - HP-UX 11i v2 Update 2 (11.23 PI-PA)
  - HP-UX 11i v3 (11.31 IA/PA)
  - HP NonStop Kernel
  - OpenVMS 8.3
  - OpenVMS 8.4

- **Linux managed systems**
  - Oracle Enterprise Linux 6.2 x86
  - Oracle Enterprise Linux 6.2 AMD64/EM64T
  - Oracle Enterprise Linux 5.8 x86
  - Oracle Enterprise Linux 5.8 AMD64/EM64T
  - Oracle Enterprise Linux 5.7 x86
  - Oracle Enterprise LInux 5.7 AMD64/EM64T
  - Oracle Enterprise Linux 5.6 x86
  - Oracle Enterprise Linux 5.6 AMD64/EM64T
  - Red Hat Enterprise Linux 6.5 x86
  - Red Hat Enterprise Linux 6.5 AMD64/EM64T
  - Red Hat Enterprise Linux 6.4 for x86
  - Red Hat Enterprise Linux 6.4 for AMD64/EM64T
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 7 AMD64/EM64T
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 6.5
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 6.4
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 5.5
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 5.6
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 5.7
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 5.8
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 5.10
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 6.1
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 6.2
  - Kernel-Based Virtual Machine on Red Hat Enterprise Linux 6.3
  - Kernel-Based Virtual Machine on SLES 11 SP2
  - Red Hat Enterprise Linux 7 AMD64/EM64T
  - Red Hat Enterprise Linux 6.3 IPF
  - Red Hat Enterprise Linux 6.3 x86
  - Red Hat Enterprise Linux 6.3 AMD64/EM64T
  - Red Hat Enterprise Linux 6.2 IPF
  - Red Hat Enterprise Linux 6.2 x86
  - Red Hat Enterprise Linux 6.2 AMD64/EM64T

- Red Hat Enterprise Linux 6.1 IPF
- Red Hat Enterprise Linux 6.1 x86
- Red Hat Enterprise Linux 6.1 AMD64/EM64T
- Red Hat Enterprise Linux 6 IPF
- Red Hat Enterprise Linux 6 x86
- Red Hat Enterprise Linux 6 AMD64/EM64T
- Red Hat Enterprise Linux 5.10 x86
- Red Hat Enterprise Linux 5.10 AMD64/EM64T
- Red Hat Enterprise Linux 5.9 IPF
- Red Hat Enterprise Linux 5.9 x86
- Red Hat Enterprise Linux 5.9 AMD64/EM64T
- Kernel-Based Virtual Machine on Red Hat Enterprise Linux 5.9
- Red Hat Enterprise Linux 5.8 IPF
- Red Hat Enterprise Linux 5.8 x86
- Red Hat Enterprise Linux 5.8 AMD64/EM64T
- Red Hat Enterprise Linux 5.7 IPF
- Red Hat Enterprise Linux 5.7 x86
- Red Hat Enterprise Linux 5.7 AMD64/EM64T
- Red Hat Enterprise Linux 5.6 IPF
- Red Hat Enterprise Linux 5.6 x86
- Red Hat Enterprise Linux 5.6 AMD64/EM64T
- Red Hat Enterprise Linux 5.5 IPF
- Red Hat Enterprise Linux 5.5 x86
- Red Hat Enterprise Linux 5.5 AMD64/EM64T
- Red Hat Enterprise Linux 5.4 IPF
- Red Hat Enterprise Linux 5.4 x86
- Red Hat Enterprise Linux 5.4 AMD64/EM64T
- Red Hat Enterprise Linux 5.3 IPF
- Red Hat Enterprise Linux 5.3 x86
- Red Hat Enterprise Linux 5.3 AMD64/EM64T
- Red Hat Enterprise Linux 5 IPF, Update 8
- Red Hat Enterprise Linux 5 x86, Update 8

- SUSE Linux Enterprise 11, SP3
- SUSE Linux Enterprise 11 IPF, SP3
- SUSE Linux Enterprise 11 x86, SP3
- SUSE Linux Enterprise 11 AM64/EM64T, SP3
- SUSE Linux Enterprise 11 IPF, SP2
- SUSE Linux Enterprise 11 x86, SP2
- SUSE Linux Enterprise 11 AMD64/EM64T, SP2
- SUSE Linux Enterprise 11 IPF, SP1
- SUSE Linux Enterprise 11 x86, SP1
- SUSE Linux Enterprise 11 AMD64/EM64T, SP1
- SUSE Linux Enterprise 10 IPF, SP4
- SUSE Linux Enterprise 10 x86, SP4
- SUSE Linux Enterprise 10 AMD64/EM64T, SP4
- SUSE Linux Enterprise 10 IPF, SP3
- SUSE Linux Enterprise 10 x86, SP3
- SUSE Linux Enterprise 10 AMD64/EM64T, SP3
- Debian 5.5
- Ubuntu 10.40 LTS
- Ubuntu 12.04 LTS
- Ubuntu 12.04.3
- Ubuntu 13.10
- Ubuntu 14.04

- **VMware managed systems**
  - VMware vSphere 5.5 Update 2
  - VMware vSphere 5.5 Update 1
  - VMware ESXi 5.5
  - VMware vSphere 5.1 Update 2
  - VMware ESXi 5.1 Update 1
  - VMware ESXi 5.1
  - VMware ESXi 5.0 Update 3
  - VMware ESXi 5.0 Update 2
  - VMware ESXi 5.0 Update 1

- VMware ESXi 5.0
- VMware ESX 4.1 Update 2
- VMware ESX 4.1 Update 1
- VMware ESXi 4.1 Update 3
- VMware ESX 4.1 Update 3
- VMware ESXi 4.1 Update 2
- VMware ESXi 4.1 Update 1
- VMware ESX 4.0 Update 4
- VMware ESX 4.0 Update 3
- VMware ESX 4.0 Update 2
- VMware ESXi 4.0 Update 4
- VMware ESXi 4.0 Update 3
- VMware ESXi 4.0 Update 2
- Xen on RHEL 5.8
- Xen on RHEL 5.7
- Xen on RHEL 5.6
- Xen on RHEL 5.5
- Xen on RHEL 5.4
- Xen on SLES10 SP4
- Xen on SLES10 SP3
- Xen on SLES 11 SP2
- Xen on SLES 11 SP1
- Integrity VM Windows (running guest OS Windows)
- Integrity VM Linux (running guest OS Linux)
- Integrity VM HP-UX (running guest OS HP-UX 11i v2)
- Integrity VM HP-UX (running guest OS HP-UX 11i v3)
- Microsoft Virtual Server 2005 R2 SP1
- Microsoft Virtual Server 2005 R2
- Microsoft Windows Server 2008 Hyper-V SP2 running guest Windows
- Microsoft Windows Server 2008 R2 Hyper-V SP1 running guest Windows
- Microsoft Windows Server 2008 R2 Hyper-V running guest Windows
- Microsoft Hyper-V Server 2008 SP2 running guest Windows

- Microsoft Hyper-V Server 2008 R2 SP1 running guest Windows
- Microsoft Hyper-V Server 2008 R2 running guest Windows
- Microsoft Hyper-V Server 2012 R2
- Microsoft Hyper-V Server 2012

- **Novell managed systems**
  - Netware 6.5
  - Netware 6.0
- **SUN managed systems**
  - Solaris 10 Sparc
  - Solaris 9 Sparc
  - Solaris 11 Intel Platform
  - Solaris 10 Intel Platform
  - Solaris 9 Intel Platform
  - Solaris 8 Intel Platform
- **IBM managed systems**
  - AIX 6.1
  - AIX 5.3

Hardware

- **For Windows:**
  - Any HP ProLiant system
  - Any HP Itanium-based system
- **For HP-UX:**
  - Any HP PA-RISC system
  - Any HP Itanium®-based system
- **For Linux:**
  - Any HP ProLiant system
  - Any HP Itanium-based system

Software

This software is not required, but if you want improved management capabilities, HP recommends that you install these components.

For Windows:

- OpenSSH Services 5.9 p1
- HP ProLiant Support Pack baselined at v 9.2
- HP Service Pack for ProLiant 2014.09.0 Gen9 Snap 1 updates
- HP Service Pack for ProLiant 2013.09.0 (B)

- HP Support Pack for ProLiant (SPP) 2013.02.0
- WBEM/WMI
- SNMP (recommended as an alternative to WBEM)

For Linux:

- SSH
- HP Service Pack for ProLiant 2014.09.0 Gen9 Snap 1 updates
- HP Service Pack for ProLiant 2013.09.0 (B)
- HP Service Pack for ProLiant (SPP) 2013.02.0
- HP Service Pack for ProLiant 2012.08.0
- SNMP (recommended as an alternative to WBEM)

This software is not required, but if you want improved HP SIM capabilities, HP recommends that you install these components, which can be purchased or downloaded from many software suppliers:

- SSH Client
- X Window Server

Required web browsers

- **For Windows:**
  - Google Chrome 3x.x
  - Microsoft Internet Explorer 9
  - Microsoft Internet Explorer 8
  - Microsoft Internet Explorer 10
  - Microsoft Internet Explorer 11
  - Mozilla Firefox Extended Support Release 24.0

  NOTE: For optimum performance, the minimum resolution for the browser must be 1024 x 768.

- **For HP-UX:**
  - Mozilla Firefox 3.5 (3.5.09.00)
  - Mozilla Firefox 3.6
  - Mozilla Firefox 3.x
  - Mozilla Firefox 6.x
  - Mozilla Firefox 9.x
  - Mozilla Firefox 10.x
- **For Linux:**
  - Mozilla Firefox ERS 17.0
  - Mozilla Firefox 24.0
  - Mozilla Firefox 10.x
  - Mozilla Firefox 9.x
  - Mozilla Firefox 6.x
  - Mozilla Firefox 3.x

  NOTE: For all Internet Explorer browsers, you must have the SSL 3.0 or TLS 1.0 browser security options enabled for HP SIM to work properly.

Installing Red Hat Enterprise Linux (RHEL) version 6.0

To install Red Hat Enterprise Linux (RHEL) version 6.0, follow these steps:

1. Choose **Basic Server**.
2. Select **Customize Now**.

3. Select the following additional libraries under **Base System**:
   - Compatibility libraries
   - Under Hardware Monitoring Utilities, the following must be selected
     - lm_sensors-3.1.1-10.el6-

Managed storage system

To view the latest information regarding HP SIM support for a particular storage system, including Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters), see the HP SIM SMI-S Provider web page at http://www.hp.com/go/hpsim/providers.

This webpage also offers information on obtaining and installing SMI-S providers.

SSH requirements

SSH is locally configured during HP SIM local installation on the CMS.

Custom tools on the **Tools** menu require SSH version 1.0 or later on the CMS to run properly. These commands run on the CMS with environment variables set to the context of specific events or devices.

You can install and configure SSH version 1.0 or later on each of the managed systems and have HP SIM exchange keys with the managed systems (through the `mxagentconfig` command or for Windows, through the Install SSH task). If you do this, then the **Command Line Tools** option on the **Tools** menu works for these managed systems. If you choose not to configure it to work with remote SSH clients, then these commands fail. There is no other loss of functionality without SSH.

Foreign language support

Japanese, Korean, Simplified Chinese, and Traditional Chinese are supported on all platforms as listed in "System requirements" (page 5). French, German, Italian, Spanish are supported on Windows systems only.

HP CloudSystem Integrated Manager requirements

HP CloudSystem Integrated Manager is comprised of blade computer systems, integrated connectivity to data and storage networks, and shared power subsystems. The HP CloudSystem Integrated Manager enables you to quickly navigate your HP CloudSystem environments including server blades and desktops, enclosure infrastructures, racks, and integrated switches, through hierarchical tree views/picture views. Users are able to conveniently manage individual or groups of blade systems.

System support

CloudSystem Integrated Manager manages blade infrastructures. For an updated list of supported systems, see http://h18002.www1.hp.com/products/servers/management/bsme/index.html. On the right side of the screen, select **Support & Documents**. Under Resources for HP CloudSystem Integrated Manager Software, select **Manuals**. Under General reference, select **HP BladeSystem Integrated Manager Support Matrix**.

Hardware support

Table 1 Supported HP c-Class platforms

Product Models	Minimum Software Management firmware version
BladeSystem c3000	2.00 or later
BladeSystem c3000 Tower Model	2.10 or later
BladeSystem c7000	1.30 or later

Table 2 Supported HP e-Class platforms

Product Models	Minimum Software Management firmware version
ProLiant BL 10e Enclosure	NA

Table 3 Supported HP p-Class platforms

Product Models	Minimum Software Management firmware version
ProLiant p-Class 1U Power Enclosure	2.40
ProLiant p-Class 3U Power Enclosure	2.40
ProLiant p-Class Enhanced Enclosure	2.40
ProLiant p-Class Standard Enclosure	2.40

Table 4 Supported c-Class Servers

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
AiO SB600c storage solution	2008.01.24	1.43	Microsoft Windows Storage Server 2003	7.91.0.0
HP carrier grade AMC Expansion	NA	NA	NA	NA
HP Tape Blade	NA	T61D[2]	Microsoft Windows 2000	NA
HP SB40c for HP c-Class Blade System	NA	2.0.0.0[2]	NA	NA
Integrity BL870c	03.11	TO2.05 or later	Windows, Linux, and HP-UX	NA
PCI expansion blades	NA	NA	NA	NA
ProLiant BL260c G6	NA	1.75 or later	Windows, Linux, Solaris, and NetWare	8.20
ProLiant BL260c G5	I20 02/14/2008	1.50 or later	Windows and Linux	8.00
ProLiant BL280c G6	I22 3/11/09	1.75	Windows and Linux	8.20
ProLiant BL460c	5/1/2007	1.24 or later	Windows and Linux	7.50 or later
ProLiant BL460c G6	I24 2/24/09	1.75	Windows and Linux	8.20
ProLiant BL465c	6/1/2005	1.24 or later	Windows and Linux	7.60 or later

Table 4 Supported c-Class Servers *(continued)*

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
ProLiant BL465c G5	9/12/2008	1.70	Windows Server 2003 and 2008, Linux, Solaris, and VMWare ESX Server	8.15
ProLiant BL480c	5/1/2007	1.24 or later	Windows and Linux	7.50 or later
ProLiant BL490c G6	I21 2/23/09	1.75	Windows and Linux	8.20
ProLiant BL495c G6	A14 05/07/2009	1.78	Windows 2003, Windows 2008, RHEL 5 Update 3, RHEL 4 (minimum Update 8), VMWare ESX 4.0.0 or later, XenSource, RedHat XEN, and SLES XEN	8.25
ProLiant BL495c G5	8/29/2008	1.61	Windows Server 2003 and 2008, Linux, and VMWare ESX Server	8.11
ProLiant BL680c G5	10/18/2007	1.35 or later	Windows and Linux	7.9 or later
ProLiant BL685c	6/1/2005	1.24 or later	Windows and Linux	7.60 or later
ProLiant BL685c G6	A17 2/14/2009	1.75	Windows and Linux	8.20
ProLiant BL2x220c G5	I19 03/03/2008	1.50 or later	Windows and Linux	8.00
ProLiant BLxw460c Blade Workstation	7/31/2007	1.30 or later	Windows XP or Vista, and Linux	7.91 or later
ProLiant xw2x220c Blade Workstation	09/16/2008	1.60	Windows XP or Vista	8.15
ProLiant BL460c G7	127 5/10/2010	iLO 3	Windows, RHEL, SLES, Oracle Solaris, VMware, and Citrix XenServer	PSP 8.7
ProLiant BL465c G7 (AMD Opteron 6100)	A19	iLO 3 version 1.05	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Solaris VMware ESX Citrix XenServer	PSP 8.7
ProLiant BL465c G7 (AMD Opteron 6200)	A19	iLO 3 version 1.05	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Solaris VMware ESX Citrix XenServer	PSP 8.7
ProLiant BL490c G7	I28 2011/01/29	iLO3	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Solaris	PSP 8.7

Table 4 Supported c-Class Servers *(continued)*

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
			VMware Citrix XenServer	
ProLiant BL620c G7	I25 7/9/2010	iLO 3	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Oracle Solaris VMware Server Citrix XenServer	PSP 8.7
ProLiant BL680c G7	I25 6/4/2010	iLO 3	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Oracle Solaris VMware Server Citrix XenServer	PSP 8.7
ProLiant BL685c G7 (AMD Opteron 6100)	A20	iLO 3 Version 1.05 and OA version 3.10	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Solaris VMware Citrix XenServer	PSP 8.7
ProLiant BL685c G7 (AMD Opteron 6200)	A20	iLO 3 version 1.05 and OA version 3.10	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Solaris VMware Citrix XenServer	PSP 8.7
ProLiant BL460c Gen8	I31 2011/12/21	iLO 4 version 1.01 or later and OA version 3.50	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Oracle Solaris VMware Citrix XenServer	HP Service Pack for ProLiant 2013.09.0
BL420c Gen8	I30, 08/20/2012	ILO4 firmware 1.10 or later, OA firmware 3.55	Microsoft Windows server, RHEL, SLES, Solaris, VMware	HP Service Pack for ProLiant 2012.10.0
ProLiant BL465c Gen8	A26, 08/14/2012	ILO4 firmware 1.10 or later	Microsoft Windows server, RHEL, SLES, Oracle Solaris, Vmware, Citrix Xenserver	HP Service Pack for ProLiant 2012.10.0
ProLiant BL460c G5	I23, 05/02/2011	ILO2 firmware 2.12 or later	Microsoft Windows Server Microsoft Windows Server Hyper-V, RHEL, SLES, Oracle Enterprise Linux (OEL) Solaris 10 for x86/x64 based	PSP 8.0 or later

Table 4 Supported c-Class Servers *(continued)*

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
			Systems, Vmware, Citrix XenServer	
ProLiant BL465c G6	A13, 05/02/2011	ILO2 firmware 2.12 or later	Microsoft Windows server, RHEL, SLES, Solaris 10 for x86/x64 based systems, VMware ESX, Citrix Xenserver	PSP 8.5 or later
ProLiant BL685c G5	A08, 05/02/2011	ILO2 firmware 2.12 or later	Microsoft Windows Server, Microsoft Windows Server Hyper-V, RHEL, SLES, Oracle Enterprise Linux(OEL), Solaris 10 for x86/x64 based Systems,Vmware, Citrix XenServer	PSP 8.0 or later
ProLiant BL2x220c G6	I26, 05/05/2011	ILO2 firmware 2.12 or later, OA firmware 2.6 or later	Microsoft Windows Server, RHEL, SLES, Solaris 10 for x86/x64 based Systems, Vmware, Citrix XenServer	PSP 8.3 or later
ProLiant BL2x220c G7	I29, 05/05/2011	ILO3 firmware 1.5 or later, OA firmware 3.11 or later	Microsoft Windows Server, RHEL, SLES Oracle Solaris, Vmware, Citrix Xenserver	PSP 8.7 or later
BL660c Gen8	12/20/2013 ; Gen8 ROM (I32) is 8/3/2014	iLO4 firmware 1.10 or later, OA firmware 4.30	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Solaris, VMware	HP Service Pack for ProLiant 2013.09.0b
BL460c Gen9	ROM-I36 ; 7/11/2014	iLO4 firmware 2.00 or later, OA firmware 4.30	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Solaris, VMware	HP Service Pack for ProLiant 2014.09.0 Gen9 Snap 1 updates

[1] For specific version of the operating systems, browse the ProLiant support matrix at http://h10018.www1.hp.com/wwsolutions/index.html

[2] Firmware - Storage Tape

Table 5 Supported Servers HP Consolidated Client Infrastructure (CCI)

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required

Table 5 Supported Servers HP Consolidated Client Infrastructure (CCI) *(continued)*

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
				Windows
ProLiant BL1000	2.04 A	4.01 Rev. A[2] 15 Jan 2008	Windows XP	NA
ProLiant BL1500	1.02 Rev. A	4.01 Rev. A[2] 15 Jan 2008	Windows XP or Vista	NA
ProLiant BL2000	2.06 Rev. A	4.01 Rev. A[2] 15 Jan 2008	Windows XP or Vista	NA
ProLiant BL2500	2.06 Rev. A	4.01 Rev. A[2] 15 Jan 2008	Windows XP or Vista	NA

[1] For specific version of the operating systems, browse the ProLiant support matrix at http://h10018.www1.hp.com/wwsolutions/index.html

[2] HP PC BL Enclosure Integrated Administrator

Table 6 Supported e-Class Servers

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
ProLiant BL 10e	2003.02.17 (C)	4.00 A[2] 7 Nov 2005	Microsoft Windows 2000	NA
ProLiant BL 10e G2	2003.02.17 (C)	4.00 A[2] 7 Nov 2005	Microsoft Windows 2000	NA

[1] For specific version of the operating systems, browse the ProLiant support matrix at http://h10018.www1.hp.com/wwsolutions/index.html

[2] HP ProLiant BL e-Class Integrated Administrator

Table 7 Supported p-Class Servers

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
Integrity BL60p	01.70	H.03.21	HP-UX	NA
ProLiant BL20p	2004.05.01 (14 May 2004)	1.70 or later	Windows and Linux	7.10 or later
ProLiant BL20p G2	4.09 (I04-09/16/2004)	1.70 or later	Windows and Linux	7.10 or later
ProLiant BL20p G3	2006.02.14 (25 May 2006)	1.80 or later	Windows and Linux	7.10 or later
ProLiant BL20p G4	2007.11.13 (A)	1.24 or later	Windows and Linux	7.50 or later

Table 7 Supported p-Class Servers *(continued)*

Product Models	Minimum BIOS — System ROM required	Minimum Integrated Lights-Out (iLO) / iLO 2 / firmware version required	Operating Systems Supported[1]	Minimum ProLiant Support Pack (PSP) required Windows
	(17 Jan 2008)			
ProLiant BL25p		1.70 or later	Windows and Linux	7.20 or later
ProLiant BL25p G2	2007.09.23 (A) (4 Dec 2007)	1.24 or later	Windows and Linux	7.60 or later
ProLiant BL25xwp		1.88 or later	Windows and Linux	
ProLiant BL30p	2005.10.27 (21 Jun 2006)	1.70 or later	Windows and Linux	7.10 or later
ProLiant BL35p		1.70 or later	Windows and Linux	7.20 or later
ProLiant BL40p	2003.07.25 (12 Aug 2003)	1.70 or later	Windows and Linux	7.10 or later
ProLiant BL45p		1.70 or later	Windows and Linux	7.20 or later
ProLiant BL45p G2	2007.09.23 (A) (4 Dec 2007)	1.24 or later	Windows and Linux	7.60 or later

[1] For specific version of the operating systems, browse the ProLiant support matrix at http://h10018.www1.hp.com/wwsolutions/index.html

Table 8 Supported c-Class Interconnects/Switches

Product Models	Minimum Software Management firmware version
Cisco Catalyst Blade Switch 3020 for HP c-Class Blade System	12.2(25)SEF1
Cisco Catalyst Blade Switch 3120G for HP	IP Base IOS firmware package[1]
Cisco Catalyst Blade Switch 3120X for HP	IP Base IOS firmware package[1]
Cisco MDS 9124e Fabric Switch	3.3(1a)
HP 1:10Gb Ethernet BL-c Switch	1.0.0
HP 1Gb Ethernet Pass-Thru Module for HP c-Class BladeSystem	NA
HP 10Gb Ethernet BL-c Switch	1.1.0
HP 1/10Gb Ethernet Blade Switch	1.0.0
HP 1/10Gb Virtual Connect Ethernet Module	1.22
HP 1/10Gb-F Virtual Connect Ethernet Fiber Module	1.22
HP 1/10Gb-F VC Module	NA
HP 3Gb SAS BL-c Pass-Thru Module	NA
HP 4Gb Fiber Channel Pass-Thru Module for c-Class BladeSystem	NA
HP 4Gb Virtual Connect Fiber Channel Module for c-Class BladeSystem	1.22
HP GbE2c Ethernet Blade Switch for HP	2.0.4

Table 8 Supported c-Class Interconnects/Switches *(continued)*

Product Models	Minimum Software Management firmware version
HP GbE2c Layer 2/3 Ethernet Blade Switch	2.0.4
HP Virtual Connect Flex-10 10Gb Ethernet Module for BladeSystem c-Class	2.25
HP Virtual Connect 8Gb Fibre Channel Module (24-port)	NA
Brocade 8Gb SAN Switch for HP BladeSystem c-Class	NA
HP NC382m Dual Port 1GbE BL-c Adapter	Boot code version 4.4.14 and MBA version 4.4.16
QMH2562 8Gb FC for HP BladeSystem c-Class	4.04.04
HP NC532m Dual port 10GbE BL-c Adapter	Boot code version 4.5.10 and MBA version 4.5.20
LPe 1205-HP 8Gb FC for c-Class	1.10a4
HP 3G SAS BL Switch Module	NA
HP VC FlexFabric-20/40 F8 Module	4.30

[1] For more information on the IP Base IOS firmware package, see www.hp.com.

Table 9 Supported e-Class Interconnects/Switches

Product Models	Minimum Software Management firmware version
HP BladeSystem PC Blade Switch	1.1.1.4 Rev. A
HP ProLiant BL e-Class (C-GbE) Interconnect Switch	2.1.6 A

Table 10 Supported p-Class Interconnects/Switches

Product Models	Minimum Software Management firmware version
Brocade 4GB SAN Switch for HP p-class Blade system	v5.3.0d
Mcdata 4GB SAN Switch for HP p-class Blade system	6.4.0.07.00
HP ProLiant BL p-Class Cisco Gigabit Ethernet Switch Module	12.2(44)SE
HP ProLiant BL p-Class GbE Interconnect Switch Module	2.1.9
HP ProLiant BL p-Class GbE2 Interconnect Switch Module	3.2.3.0

2 Installing HP SIM on the CMS for the first time

Preparing the system

Perform step 1 for a first time install of HP SIM on your CMS.

1. **Install and configure the CMS.**
2. Install and configure the required management software on the systems that will be managed by the CMS. For details, see "Setting up managed systems" (page 35).
3. Configure HP SIM for your environment. For more information, see "Configuring HP SIM" (page 38).

This procedure verifies that your system meets the minimum requirements and prepares your system for HP SIM installation.

To verify and prepare your system, perform the following procedure:

Procedure 1 Prepare the system

1. Verify your system meets the minimum requirements. For details, see "System requirements" (page 5).
2. Disable the firewall and/or Security-Enhanced Linux.

   Many Linux distributions automatically install security layers such as a firewall and/or Security-Enhanced Linux (SELinux) that can interfere with the operation of HP SIM. Configurations in the support matrix are tested without these options enabled.

   NOTE: If you chose to install HP SIM without disabling the SELinux environment, then must be opened for smooth operation. For enabling ports under the SELinux firewall, see Firewall Configuration.

3. If you plan to use an Oracle database, refer to your Oracle provider for instructions.

   NOTE: The Oracle database must be created with Unicode character set of AL32UTF8 and national character set of AL16UTF16 before installing HP SIM. The NLS Length must be set to BYTE. You must also specify the thin client .jar file location. HP SIM requires Oracle database and Transparent Network Substrate (TNS) listener services to be up and running when system is restarted. Oracle by itself does not start the Oracle database and TNS listener automatically. An Oracle database administrator (DBA) must set these services to be restarted when the server is reset. For details on how to automatically start these services, see the Oracle documentation at http://www.oracle.com/pls/db102/homepage. Access to this link requires registration. The Oracle DBA who manages the Oracle installation must perform this task.

   Install Oracle on the local system before installing HP SIM. Create a database user name with DBA privileges, or if you plan on using Oracle as the remote database, you must have the database and user name with DBA privilege to configure HP SIM. To configure HP Systems Insight Manager to use a newly created Oracle database, see "After installing HP SIM" (page 29).

4. Download the HP SIM software. To download the software, see http://www.hp.com/go/hpsim and on the upper-left of the page under HP Systems Insight Manager, click **Download**. The HP SIM **Download** Page appears. Under **Download HP Systems Insight Manager**, select **HP SIM-Linux** and **Download latest version of HP SIM-Linux** for a full product install.
5. In the directory where you downloaded or copied the files, change user permissions to add execute permissions to the `bin` file:

   ```
   chmod +x *.bin
   ```

   or

   ```
   chmod +x HPSIM*.bin
   ```

6. Verify that the following required software dependencies are available on your system, and install any that are not already installed.
   a. Verify that SSH is installed by executing the following command:

      `rpm -qa | grep ssh`

      If SSH is not installed, the previous command does not return any results. Install SSH from your Linux operating system CD before continuing with the HP SIM installation.
   b. Verify that SNMP is installed by executing the following command:

      `rpm -qa | grep snmp`

      If SNMP is not installed, the previous command does not return any results. Install SNMP from your Linux operating system CD before continuing with the HP SIM installation.
   c. Verify that standard C++ libraries (`compat-libstdc++`) are installed:

      `rpm -qa | grep compat`

      If the standard C++ libraries are not installed, the previous command does not return any results. Install them from your Linux operating system CD before continuing with the HP SIM installation.
   d. Verify that the Linux glibc library is installed. (Glibc is the C library shipped with many Linux distributions.)

      `rpm -qa | grep glib`

      If the Linux `glibc` library is not installed, the previous command does not return any results. Install the Linux `glibc` library from your Linux operating system CD before continuing with the HP SIM installation.
7. Optional: If you are planning to run the Firefox browser on the CMS, verify that Firefox 3.5 or later is installed. To verify which version is installed, open the Firefox browser, and select **Help→About Firefox**.

   NOTE: Firefox is not required on the CMS. It can be used to access HP SIM from any network client. Install Firefox 9 or later on the Linux managed node.

Installing and configuring the software

You can install HP SIM automatically or manually. An automatic install executes the `.bin` file, automatically installing hpsmdb (HP SIM private version of PostgresSQL) and HP SIM with minimal user interaction. A manual install requires that you execute the separate steps to unpack files and install hpsmdb and HP SIM. If you are installing HP SIM with an Oracle database, HP recommends the manual install. Installation of HP SIM includes the hpsmdb software dependency.

Automatically installing HP SIM

To install HP SIM with `hpsmdb`, execute the following command:

`./HPSIM-Linux*.bin`

NOTE: For information on setting permissions, see Step 5.

The `HPSIM-Linux*.bin` file will extract the RPM Package Manager (RPM) files, install hpsmdb, and then continue with the HP SIM installation.

NOTE: After installation is complete, log out of the operating system and then log back in to set all the correct file permissions and system environments.

NOTE: HP Linux VCRM is automatically installed along with HP SIM and HP SMH. The installer will do the automatic Upgrade of Linux VCRM and HP SMH if lower version is found pre-installed.

NOTE: Installing VCRM on Linux is only supported via HP SIM.

To complete the initial set up of HP SIM refer to "After installing HP SIM" (page 29).

Manually installing HP SIM

1. Extract the `.rpm` files from the `.bin` file. Set the permissions to include the right to execute the `.bin` file by executing the following command:

   `chmod u+x HPSIM-Linux-07.*.bin (where "HPSIM-Linux-C.07.*.bin" is the HPSIM package)` and then execute `./HPSIM-Linux-C.07.*.bin --noexec --target mxserver`

   NOTE: For information on setting permissions, refer to Step 5.

2. To change the directory to mxserver, execute the following command:

   `cd mxserver`

   NOTE: If you are using `hpsmd` as your database, continue with Step 3 through Step 5. If you are using Oracle as your database, skip to Step 6.

3. Install the hpsmdb database, using the appropriate `.rpm` files in the following order.

   NOTE: The `rpm -i hpsmdb-*.rpm` command installs hpsmdb on your system.

   - SUSE Linux Enterprise Server 11 SP2 or later

     `rpm -ivh hpsmdb-sles11-*.i586.rpm`

   - 64-bit SUSE Linux Enterprise Server 11 SP2 or later

     `rpm -ivh hpsmdb-sles11-*.x86_64.rpm`

   NOTE: If you are using SUSE 9 with older version of HP SIM, then you must upgrade to SUSE 11.

4. Verify that the hpsmdb status reads `running`.
   - For Red Hat Enterprise Linux (all versions):

     NOTE: By default, the **hpsmdb** service is configured to run in INIT 3 and 5 level.

     a. Execute the `serviceconf` command. The Service Configuration window appears.

     NOTE: Use the `ntsysv` command instead of `serviceconf` if you are running from a CLI prompt.

     b. Scroll down to the **hpsmdb** entry.
     c. Select the checkbox, save the changes, and then start the service.
     d. To start hpsmdb by using the command line, execute the following command:

     `/etc/rc.d/init.d/hpsmdb start`

     Or

```
/etc/init.d/hpsmdb start
```

- For SUSE Linux Enterprise Server 11 SP2 or later:
  a. View the status by executing the following command:

     ```
     /etc/init.d/hpsmdb status
     ```

  b. Configure hpsmdb to run during startup by executing the following command:

     ```
     chkconfig hpsmdb 345
     ```

  c. If the status is `unused` in any version of Red Hat Linux or SUSE Linux, start the daemon by executing the following command:

     - For SUSE Linux Enterprise Server 11 SP2 or later:

       ```
       /etc/init.d/hpsmdb start
       ```

     - For Red Hat Enterprise Linux (all versions)

       ```
       /etc/rc.d/init.d/hpsmdb start
       ```

       Or

       ```
       /etc/init.d/hpsmdb start
       ```

     NOTE: To install HP SIM on a system without OpenSSH or with a purchased version of SSH, use the **`--nodeps`** option on rpm.

     For example, **`rpm --nodeps -ivh`** followed by the rpm files.

5. If you are using hpsmdb as your database and hpsmdb is configured properly and running, install HP SIM using the `.rpm` files by executing the following command:

   ```
   rpm -ivh hpsim*.rpm
   ```

6. If you are using Oracle as your database, install HP SIM using `.rpm` files by executing the following command:

   ```
   rpm -ivh hpsim-C.7.x.rpm --nodeps
   ```

7. If you want to install Linux VCRM, execute the command: `rpm -ivh cpqsrhmo-*.linux.rpm`

   NOTE: It is mandatory to install HP SMH before installing Linux VCRM.

After installing HP SIM

Procedure 2

1. If you are using Oracle as your database, continue with step 2. If you are using `hpsmdb` as your database, continue with step 3.
2. For an Oracle database, run one of the following commands:

   ```
   mxoracleconfig
   ```

   located at `/opt/mx/bin` before proceeding with the following steps. This command can be invoked with or without command line arguments.

   ```
   mxoracleconfig
   ```

   You will be prompted for individual information for your Oracle database.

   Host: Enter the IP address or host name of the Oracle server.

   Port [1521]: Enter the same port number, then press **Enter**.

   Database name: Enter your database name.

   Username: Enter the username of your database.

Password: Enter the password of your database.

Oracle driver jar file: Enter the full location of the Oracle jar file.

Force [N]: Press **Enter**.

Or

You can use the **mxoracleconfig** command with all parameters as shown below:

```
mxoracleconfig -h hostname [-n port number] -d database name -u
username -p password [-j driver jar file location] [-f ]
```

-h Hostname

Full DNS name or IP address of the Oracle server.

-n Port number

Port number to be used to connect to the oracle instance. Default port is 1521.

-d Database name

Name of database instance.

-u Username

Database user name.

-p Password

Database password for the corresponding user name.

-j Driver file location

Full path to thin driver `.jar` file. This is not required if the `.jar` file is already in the class path for HP SIM and JBoss. `Mxoracleconfig` reports an error if the driver class cannot be loaded. `Mxoracleconfig` will not copy over a `.jar` file if it already exists in the class path for HP SIM and JBoss.

NOTE: By default, the **ojdbc14.jar** file is not shipped with HP SIM.

-f Force flag to force a re-run.

Typically, this command is run only once. This flag is provided if a re-run is required because of some type of user error such as specifying the wrong Oracle server or database instance.

NOTE: Execute the **mxoracleconfig** command before the **mxinitconfig** command so that mxinitconfig will use Oracle as the database.

3. Test the prerequisites by executing the following command:

   /opt/mx/bin/mxinitconfig -l

   This utility reports that all server components are `OK` and that it completed all tasks successfully.

   NOTE: HP recommends resolving any warnings before continuing with the initializing and configuring HP SIM process. Click **OK** to ignore the warnings and continue.

4. Initialize and configure HP SIM by executing the following command:

   /opt/mx/bin/mxinitconfig -a

   NOTE: The initialization of the upgrade is done in the background, which takes several minutes. To verify if the upgrade is 100% complete, view the file by executing the following command:

   more /var/opt/mx/logs/initconfig.log

NOTE: After upgrading from a previous version of HP SIM, if you notice a pre-existing collection returning an unexpected result, and HP SIM has not been restarted since the upgrade, then stopping and restarting the HP SIM service should resolve this problem.

5. Verify that the `mxdomainmgr`, `mxinventory` and `mxdtf` daemons are running by executing the following command:

   `ps -ef | grep mx`

   If they are not running, start them by executing the following command:

   `/opt/mx/bin/mxstart`

NOTE: The JRE bundled with HP SIM 7.4 is jre1.7.

6. Optional: Configure the system to send SNMP traps.

NOTE: These steps might vary slightly, depending on your version of Linux. Refer to your Linux provider for details if these file paths and file names do not exist on your system.

a. Verify that SNMP is installed by executing the following command:

`rpm -qa | grep snmp`

If SNMP is not installed, the previous command does not return a components list. Refer to your Linux provider for information on installing SNMP.

b. Verify if the hp-snmp-agents from the ProLiant Support Pack for Linux is installed by executing the following command:

`rpm -qa | grep hp-snmp-agents`

If the hp-snmp-agents is not installed, the previous command does not return a components list. If it is installed, verify that the hp-snmp-agents daemon are running by executing the following command:

`/etc/init.d/hp-snmp-agents status`

c. If the hp-snmp-agents daemons are running, stop them using the following command:

`/etc/init.d/hp-snmp-agents stop`

NOTE: If the hp-snmp-agents daemon is not installed, omit this step and step g.

d. Stop the SNMP daemon:

`/etc/init.d/snmpd stop`

e. Edit the `snmpd.conf` file using any text editor.

For Red Hat Linux, run the following command for opening this file in the vi editor:

`vi /etc/snmp/snmpd.conf`

For SUSE Linux Enterprise Server 10 SP3 and SUSE 11, run the following command for opening this file in the vi editor:

`vi /etc/snmp/snmpd.conf`

i. Remove the comment symbol (#) from the trapsink line, and add the IP address of the CMS. This system has HP SIM application running:

`trapsink` ***`IPaddress`***

where *`IPaddress`* is the IP address of the CMS.

NOTE: If snmpd is already installed, type **`man snmpd`** and read the manpage to determine how to configure the trapsink parameter.

NOTE: If the trapsink entry is not available in the snmpd.conf, enter it manually using the following command:

`trapsink CMS IP`

where CMS IP is the location you want to send the traps from the managed nodes.

ii. If the following line exists in the read-only community:

`community` ***`CommunityName IPaddress`***

Change it to:

rocommunity *`CommunityName IPaddress`*

If the line is not present, enter the CMS to the read-only community manually by adding the line:

`rocommunity` ***`CommunityName IPaddress`***

where *CommunityName* is the SNMP community string used by the CMS and *IPaddress* is the IP address of the CMS.

iii. Save the changes to the file. To save and close this file using the vi editor, press the **Esc** key, enter `:wq!`, and press the Enter key.

f. Start the SNMP daemon by executing the following command:

```
/etc/init.d/snmpd start
```

g. Start the hp-snmp-agents daemon if it is installed on your system:

```
/etc/init.d/hp-snmp-agents start
```

Enabling Linux VCRM features

After HP SIM is installed, Linux VCRM is automatically installed during a fresh installation. However, to enable the VCRM support, download and install certain packages as pre-requisites.

NOTE: Before installing the packages, ensure that you install python version 2.5 or above.

Download and install the following packages:

1. Download `jre-7u67-linux-i586.gz` package from http://www.java.com/en/download/manual.jsp, and run the package.
2. Download and extract `xalan-j_2_7_1-bin.zip` file from http://apache.osuosl.org/xalan/xalan-j/, and copy the following jar files to the `/usr/java/jre1.6.0_27/lib/ext` directory:
   - serializer.jar
   - xalan.jar
   - xercesImpl.jar
   - xml-apis.jar
3. Download and extract `rhino1_7R4.zip` file from https://developer.mozilla.org/en/Rhino_downloads_archive, and copy the following jar file to the `/usr/java/jre1.6.0_27/lib/ext` directory:
   - Js.jar
4. Download and extract `bsf-3.0-bin.tar.gz` file from http://archive.apache.org/dist/jakarta/bsf/binaries/, and copy the following jar file to the `/usr/java/jre1.6.0_27/lib/ext/` directory:
   - bsf.jar
5. Download and extract `commons-logging-1.0.3.zip` file from http://archive.apache.org/dist/commons/logging/binaries/, and copy the following jar files to the `/usr/java/jre1.6.0_27/lib/ext` directory:
   - commons-logging-tests.jar
   - commons-logging-api-1.0.3.jar
   - commons-logging-adapters-1.0.3.jar
   - commons-logging-1.0.3.jar
   - commons-logging-1.0.3–sources.jar
   - commons-logging-1.0.3–javadoc.jar

Linux VCRM is a non-interactive RPM. Instead of prompting for a user input, it only prints a message instructing users on how to configure it.

To configure HP Linux VCRM, run the **vcrepositoryconfig.sh** script as a 'root' user. The script is available at the location: **/opt/hp/vcrepository/etc/**. Run the script with —R or —r option to enable the repository feature and set the repository folder.

NOTE: If the CMS is mapped to a Linux VCRM, then you can deploy software and firmware tasks only to a Linux target system and not to a windows target system.

Next steps

Install and configure the required Insight Management Agents on the systems that will be managed by the CMS. Next, complete the initial setup of HP SIM. Initial setup involves adding managed systems, adding users, setting up authorizations, and configuring event handling. For more information, see "Setting up managed systems" (page 35).

Start the HP SIM graphical user interface (GUI) using Firefox or Internet Explorer at http://<IP_Address>:280/.

NOTE: The HP SIM Registration window and First Time Wizard appear when a user with full configuration rights logs in to HP SIM for the first time. Follow the onscreen instructions to register HP SIM or click the **Register Later** button to register at another time. If your HP SIM system is not connected to the internet, you can use another system that has internet access and navigate to http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPSIM-LIC to register and retrieve a code to confirm to the HP SIM application that it is registered and to discontinue the registration prompt. The First Time Wizard configures only the basic settings of an initial setup for HP SIM. Refer to the HP Enterprise Information Library for more information.

3 Setting up managed systems

Perform step 2 to install and configure the required management software.

1. Install and configure the CMS. For more information, see "Installing HP SIM on the CMS for the first time" (page 26).
2. **Install and configure the required Insight Management Agents on the systems that will be managed by the CMS.**
3. Configure HP SIM for your environment. For more information, see "Configuring HP SIM" (page 38).

Setting up managed systems involves installing the required management software. The management software being installed depends on the type of managed system.

- Linux
- Storage systems
- Windows systems - see the HP Enterprise Information Library
- HP-UX - see the HP Enterprise Information Library

Installing the ProLiant or Integrity Support Pack on a Linux system for the first time

For Linux systems, use the Linux Deployment Utility to install the latest support pack with the preconfigured components to the local system. For more information regarding installing a support pack using the Linux Deployment Utility, see http://www.hp.com/servers/psp.

Setting up managed storage systems

Storage Management Initiative Specification (SMI-S) is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices. HP SIM uses this standard to discover and manage the storage systems it supports.

You must have a storage system's WBEM SMI-S provider installed and configured for HP SIM to discover it. This includes storage devices such as Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters).

Refer to the HP SIM SMI-S Provider webpage, http://www.hp.com/go/hpsim/providers, to view the latest information regarding HP SIM support for a particular device. This webpage offers information on obtaining, installing, and configuring SMI-S providers.

Installing SMI-S providers

Each storage vendor provides the SMI-S provider and installation instructions for its storage system. The webpage referenced in the previous section provides information on obtaining SMI-S providers. Also, consult the storage vendor's website or representative for more information regarding their SMI-S providers. For each storage system:

1. Verify that the applicable SMI-S provider is installed.
2. If the SMI-S provider is not installed, obtain and install it per the vendor's installation instructions.

Verifying SSL

HP SIM requires that Secure Sockets Layer (SSL) is enabled for the SMI-S provider in order to discover and manage the storage system that the provider supports. Verify that SSL is enabled for each SMI-S provider.

Configuring SMI-S providers

Occasionally, it might be necessary to modify an SMI-S provider's port number or password. Use the provider documentation to perform these modifications.

For example, if two CIMOMs exist on the same host, you must configure them to use different ports to communicate with the CMS.

Configuring HP SIM to discover storage systems

After verifying that each storage system's SMI-S provider is installed and configured, configure HP SIM to discover the storage systems by performing the following steps:

1. Enter the user name and password for each provider's SMI CIMOM in the Default WBEM settings section on the Setting Global Protocols page.
2. Add each SMI CIMOM IP address to the **System Automatic Discovery** task or to the **Creating a New Discovery** task. For more information, see the HP Enterprise Information Library.

HP SIM discovers the storage systems after the next automatic discovery task. To discover your storage systems immediately, run the discovery task as described in the Running a Discovery Task section of the HP Enterprise Information Library.

RHEL 6.3 installation instructions

For successfully installing RHEL 6.3 or later, the versions/packages mentioned in this section must be followed as pre-requisites:

NOTE: These libraries are necessary for the optimal deployment of the software and firmware upgrade tasks on the system, where HP Version Control Agent is not used on the target systems.

- lm-sensors-libs-3.1.1-10.el6.<arch>.rpm
- net-snmp-libs-5.5-27.el6.<arch>.rpm
- net-snmp-5.5.27.el6.<arch>.rpm
- kernel-headers-2.6.32-71.el6.<arch>.rpm
- redhat-rpm-config-9.0.3-25.el6.noarch.rpm
- kernel-devel-2.6.32-71.el6.<arch>.rpm
- rpm-build-4.8.0-12.el6.<arch>.rpm
- gcc-4.4.4-13.el6.<arch>.rpm
- libuuid-2.17.2-6.el6.i686.rpm
- freetype-2.3.11-5.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libICE-1.0.6-1.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- libXcb-1.5-1.el6.i686.rpm
- libXau-1.0.5-1.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libXrandr-1.3.0-4.el6.i686.rpm
- libXfixes-4.0.4-1.el6.i686.rpm

- libXcursor-1.1.10-2.el6.i686.rpm
- fontconfig-2.8.0-3.el6.i686.rpm
- expat-2.0.1-9.1.el6.i686.rpm
- expect-5.44.1.15-2.el6.<arch>.rpm
- zlib-1.2.3-25.el6.i686.rpm
- libstdc++-4.4.4-13.el6.i686.rpm
- net-snmp-5.5-27.el6.<arch>.rpm

In addition, the build directory for RPMs built from source has changed depending on the name of the user building them. Under RHEL 6.x, the directory is `/root/rpmbuild/RPMS/`, if the user is logged in as root. For users other than root, the directory is `/$USER/home/rpmbuild/RPMS/`.

NOTE: The versions/packages given in this section are needed as a minimum. However, you could use later versions/packages as well.

4 Configuring HP SIM

Perform step 3 to configure HP SIM for your environment.

1. Install and configure the CMS. For more information, see "Installing HP SIM on the CMS for the first time" (page 26).
2. Install and configure the required Insight Management Agents on the systems that will be managed by the CMS. For more information, see "Setting up managed systems" (page 35).
3. **Configure HP SIM for your environment. For more information, see "Configuring HP Systems Insight Manager using the First Time Wizard" (page 38), "Configuring HP SIM using the Options menu" (page 39), or "Setting up Linux managed systems manually" (page 40).**

Configuring HP Systems Insight Manager using the First Time Wizard

The initial setup of HP SIM uses the First Time Wizard to provide step-by-step instructions for performing the initial configuration of HP SIM CMS as well as steps for setting up managed systems, configuring discovery, configuring event handling, adding users, and defining authorizations. To perform the initial setup, you must complete the installation of your CMS as described in "Setting up managed systems" (page 35).

The First Time Wizard is automatically launched the first time a user with administrative privileges signs in to HP SIM. The administrative account used to install HP SIM is the initial administrative account. If the wizard is canceled before completion, it restarts each time an administrative user signs in. You can cancel and disable the wizard from starting automatically by selecting the **Do not automatically show this wizard again** checkbox and clicking **Cancel**. You can start the wizard manually by selecting **Options→First Time Wizard**.

The First Time Wizard helps you configure settings on the CMS. After configuring a setting, click **Next** to continue the First Time Wizard setup procedure. The First Time Wizard does not apply any changes until you click **Finish** on the **Summary** page.

NOTE: The default settings in Firefox block the First Time Wizard. You must disable the pop-up blocker in Firefox to see the First Time Wizard.

The following is an overview of the First Time Wizard configuration screens:

- **Introduction**

  Describes the purpose of the First Time Wizard. You can cancel the First Time Wizard and disable the wizard from automatically starting when an administrative user signs in.

- **Managed Environment**

  Specifies all operating systems managed by the CMS. The selections made here configure HP Systems Insight Manager to show collections, tools, and reports only for managed environments that are selected.

  This page also displays required details for each TDEF selection, such as IP address of the Ignite server, sign in credential information, and so on.

- **Discovery**

  Use the wizard to enable discovery, set up the discovery schedule, and enter the IP address ranges or host names of the systems you want to discover. Discovery is the process HP SIM uses to find and identify systems on your network and populate the database with that information. A system must be discovered to collect data and track system health status.

- **Credentials**

  Use the wizard to set the sign-in credentials and the SNMP and SNMP v3 credentials for the Discovery task.

- **Configure Managed Systems**

  Configure managed systems as they are discovered, by configuring WBEM and WMI, SNMP, SSH access, and trust relationship.

- **WBEM/WMI Mapper Proxy**

  To retrieve managed system information on Windows systems, enter the mapper proxy system host name and port number.

  NOTE: This page only appears if you selected to manage a Windows operating system.

- **Privilege Elevation**

  Enable privilege elevation if, on HP-UX, Linux, and ESX managed systems, you are required to sign in as a non-root user and then request privilege elevation to run root-level tools.

- **E-mail**

  Enter the e-mail settings that the CMS will use to send e-mail notifications. You can set up Automatic Event Handling tasks that prompt HP Systems Insight Manager to send e-mails when the CMS receives a specific event.

- **Summary**

  Displays all First Time Wizard settings with the option to modify settings or to finish the First Time Wizard.

The First Time Wizard configures only the basic settings of HP SIM. When you are finished entering information in the HP SIM First Time Wizard, review your selections on the **Summary Page**, and then click **Finish** to save them. For more information on the First Time Wizard, see the HP SIM help system.

Configuring HP SIM using the Options menu

To configure HP SIM using the Options menu, you must configure the following for the managed systems.

1. Configure the protocol settings.

   Protocol settings define how HP SIM communicates with the managed systems. To configure these settings, Select **Options→Protocol Settings →Global Protocol Settings**.

2. Add users and user groups.

   NOTE: Users that have been added to the (CMS) cannot view or manage systems until authorizations have been configured for them.

   NOTE: HP-UX and Linux-provided command line tools, such as `ls` and `df`, are run as root by default. For security reasons, you might want them to run as a specific user to avoid permitting unintended capabilities to a user.

   To add users, select **Options→Security→Users and Authorizations→Users**, and then click **New**.

   To add user groups, select **Options→Security→Users and Authorizations→Users**, and then click **New Group**.

3. Add toolboxes.

   Toolboxes, define the set of tools to which a user has access. To add toolboxes, select **Options→Security→Users and Authorizations→Toolboxes**, and then click **New**.

4. Add authorizations.

   Authorizations give the user access to view and manage systems. Each authorization specifies a user or user group, a toolbox, and a system or system group. The specific set of tools that can be run against a system is specified in the assigned toolbox.

It is important that you plan which systems each user is going to manage and which specific set of tools the users are authorized to execute against the managed systems. A user with no toolbox authorizations on a system cannot view or manage that system.

Authorizations are additive. If a user is authorized on Toolbox1 on a system and is also authorized for Toolbox2 on the same system, the user is authorized for all tools in both Toolbox1 and Toolbox2 on that system. Similarly, a user authorized for the **All Tools** toolbox needs no other toolbox authorization on that system because the **All Tools** toolbox always includes all tools.

To add authorizations, select **Options→Security→Users and Authorizations→Authorizations**, and then click **New**.

5. Configure email settings

   Email settings enables users to receive email notification of certain events. To configure email settings, select **Options→Events→Automatic Event Handling→Email Settings**.

6. Set up automatic event handling.

   Automatic event handling defines the action that HP SIM performs when an event is received. To setup automatic event handling, select **Options→Events→Automatic Event Handling→New Task**.

7. Configure and execute discovery.

   Discovery is the process that HP SIM uses to find and identify the systems on your network and populate the database with that information. To configure and execute a discovery, you must create a Discovery task. HP SIM includes one default discovery task (system automatic discovery). However, you can create a new discovery task to discover specific systems.

   To configure Discovery, select **Options→Discovery**.

8. Configure the WMI Mapper.

   In order for HP SIM to manage Windows systems, you must install the Pegasus WMI Mapper service on a Windows system. To configure the WMI Mapper, select **Options→Protocol Settings→WMI Mapper Proxy**.

For more information on the Options menu items, see the HP SIM help system.

Setting up Linux managed systems manually

You can use the HP SIM Configure or Repair Agents tool to configure Linux managed systems simultaneously, or you can configure each managed system manually.

To manually configure Linux managed systems, perform the following on each managed system:

Procedure 3

1. Install and configure SSH.
   a. Verify that SSH is installed on the managed system:

      ```
      rpm -qa | grep ssh
      ```

      If it is not installed, see your Linux provider for information on installing SSH.

   b. On the CMS, copy the SSH generated public key from the CMS to the managed system, and place it in the authorized keys file of the execute-as user (root or administrator).

IMPORTANT: On a non-English CMS, ensure that an administrator account (spelled exactly as follows, administrator) exists on the CMS, and that `mxagentconfig` has been run on the CMS for the created administrator account.

- Execute the following command in the CMS command prompt:

  ```
  mxagentconfig -a -n hostname/IP -u username -p password
  ```

2. Optional: Configure the system to send SNMP traps.

NOTE: These steps might vary slightly, depending on your version of Linux. See your Linux provider for details if these file paths and file names do not exist on your system.

a. Verify that SNMP is installed:

```
rpm -qa | grep snmp
```

If it is not installed, see your Linux provider for information on installing SNMP.

b. Stop the hp-snmp-agents daemons on the platform where you are installing HP SIM using the following command:

```
/etc/init.d/hp-snmp-agents stop
```

NOTE: If the hp-snmp-agents daemon is not installed, omit this step and step F.

c. Stop the SNMP daemon:

```
/etc/init.d/snmpd stop
```

d. Edit the `snmpd.conf` file using any text editor.

For Red Hat Linux, run the following command for opening this file in the vi editor:

```
vi /etc/snmp/snmpd.conf
```

For SUSE Linux Enterprise Server 10, run the following command for opening this file in the vi editor:

```
vi /etc/snmp/snmpd.conf
```

i. Remove the comment symbol (#) from the trapsink line, and add the IP address of the CMS:

```
trapsink IPaddress
```

where *IPaddress* is the IP address of the CMS.

ii. Add the CMS to the read only community by adding the line:

```
rocommunity CommunityName IPaddress
```

where *CommunityName* is the SNMP community string used by the CMS and *IPaddress* is the IP address of the CMS.

iii. Save the changes to the file. To save and close this file using the vi editor, press the **esc** key, enter `:wq!`, and press the **Enter** key.

e. Start the SNMP daemon:

```
/etc/init.d/snmpd start
```

f. Start the hp-snmp-agents daemon if it is installed on your system:

```
/etc/init.d/hp-snmp-agents start
```

5 Upgrading from HP SIM

This chapter provides the steps to upgrade HP SIM 7.x and later. Before beginning the HP SIM upgrade, verify that your user name and password to access to the database are valid. When you perform and upgrade, HP SIM checks for a previous installation of HP SIM, stops HP SIM and all related services and daemons, overwrites or copies files to the appropriate locations on the CMS, and then restarts HP SIM and all related services.

Upgrading HP SIM in Linux

You can upgrade HP SIM automatically or manually. An automatic install executes the `.bin` file, verifies the prerequisites and completes the upgrade. A manual install requires that you execute the separate steps to unpack files and then upgrade HP SIM.

NOTE: Systems Insight Manager 7.2.x or later is supported for an upgrade.

Procedure 4 Unpacking files to upgrade HP SIM

1. Extract the `.rpm` files from the `HPSIM-Linux_C.6.x or later .bin` file. Set the permissions to include the right to execute the .bin file by executing the following command:

   `./HPSIM-Linux_C.6.x or later .bin --noexec --target mxserver`

   NOTE: For information on setting permissions, refer to Step 5.

2. To change the directory to mxserver, execute the following command:

   `cd mxserver`

   NOTE: If you are using hpsmd as your database, continue with Step 3 through Step 5. If you are using Oracle as your database, skip to Step 6.

3. Install the hpsmdb database, using the appropriate `.rpm` files in the following order.

   NOTE: The `rpm -i hpsmdb-*.rpm` command installs hpsmdb on your system.

   - SUSE Linux Enterprise Server 11 SP2 or later

     `rpm -ivh hpsmdb-sles11-*.i586.rpm`

   - 64-bit SUSE Linux Enterprise Server 11 SP2 or later

     `rpm -ivh hpsmdb-sles11-*.x86_64.rpm`

   NOTE: If you is using SUSE 9 with older version of HP SIM, then user has to upgrade SUSE 11.

4. Verify that the hpsmdb status reads `running`.

   - For Red Hat Enterprise Linux (all versions):

     NOTE: By default, the **hpsmdb** service is configured to run in INIT 3 and 5 level.

     a. Execute the `serviceconf` command. The Service Configuration window appears.

     NOTE: Use the `ntsysv` command instead of `serviceconf` if you are running from a CLI prompt.

     b. Scroll down to the **hpsmdb** entry.

c. Select the checkbox, save the changes, and then start the service.
d. To start hpsmdb by using the command line, execute the following command:

`/etc/rc.d/init.d/hpsmdb start`

Or

`/etc/init.d/hpsmdb start`

- For SUSE Linux Enterprise Server 11 SP2 or later:
  a. View the status by executing the following command:

  `/etc/init.d/hpsmdb status`

  b. Configure hpsmdb to run during startup by executing the following command:

  `chkconfig hpsmdb 345`

  c. If the status is `unused` in any version of Red Hat Linux or SUSE Linux, start the daemon by executing the following command:

  - For SUSE Linux Enterprise Server 11 SP2 or later:

    `/etc/init.d/hpsmdb start`

  - For Red Hat Enterprise Linux (all versions)

    `/etc/rc.d/init.d/hpsmdb start`

    Or

    `/etc/init.d/hpsmdb start`

  NOTE: To install HP SIM on a system without OpenSSH or with a purchased version of SSH, use the **`--nodeps`** option on rpm.

  For example, **`rpm --nodeps -ivh`** followed by the rpm files.

5. Install HP SIM using the `.rpm` files:

   `rpm -Uvh hpsim*`

   NOTE: The initialization of the upgrade is done in the background, which takes several minutes. To verify if the upgrade is 100% complete, view the file by executing the following command:

   `cat /var/opt/mx/logs/initconfig.log`

   NOTE: If PostgreSQL is used by HP SIM and hpsmdb is installed successfully, the HP SIM upgrade process automatically migrates the HP SIM data from PostgreSQL to hpsmdb. If hpsmdb cannot be installed successfully, the upgraded HP SIM continues to use PostgreSQL.

6. If you have an Oracle database, after upgrading HP Systems Insight Manager do the following:
   a. Stop HP Systems Insight Manager.
   b. Search for a file named `ojdbc6.jar` in the [installdir]/lib and [installdir]/jboss/server/hpsim/lib directories and remove it from any locations where it is found.
   c. Download the new driver from the Oracle website at http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html.
   d. Copy the JDBC driver file (`ojdbc6.jar`) to the [installdir]/lib and [installdir]/jboss/server/hpsim/lib directories.

7. Complete the upgrade by restarting the HP SIM daemons using mxstop and mxstart.

   HP SIM is now installed and initialized on the CMS. To browse to HP SIM, start the HP SIM graphical user interface (GUI) using Firefox, or Internet Explorer at http://<IP_Address>:280/.

8. After upgrading to HP SIM 7.4 and above, sign in to HP SIM, and run the Daily Device Identification task to ensure that all your associations are updated correctly.

   NOTE: Before running the Daily Device Identification task, if there is a WMI Mapper Proxy node configured from the previous release, you must first re-identify the WMI Mapper node and verify that the Properties page for the WMI Mapper is working properly. See "Configuring HP SIM" (page 38) for details.

   To run the daily Identification task:

   a. Select **Tasks & Logs**>**View All Scheduled Tasks**. The **All Scheduled Tasks** page appears.
   b. Select the **Daily Device Identification** task.
   c. Click **Run Now**.

NOTE: Some tools in the Monitor Tools toolbox of previous versions of HP SIM have been removed from HP SIM 5.x. They either provide administrator-type functionality or access to administrator-level files to non-administrator users of HP SIM. If upgrading from a previous version, these tools remain in the Monitor Tools toolbox. You must review the contents of the Monitor Tools toolbox and any other toolboxes you have created, and remove these tools accordingly.

If upgrading from HP SIM 6.x and above, the list of tools include:

Table 11 Available tools

Monitor tools	General tools
type	General Tools
cat	General tools
find	General tools

Procedure 5 Removing tools

1. Sign in to HP SIM as administrative rights user.
2. Select **Options**>**Security**>**Users and Authorizations**, and then click the Toolboxes tab.
3. Select the **Monitor Tools toolbox**.
4. Click **Edit**.
5. In the **Toolbox contents** panel, select the tools you want to remove and click the **<>** button.
6. Click **OK** to save.

NOTE: After upgrading to HP SIM to ensure that all network devices, racks, and enclosures are properly identified, run Identification. Select **Options**→**Identify Systems**. The **Identify Systems** page appears. See the HP Enterprise Information Library for more information.

6 Uninstalling HP SIM

Uninstalling HP SIM from a Linux system

CAUTION: Removing HP SIM permanently deletes the information in the database unless you back it up before removing the software.

Procedure 6 Removing HP SIM

1. Stop the HP SIM daemons:

   `/opt/mx/bin/mxstop`

2. Verify that the daemons are no longer running:

   `ps -ef | grep mx`

   If any of the HP SIM daemons are running, record the `PID` and kill the process:

   `kill -9 pid`

   where pid is the PID of the daemon. For example,

   `kill -9 3456`

3. Remove the HP SIM software:

   NOTE: If a registered plug-in is installed and dependant on HP SIM. If any registered plug-ins with dependencies on HP SIM are installed, uninstall them first.

   `rpm -qa | grep hpsim | xargs rpm -e`

4. Stop hpsmdb:

   - For Red Hat:

     `/etc/rc.d/init.d/hpsmdb stop`

   - For SUSE:

     `/etc/init.d/hpsmdb stop`

5. Now remove the hpsmdb database:

   `rpm -qa | grep hpsmdb | xargs rpm -e`

   If any packages with dependencies on hpsmdb are installed, uninstall them first. Alternatively, you can run rpm with the following options:

   `rpm -qa | grep postgresql | xargs rpm -e --nodeps`

   Run the following command to remove the HP SIM and PostgreSQL directories:

   `rm -rf /var/opt/mx /etc/opt/mx /opt/mx /var/opt/hpsmdb/opt/hpsmdb`

6. Restart the system.

7 Configuration options

Several configurable parameters in HP SIM that are not available from the GUI. These parameters can only be configured by editing a configuration file on the CMS.

NOTE: All HP SIM parameters have been set to predefined values that are appropriate for most situations. These parameters should only be changed if you are experiencing issues with the default values.

There are two main default locations where configuration files are stored.

- `/etc/opt/mx/config`
- `/opt/hpwebadmin/lib`

These files follow the format of a Java properties file. Therefore, the keys in these files are case-sensitive. In addition, the backslash (\) must be represented by a double-backslash (\\). For more information about the Java property file format, refer to http://www.oracle.com/technetwork/java/index.html.

This chapter provides information on the following configuration options:

- "CPU utilization during data collection" (page 46)
- "GUI time-out policy" (page 46)
- "Systems Insight Manager audit log configuration" (page 47)
- "Configuring task results" (page 48)

CPU utilization during data collection

Overview

The data collection task runs many threads in parallel to overlap computing and database operations with the wait for managed systems to respond. On slower systems, this might temporarily saturate the CPU, depending on the processor speed of the CMS system and the number of systems being collected. Therefore, Systems Insight Manager provides some strategies to lessen the CPU usage.

Implementation

To lessen the CPU usage during data collection on the CMS:

- Limit the number of systems that are being collected at one time. For example, create separate data collection tasks for different groups of systems and schedule them to run at different times.
- Configure the CMS to use a remote database on a system other than the CMS. A substantial portion of the CPU load is consumed by the database during data collection. This option supports Windows, Linux, and HP-UX CMS.
- Lower the `DataCollectionThreadCount` parameter in the `globalsettings.props` file. This parameter defaults to 3. Lowering it to 2 or 1 reduces the CPU demand of data collection tasks, but it increases the time required to complete the tasks.

GUI time-out policy

Overview

Systems Insight Manager provides two alternative time-out policies. The first time-out policy is for environments in which Systems Insight Manager is used to monitor system status, which is called the monitor time-out policy. The second time-out policy is more strict and will time-out inactive users. This is called the active time-out policy and it is similar to the policy, used by Servicecontrol Manager.

Monitor time-out policy

The monitor time-out policy keeps sessions alive, provided the user has a web browser window open displaying the Systems Insight Manager GUI. Closing the browser or navigating to another web page starts the timer for the time-out period. The default time-out period is 20 minutes. Users must use some other means to protect an unattended session from illegal use, such as password-protected screen savers.

Active time-out policy

The active time-out policy only keeps sessions alive if the user is actively using the GUI, such as clicking on links and buttons. Display and refresh of the banner is not sufficient to keep the session alive. The user is timed-out either by inactivity, closing the browser, or navigating to another site. The default time-out period is 20 minutes.

Implementation

- To configure the time-out policy, edit the `globalsettings.props` file. You can switch between these modes or change the time-out period. The default time-out policy is the monitor policy. The monitor policy is enabled when:

  `EnableSessionKeepAlive=true`

  To enable the active time-out policy, change this value to **`false`**.

  `EnableSessionKeepAlive=false`

- To change the default time-out period, edit the `web.xml` file. The default location for this file is:

  `/opt/mx/jboss/server/hpsim/deploy/jboss-web.deployer/conf/web.xml`

  Locate the `session-timeout` element, and set it to a new value in minutes.

  `<session-timeout>20</session-timeout>`

Systems Insight Manager audit log configuration

Overview

Several features of the Systems Insight Manager Audit Log are configurable. For example, you can specify which tools log data and the maximum Audit Log file size. The Systems Insight Manager Audit Log is configured through the `log.properties` file, and tool logging is enabled or disabled through the XML tool definition files.

Tool behaviors

The XML tool definition file provides an option to disable logging of single-system aware (SSA) and multiple-system aware (MSA) command tools. The log attribute for the command element specifies whether the results of the command are output to the Systems Insight Manager log file. Command output is logged by default.

Audit log parameters

In the `log.properties` file, you can configure the following Audit Log parameters:

- File name
- File extension
- Maximum file size in megabytes
- File extension of the roll-over name
- Amount of memory allocated for queuing items to be written to the Audit Log

Audit log location

The location of the Audit Log can be configured using the `path.properties` file.

Implementation

Changes made to the `log.properties` file do not take effect until the log manager daemon or service is restarted. Restart the Systems Insight Manager service.

CAUTION: The queue size should be changed only with extreme care. If the queue is set too high, the log manager consumes too much system memory.

NOTE: When the Audit Log file reaches the maximum file size, the log is renamed with `MX_LOGROLLFILEEXT` extension and a new file is started. If a previous version of the file has already been renamed with the `MX_LOG_ROLLFILEEXT` extension, it will be an automatic roll-over of an audit log file. A roll-over will not occur until a task running is completed. However, after one hour of exceeding the maximum file size, if the task is not finished, then the audit log file will roll over to another file.

Procedure 7 Configuring the Systems Insight Manager Audit Log file location

1. Create a file named `path.properties` under `C:\Program Files\HP\Systems Insight Manager\config`.

   Create a file named `path.properties` under `/etc/opt/mx/config`.
2. Add the following entry in the path.properties file: **`LOG=/var/opt/mx/logs`** .

   NOTE: *`/var/opt/mx/logs`* is listed here as an example. This path is user-defined.
3. Restart the Systems Insight Manager service and Restart the Systems Insight Manager daemons (`mxstop` and `mxstart`). After restarting the services, a new log file named `mx.log` resides in the directory specified in `path.properties` file.

Configuring task results

Systems Insight Manager enables you to set how long entries remain on the **Task Results Page** after a task completes.

Short and long task lifetimes

Some task results are kept for a short time, while other task results are kept for a longer time. Tasks fall into one or the other category based on the type of tool associated with them. Tasks for the following tools have a short lifetime:

- Web-launch tools
- Tools that run from the `mxexec` command line using the `-O` or `-o` options to save the command output
- Tools that run X-Window commands
- Tools that specify in their tool definition the “job-log” flag as disabled, including:
  - Hardware Status Polling
  - Data Collection
  - Identify Systems
  - Software Status Polling
  - Delete Events
  - System Protocol Settings
  - Automatic Discovery

Tools in this category have no task output, have task output that is saved outside of Systems Insight Manager, or have task results that are unlikely to be of long-term interest. Tasks for all other tools are considered long-term.

Frequently scheduled tasks

Task results can also be removed from the **Task Results Page** if a certain number of task results for a scheduled task accumulate. This setting defaults to 10 instances of a single task. If more than 10 accumulate on the results page, then the oldest task result for this scheduled task is removed.

Last result tasks

A task result is kept indefinitely if it is the last result for a scheduled task. For example, if a scheduled task is disabled, its final task result is kept indefinitely or until the task is enabled and more task results accumulate.

To configure task results using the Systems Insight Manager interface, select **Options→Task Results Settings**. For more information, see the Systems Insight Manager help page.

To configure the short and long task lifetimes manually, edit the `globalsettings.props` file.

- The long lifetime defaults to 30 days. To change that time, edit:

  `MX_JOB_MAX_COMPLETED_JOB_AGE=30`

- Task results for frequently scheduled tasks start to drop off after 10 instances. To change this value, edit:

  `MX_JOB_MAX_COMPLETED_JOBS_PER_TASK=10`

  NOTE: The limit of 10 task results applies to scheduled tasks with the "job-log" flag enabled in the tool definition. Scheduled tasks for the tools with the "job-log" flag disabled have a limit of 1. This value is not configurable.

- By default, the last task results for a scheduled task is kept indefinitely.

  Procedure 8 Keeping more than one job

  1. Stop Systems Insight Manager.
  2. Edit `globalsettings.props` and add:

     `MX_JOB_MIN_COMPLETED_JOBS_PER_TASK=`*`n`*

     Where *n*, is the number of task result you want to retain.
  3. Start the Systems Insight Manager service to reflect the changes.

8 Troubleshooting

Q & A 8.1 “Browser issues”
Q & A 8.2 “GUI issues”
Q & A 8.3 “Installation issues”
Q & A 8.4 “Sign in issues”
Q & A 8.5 “GUI issues”

8.1 Browser issues

8.8.1.1 **Accessing some of the menu items on a Linux CMS causes the page to go blank.**

Solution: If using Firefox and this happens, click back on the displayed page, and the menus will be refreshed.

8.2 GUI issues

8.8.2.1 **Parts of the GUI do not show up on my Linux system, such as the devices in the system list, or the System and Events Lists area on the left.**

Solution: Remove everything and re-install. You might have a previous version of PostgreSQL or HP SIM on your system that you failed to remove before installing the new version.

8.8.2.2 **When browsing into a Linux or HP-UX CMS on which the Insight Management Advisor are installed, a Security Alert dialog box appears when I click an Insight Management Agents.**

Solution: The Management HTTP server certificate has not been overwritten with the HP SIM certificate because OpenSSL is not configured correctly. On Linux, OpenSSL should be installed in the `/usr/bin/` directory. On HP-UX, OpenSSL should be installed in the `/opt/openssl/bin/` directory. Install OpenSSL to the correct directory, and then create a new HP SIM certificate to resolve this issue.

8.3 Installation issues

8.8.3.1 **During the installation, the system reboots, and then the installation launches the browser. Internet Explorer displays a message saying that it could not establish a connection with the local host. The browser is being launched before the service has had time to start.**

Solution: Try to access the URL again by placing the cursor in the URL field and pressing the **Enter** key. Keep trying until the application loads in the browser.

Execute the command `ps -ef | grep mx` to check if the service is up and running. The services **mxdtf**, **mxdomainmgr**, and **mxinventory** should be running to confirm that HP SIM is running.

8.8.3.2 **The system was rebooted during `mxinitconfig -a`.**

Solution: Execute the command `mxinitconfig -r` to unconfigure HP SIM and then execute the command `mxinitconfig -a` to configure it again.

8.8.3.3 **The following error message is displayed during installation:**

error: %pre(hpsim-6.x.00.00-1.i386) scriptlet failed, exit status 255

error: install: %pre scriptlet failed (2), skipping hpsim-6.x.00.00-1

Solution: You are attempting to manually install on an unsupported IPF system. Installing an HP SIM CMS on Linux IPF is not supported.

8.8.3.4 **The following error message is displayed on an automatic install during the database configuration step of checking requisites:**

ERROR - PostgreSQL script returns an error, see the following log for detail: /var/opt/mx/logs/PgSQL_Config.log

When you examine the contents of PgSQL_Config.log, the following lines are displayed:

Starting PostgreSQLpg_ctl: postmaster does not start...failed

No PostgreSQL RPM

Solution: Manually start the PostgreSQL service by performing the following steps:

Procedure 9 Manually starting the PostgreSQL service

1. Navigate to the /etc/init.d directory and execute the following command:

   `./postgresql stop`
2. Log in as user **`postgres`** (su postgres).
3. Execute the following command:

   `postmaster -D /usr/local/pgsql/data`

   The postmaster and PostgreSQL start.
4. Run **`mxinitconfig -a`**. Initial configuration completes successfully and service starts.

8.8.3.5 HP SIM and PostgreSQL functionality breaks when I attempt to install HP SIM on Red Hat Enterprise Linux operating system that has PostgreSQL installed externally.

PostgreSQL and HP SIM functionality breaks when I install HP SIM on Red Hat Enterprise Linux (RHEL) operating system where external PostgreSQL database is already installed. After installing HP SIM 7.1, where I have installed PostgreSQL as an external package on RHEL, the PostgreSQL binaries does not work as expected. I get the following error when I execute the psql command.`psql: symbol lookup error: psql: undefined symbol: PQconnectionNeedsPassword`

To resolve this issue, it is recommended to not use external PostgreSQL along with HP SIM. HP SIM supports only the database bundled with its installation package. The bundled PostgreSQL database is installed during HP SIM installation. If PostgreSQL is already installed before HP SIM is installed on the CMS, then you must first uninstall the existing PostgreSQL before proceeding with the installation steps.

8.8.3.6 HP SIM returns a warning message when I attempt to install Linux HP VCRM along with HP SIM on a Linux operating system.

When Linux HP VCRM is either freshly installed via HP SIM or is upgraded from an older un-configured HP VCRM, I encounter the following warning message:

`The setup is incomplete!`

To resolve this issue, you can configure Linux HP VCRM from the HP VCRM user interface available from the HP System Management Homepage application.

8.4 Sign in issues

8.8.4.1 I cannot sign in to HP SIM or to managed systems browsing from HP SIM using Internet Explorer 8.0, Internet Explorer 8.0 SP2 or later.

Reason 1: Internet Explorer has a problem with underscores in system names, which prevents the authentication cookie from working properly.

Solution: If the names of the systems have an underscore, use the IP address of the system. Configure HP SIM to create links to the system using the IP address instead of the name:

Procedure 10 Creating links to systems using the IP address

1. Browse and sign in to HP SIM.
2. Select **Options→Security→System Link Configuration**. The System Link Configuration page appears
3. Select **Use the system IP address**.

4. Click **OK**.

NOTE: By using IP addresses instead of names, you might encounter security alerts, if the name in the managed system certificate does not match the name in the link. The default certificate for managed systems uses the system name, not the IP address.

Reason 2: For managed systems, the privacy policy setting in Internet Explorer 6.0 is blocking the authentication cookies from the managed systems.

Solution 2A: (Recommended) Remove the systems from the Internet Zone. The privacy policy only affects systems in the browser **Internet Zone**. Therefore, by removing systems from that zone, you prevent the privacy policy from affecting those systems. To change the browser privacy policy setting, select **Tools→Internet Options**, and click the **Privacy** tab from the Internet Explorer browser menu. Modify the privacy setting in **one** of the following ways:

- Browsing to systems by IP address instead of by name can cause the browser to consider those systems to be in the **Internet Zone**. Instead, browse by name. You can configure HP SIM to use system names when creating links to systems by selecting **Options→Security→System Link Configuration** and selecting **Use the system name**.
- If your browser is configured to use a proxy server, you can configure your browser to bypass the proxy server for specific systems, which removes those systems from the browser **Internet Zone**. From the browser menu, select **Tools→Internet Options**, and click the **Connections** tab. Click **LAN Settings**, and if you are configured to use a proxy server, click **Advanced**. In the **Exceptions** list, you can specify a list of addresses that should bypass the proxy server. These addresses are no longer in the **Internet Zone** and are not affected by the privacy settings policy.

Solution 2B: (Not Recommended) Change the browser privacy security policy setting. From the Internet Explorer browser menu, select **Tools→Internet Options**, and click the **Privacy** tab. The privacy setting can be modified in one of the following ways:

- Set the privacy setting to **Accept all Cookies** by sliding the slider bar to the bottom. This setting allows a browser to accept all cookies for both first-party and third-party sites. When browsing to HP SIM or directly to a managed system, it is considered a first-party site. When navigating to a managed system through HP SIM, the system is considered a third-party site.
- Customize the handling of cookies by clicking **Advanced** and enabling **Override automatic cookie handling**. Then select the appropriate radio buttons for first-party and third-party cookies to **Accept** or **Prompt**. If you select **Prompt**, the browser prompts you on how to handle a cookie each time a cookie is received. You can choose to block or allow the cookie each time, or for all times. Enabling **Always allow session cookies** does not resolve the problem because the Web Agents do not use session cookies.
- Individually specify the handling of cookies for each system. Click **Edit** in the **websites** section and add the address of the system in the specified field. Click **Allow** to always allow cookies to that system. Repeat this for all systems.

8.5 GUI issues

8.8.5.1 I cannot import any HP SIM certificates. I have installed HP System Management Homepage and HP SIM on the same Linux Server

Solution: To run HP SIM and HP SMH on the same server, you must install or upgrade HP SMH after installing HP SIM. If you are experiencing issues, reinstall or upgrade HP SMH after completing your installing HP SIM.

9 Support and other resources

Information to collect before contacting HP

Be sure to have the following information available before you contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware and software
- Technical support registration number – SAID (Service Agreement Identifier)

How to contact HP

Use the following methods to contact HP technical support:

- In the United States, see the Customer Service / Contact HP United States website for contact options:

  http://welcome.hp.com/country/us/en/contact_us.html

- In the United States, call 1-800-HP-INVENT (1-800-474-6836) to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.
- In other locations, see the Contact HP Worldwide website for contact options:

  http://welcome.hp.com/country/us/en/wwcontact.html

Security bulletin and alert policy for non-HP owned software components

Open source software (such as OpenSSL) or third-party software (such as Java) are sometimes included in HP products. HP discloses that the non-HP owned software components listed in the Insight Management end user license agreement (EULA) are included with Insight Management. The EULA is included with the Insight Management Installer on Insight Management DVD #1.

HP addresses security bulletins for the software components listed in the EULA with the same level of support afforded HP products. HP is committed to reducing security defects and helping you mitigate the risks associated with security defects when they do occur.

When a security defect is found, HP has a well defined process that culminates with the publication of a security bulletin. The security bulletin provides you with a high level description of the problem and explains how to mitigate the security defect.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

Registering for software technical support and update service

HP SIM is supported in any one of the following situations:

- A valid warranty exists (90 days Global Limited Warranty)
- Purchase of Insight Control (having 1-year 24x7 Technical Support bundled with the license purchase)
- The customer purchases a HP SIM Care Pack (Part #: UR389E)

Support includes 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 in electronic form as they are made available from HP.

With this service, customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

www.hp.com/services/insight

Registration for this service takes place following online redemption of the license certificate.

How to use your software technical support and update service

As HP releases updates to software, the latest versions of the software and documentation are made available to you. The Software Updates and Licensing portal gives you access to software, documentation, and license updates for products on your HP software support agreement.

You can access this portal from the HP Support Center:

http://www.hp.com/go/hpsc

After creating your profile and linking your support agreements to your profile, see the Software Updates and Licensing portal at http://www.hp.com/go/hpsoftwareupdatesupport to obtain software, documentation, and license updates.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator website:
  http://www.hp.com/service_locator
- In other locations, see the Contact HP worldwide website:
  http://www.hp.com/go/assistance

Related information

Documents

- HP Insight Control documentation:
  http://www.hp.com/go/insightcontrol/docs
- Systems Insight Manager documentation:
  http://www.hp.com/go/insightmanagement/sim/docs
- HP Matrix Operating Environment documentation:
  http://www.hp.com/go/matrixoe/docs

Websites

- HP Insight Control:
  http://www.hp.com/go/insightcontrol
- Systems Insight Manager:
  http://www.hp.com/go/hpsim

Typographic conventions

This document uses the following typographical conventions:

Table 12 Typographic conventions

Book title	The title of a book. On the web, this can be a hyperlink to the book itself.
`Command`	A command name or command phrase, for example `ls -a`.
`Computer output`	Information displayed by the computer.
Ctrl+x or **Ctrl-x**	A key sequence that indicates you must hold down the keyboard key labeled **Ctrl** while you press the letter `x`.
`ENVIRONMENT VARIABLE`	The name of an environment variable, for example, `PATH`.
Key	The name of a keyboard key. **Return** and **Enter** both refer to the same key.
Term	A term or phrase that is defined in the body text of the document, not in a glossary.
`User input`	Indicates commands and text that you type exactly as shown.
`Replaceable`	The name of a placeholder that you replace with an actual value.
[ ]	In command syntax statements, these characters enclose optional content.
{ }	In command syntax statements, these characters enclose required content.
|	The character that separates items in a linear list of choices.
...	Indicates that the preceding element can be repeated one or more times.
WARNING	An alert that calls attention to important information that, if not understood or followed, results in personal injury.
CAUTION	An alert that calls attention to important information that, if not understood or followed, results in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

10 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback **docsfeedback@hp.com**. Include the document title and part number, version number, or the URL when submitting your feedback.

Glossary

administrative rights user A user who is authorized for the **All Tools** toolbox on all systems, including the Central Management Server. This type of user has been given special privileges to administer the HP Systems Insight Manager software.

administrator A user who manages users, resource pools, and self-service requests through infrastructure orchestration console.

agent A program that regularly gathers information or performs some other service without the user's immediate presence. HP Systems Insight Manager agents provide in-depth hardware and software information and subsystem status to HP Systems Insight Manager and numerous third-party management applications.
See also management agent.

alarm A user-configurable notification displayed in the **System Status** panel of HP Systems Insight Manager when certain events occur. For instance, if a monitored item changes, an alarm notifies the user that a change has occurred.
See also trap, event.

all events collection Displays all events that have occurred for all systems.

All Tools toolbox A default toolbox that provides complete access to all tools for the authorized system or system group.

architect A user who creates a multisystem infrastructure template using HP Matrix Operating Environment infrastructure orchestration (a graphical designer) and then publishes the template for other users to create infrastructure services

attribute A single characteristic of a manageable product or component, as in an attribute of a Management Information Format (MIF) file. A set of related attributes constitutes a group. For example, the clock speed of a processor chip is an attribute of a group that describes that chip.
See also Management Information Format.

authentication The process of identifying an individual, based on a user name and password. Authentication is distinct from authorizations and ensures that the individual is who they claim to be.

authorizations A mapping of a relationship between a user, a toolbox, and a system or system group.

automatic discovery The process that HP Systems Insight Manager uses to find and identify systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status. The primary source for automatic discovery is ping sweeps configured in the automatic discovery tasks page. Other sources might include receiving events from unknown systems or from a management processor that has information about a server. Identification automatically runs on discovered systems.

available software A listing of the software components available in the repository to which the Version Control Agent (HP VCA) has been configured to point. When browsing directly into a HP VCA, these additional components can be selected for installation.

banner The section of the GUI at the top of the screen that includes the user name and links to the **Home** page and sign out functions.

caution A note to indicate that failure to follow directions could result in damage to equipment or loss of information.

Central Management Server A system in the management domain that executes the HP Systems Insight Manager software. All central operations within HP Systems Insight Manager are initiated from this system.

central processing unit polling rate The rate for how often the Cluster Monitor CPU Resource checks CPU utilization as reported by Insight Management Agents on monitored systems.

certificate An electronic document that contains a subject's public key and identifying information about the subject. The certificate is signed by a certificate authority (CA) to bind the key and subject identification together.
See also certificate authority.

certificate authority A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual they claim to be.

certificate key A value used alone or with an encryption decoder (corresponding public or private key) for cryptography. In traditional private key cryptography, the communicators share a key or cipher so that each can encrypt and decrypt messages. The risk in this system is that if any party loses the key, the system is broken. In public key cryptography, the private key is associated with a public key, so each person in the system has a personal private key that is never shared.

cleared status A status condition that indicates an event is cleared.

clearing events Changing the event status from uncleared to cleared.

clients HP desktop, portable, and workstation systems.

cluster A parallel or distributed computing system made up of many discrete systems that form a single, unified computing resource. Clusters vary in their features, complexity, and the purposes for which they are best suited.

cluster IP address The IP address of the cluster.

cluster monitor A core component of HP Systems Insight Manager. Cluster Monitor adds the ability to monitor and manage multi-node clusters. Cluster Monitor also manages multiple cluster platforms in a heterogeneous environment.

cluster monitor resource A program that provides a monitoring or management function for clustered nodes in a cluster.

cluster system identification Information about cluster systems. This information is stored in the database.

collections The method for grouping system or event.

command line interface A text-based application that can be executed from a command shell such as sh, csh, ksh or the Microsoft Windows CMD shell.

common information model An object-oriented schema defined by the Desktop Management Task Force (DMTF). CIM is an information model guide that describes and shares management information enterprise-wide. CIM is designed for extending each management environment in which it is used.

common information model object manager A CIMOM acts as the interface for communication between web-based enterprise management (WBEM) providers and management applications such as HP Systems Insight Manager. A CIMOM that provides an interface for an SMI-S provider is called an SMI CIMOM.

communications protocol *See* management protocol.

complex Computer systems that support multiple hardware partitions are referred to as a complex. For example, the HP Integrity Superdome systems support multiple hardware partitions within a single complex.

component A component is a single, self-describing, installable (interactive or silent) binary file containing a single piece of software, such as firmware image, driver, agent, or utility, that is supported by the management and update tools.

configuration history report The Survey Utility that contains reports that show configuration details for server and compares configuration history files for differences.

Configure or Repair Agents An HP Systems Insight Manager feature that enables you to repair credentials for SNMP settings and trust relationships that exist between HP Systems Insight Manager and target systems. You can also update Web Agent passwords on target systems that have 7.2 agents or earlier installed.

control tasks Sequences of instructions that are associated with a search, event, or both, such as Delete Events, Remove Disk Thresholds, Set Disk Threshold, and Set Device Access community strings.

critical status A state generated when HP Systems Insight Manager can no longer communicate with a managed system.

custom tools

Custom tools are tools that can be created by the user to run on the Central Management Server or on target systems. For example:

- **Remote tool**

  A tool that runs on selected target systems. It might copy files to the target systems or run specific X-Window applications on the target systems. You can schedule this tool.

- **CMS tool**

  A tool that runs on the CMS. It is usually a script or batch file and can pass in environment variables. Using Automatic Event Handling, you can configure this tool to run when events are received. You can schedule this tool.

- **Web page tool**

  A tool that launches a web URL. The URL is launched in a separate browser window on the CMS. You cannot schedule this tool.

data collection reports

Data collection reports include information about discovered systems in a single instance or a historical trend analysis report. HP Systems Insight Manager supports **Overwrite existing data set (for detailed analysis)**, formerly known as Single Instance Data Collection task in Insight Manager 7, and **Append new data set (for historical trend analysis)**. With **Overwrite existing data set (for detailed analysis)**, data is collected from a system at a single instance. With **Append new data set (for historical trend analysis)**, data detailing the system history is collected.

data collection tasks

Procedure that involves gathering information from a group of managed systems and storing that information in the database. HP Systems Insight Manager uses Hardware Status Polling and Data Collection Tasks to implement data collection.

Desktop Management Interface

An industry-standard protocol, primarily used in client management, established by the Desktop Management Task Force (DMTF). DMI provides an efficient means of reporting client system problems. DMI-compliant computers can send status information to a central management system over a network.

Desktop Management Task Force

An industry standard body that defines WBEM standards for the industry. HP is an active sponsor and participant in the DMTF body.

digital signatures

A technology used to validate the sender of a transaction. This technology uses private keys to digitally sign the data and public keys to verify the sender.

discovery

A feature within a management application that finds and identifies network objects. In HP management applications, discovery finds and identifies all the HP systems within a specified network range.

discovery filters

Enables users with to prevent or allow certain system types from ever being added to the database.

discovery template

Files that can be used by automatic discovery in lieu of typing the addresses directly in to the **Ping inclusion ranges** or **Exclusion ranges** fields on the **Automatic Discovery - General Settings** page and are designed to be used as a quick way to change the scope of automatic discovery.

Distributed Component Object Model

An extension of the Component Object Model (COM) that enables COM components to communicate between clients and servers on the same network.

Distributed Task Facility

A management application that manages the remote execution of tasks on managed systems.

Domain Name Service

A service that translates domain names into IP addresses.

e-mail notification

One of the notification tasks in HP Systems Insight Manager that sends notifications through e-mail.

edit collection

To modify existing collections to add or remove search criteria.

enclosure

A physical container for a set of server blades. 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.

event

Information sent to certain users that something in the managed environment has changed. Events are generated from SNMP traps. HP Systems Insight Manager receives a trap when an important event occurs. Events are defined as:

- **Warning.**

  Events of this type indicate a state that might become a problem.

- **Informational.**

  Events of this type require no attention and are provided as useful information.

- **Normal.**

  Events of this type indicate that this event is not a problem.

- **Minor.**

  Events of this type indicate a warning condition that can escalate into a more serious problem.

- **Major.**

  Events of this type indicate an impending failure.

- **Critical.**

  Events of this type indicate a failure and signal immediate attention.

event overview

A chart that summarizes the events by product type.

external sites

Third-party application URLs.

graphical user interface

A program interface that takes advantage of the graphics capabilities of the computer to make the program easier to use. The HP Systems Insight Manager GUI runs in a web browser.

health status

Health status is an aggregate status all of the status sources (which can be SNMP/SNMP v3, WBEM, and HTTP) with the most critical status being displayed.
See also system health status.

hosts files

A file that follows the UNIX, Linux, or Windows host file format, which is an IP address followed by a name and each system is listed on a separate line in this file. This file is used by discovery to manually add multiple systems to the HP Systems Insight Manager database,

HP CloudSystem Integrated Manager

HP CloudSystem Integrated Manager is an HP Systems Insight Manager plugin that enables you to manage blade systems from HP Systems Insight Manager for Windows, HP-UX and Linux. HP CloudSystem Integrated Manager is composed of blade computer systems, integrated connectivity to data and storage networks, and shared power subsystems. The HP CloudSystem 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. Users are able to conveniently configure, deploy, and manage individual or groups of blade systems.

HP Insight Control

System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables.

HP Systems Insight Manager combines the strengths of Insight Management 7.3, HP Toptools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Windows, Linux, and HP-UX. The core HP Systems Insight Manager software delivers the essential capabilities required to manage all HP server platforms. HP Systems Insight Manager can also be extended to deliver unparalleled breadth of system management with plug-ins for HP storage, power, client, and printer products. Plug-ins for rapid deployment, performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets.

HP Insight Control database

The database that stores vital information about HP Systems Insight Manager, including users, systems, and toolboxes.

HP Insight Control performance management

A software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers. HP Insight Control performance management tools consist of Online Analysis, Offline Analysis, Comma Separated Value (CSV) File Generator Report, System Summary Report, Status Analysis Report, Configuration, Licensing, and Manual Log Purge.

HP Insight Control power management	An integrated power monitoring and management application that provides centralized control of server power consumption and thermal output at the datacenter level. It extends the capacity of datacenters by enabling the user to control the amount of power and cooling required for ProLiant servers. Built on ProLiant Power Regulator Technology, it extends new server energy instrumentation levers into HP Systems Insight Manager for greater Unified Infrastructure Management.
HP Insight Control server deployment	The HP Insight Control server deployment is a multiserver deployment tool that enables IT administrators to easily deploy large numbers of servers in an unattended, automated fashion. The Insight Control server deployment is installed separately from HP SIM. It requires a license for each server managed. You must register your Insight Control server deployment product to purchase licenses or obtain a 10-node 30-day license before installing Insight Control server deployment (a 10-node 7-day evaluation license is built into the software). The Insight Control server deployment is installed from its own DVD. See http://www.hp.com/servers/rdp for information about Insight Control server deployment including a link to obtain evaluation licenses or register your product. See the Insight Control server deployment documentation for network environment setup, prerequisites for the deployment server, and installation instructions.
HP Insight Control server provisioning	HP Insight Control includes the rights for HP Insight Control server provisioning, which is a new feature replacing HP Insight Control server deployment. HP Insight Control server provisioning performs multi-server operating system provisioning to bare metal ProLiant and BladeSystem servers. You can download the HP Insight Control server provisioning installation instructions from http://www.hp.com/go/insightupdates. HP Insight Control server deployment is still available on the DVD, and can be used for upgrade purposes. However, Insight Control server deployment software license will no longer be included with the sale of Insight Control. Insight Control customers wanting a new Insight Control server deployment license will be required to purchase a standalone Insight Control server deployment license.
HP Insight Control virtual machine management	Provides central management and control of Virtual Machines on Microsoft Virtual server, Vmware's GSX and ESX. Integrated with HP Systems Insight Manager, virt provides unified management of HP ProLiant host servers and virtual machines.
HP Insight Management Agents	A program that regularly gathers information or performs some other service without the user's immediate presence.
HP VCA log	A listing of all the software maintenance tasks completed by the Version Control Agent and reports resulting from those tasks.
HP Version Control Agent	An agent that is installed on a server to enable you to see the HP software installed on that server. The HP VCA can be configured to point to Version Control Repository Manager, enabling easy version comparison and software update from the repository.
HP Version Control Repository Manager	An HP agent that enables a customer to manage HP provided software stored in a user-defined repository.
HyperText Transfer Protocol	The underlying protocol used by the World Wide Web.
identification	While discovery finds systems, identification attempts to determine what the system type is. In addition, it determines what management protocol a system supports, using credentials from the **Global Protocol Settings** page, and attempts to determine the operating system and version loaded, along with other basic attributes about the system. Finally, it determines if the system is associated with another system. For example, a management processor in a server.
infrastructure service	A running configuration of infrastructure resources that is designed to run a business application such as a multi-tier web application. It is also referred to as a service or service instance.
Insight Vulnerability and Patch Manager software	The all-in-one vulnerability assessment and patch management tool integrated into HP Systems Insight Manager, simplifying and consolidating the proactive identification and resolution of issues that can impact server availability into one central console.
installed version	A particular HP software component that is installed on the server.

Internet Protocol	Specifies the format of datagrams (packets) and the addressing scheme on a network. Most networks combine IP with Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
IP range	Systems with an IP address that falls in the specified range.
Java database connectivity	Similar to Open DataBase Connectivity (ODBC), this set of Application Program Interfaces (APIs) provides a standard mechanism to allow Java applets access to a database.
Java Remote Method Invocation	A set of protocols that enable Java objects to communicate remotely with other Java objects.
keystore	A database that maintains a list of keys. The keystore can contain a subject's own private key. A keystore can also contain a list of public keys, as published in certificates.
Major status	Status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken immediately.
managed systems	Any system managed by HP Systems Insight Manager, such as servers, desktops, storage systems, and Remote Insight Boards (RIBs).
management agent	A daemon or process running on a managed system. It receives and executes requests from the Central Management Server on the managed system.
management domain	A collection of resources called managed systems that have been placed under the control of HP Systems Insight Manager. Each Central Management Server is responsible for a management domain. The managed systems can belong to more than one management domain.
Management HTTP Server	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software. This version is available in the ProLiant Support Pack 7.10 or earlier.
Management Information Base	The data specification for passing information using the SNMP protocol. An MIB is also a database of managed objects accessed by network management protocols.
management instrumentation	Agents running on systems that provide management information for HTTP, or SNMP protocols.
management LAN	A LAN dedicated to the communications necessary for managing systems. It is typically a moderate bandwidth (10/100 BaseT) and secured through limited access.
management protocol	A set of protocols, such as WBEM, HTTP, or SNMP, used to establish communication with discovered systems.
management scope	A set of systems within the set of all discovered systems that HP Systems Insight Manager manages.
management services	A core set of capabilities such as automatic discovery, data collection, a central repository for system and event information, event management, basic notification, and secure access. These functions are used by add-ins from HP, a Management Solutions Partner, and HP Systems Insight Manager users.
management tasks	Procedures you set up to search systems or events.
manual discovery techniques	Processes that enable you to bypass a full discovery for the following tasks: • Adding a single system • Editing the system • Creating or importing an HP Systems Insight Manager database hosts file • Creating or importing generic hosts files
Microsoft Clustering Service status page	A page that summarizes cluster status as defined by Microsoft Cluster Server and lists the status and values of MSCS-defined cluster attributes. The Cluster Monitor uses color to display status based on MSCS condition values (Normal, Degraded, Failed, and Other).
Minor status	Status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken as soon as possible to prevent further failure.
Monitor Tools toolbox	A default toolbox that contains tools that display the state of managed systems but not tools that change the state of managed systems.

multiple-system aware	A run type that supports multi-system operations. Tools with this run type operate on the target systems using their own internal mechanisms instead of using the Distributed Task Facility. The MSA run type uses the Distributed Task Facility to launch the tool on a single system before the tool interacting with the other managed systems.
network clients	Any computer system connected to your network with a compatible browser used to connect to the HP Systems Insight Manager GUI.
Onboard Administrator	The Onboard Administrator is the central point for controlling an entire c-Class enclosure. It offers configuration, power, and administrative control over the rack, and its associated blades (Compute Servers), blade management processors (iLOs), network switches (depending on the models of switches used) and storage components (such as SAN or SATA). The Onboard Administrator is a single management processor, with shared resources to an optional backup twin processor for failover.
Open Service Event Manager	Enables you to collect, filter, and send problem reports for supported systems (ProLiant and Integrity) running Insight Management Agents. In addition, OSEM automatically sends service event notifications to HP Systems Insight Manager when a problem is detected on the system.
OpenSSH	A set of network connectivity tools providing encrypted communication sessions over a computer network using SSH. It was created as an open source alternative to the proprietary SSH software suite offered by SSH Communications Security.
operator rights user	A user who has limited capability to configure the Central Management Server. operator rights users have permission to create, modify, and delete all reports and their own tools.
overall software status	This section indicates whether the software on the server that the Version Control Agent is installed on has any updates available within the repository in which it has been configured to monitor.
ProLiant and Integrity Support Packs	An ProLiant and Integrity Support Packs is a set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. An ProLiant and Integrity Support Packs contains driver components, agent components, and application and utility components. All of these are verified to install together.
ProLiant Essentials license key	The contractual permissions granted by HP to the customer in the form of a coded embodiment of a license that represents a specific instance of a license. A single license can be represented by a single key or by a collection of keys.
provisioning	The process of creating a service from a template. Through the Insight Orchestration Self-Service Portal or the Insight Orchestration console, a user submits a request to create the service and Insight Orchestration controller searches its inventory allocating the computing resources to all logical resource definitions in the template.
rack	A set of components cabled together to communicate between themselves. A rack is a container for an enclosure.
Red Hat Package Manager	The Red Hat Package Manager is a powerful package manager that can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files and package information, including name, version, and description.
Reference Support Pack	A baseline bundle of HP software components that the Version Control Agent can be configured to point to in the repository. This setting enables users to indicate that they want to keep all of their software up to a certain Support Pack level.
remote wakeup	Sometimes referred to as Wake-On-LAN (WOL). The remote powering up of a system through its resident WOL network card, provided that the system has been enabled to be so awakened using the ROM or F10 Setup. This is a capability on which HP Systems Insight Manager relies to turn on the systems for scheduled Software Updates or Replicate Agent Settings.
remove all disk thresholds	A task provided by HP Systems Insight Manager to remove disk thresholds for systems in an associated collection. This task only removes disk thresholds that were set by HP Systems Insight Manager or by browsing directly to the Web Agent. Any thresholds set by HP Systems Insight Manager for Windows 32, including disk thresholds, are not removed by this task.
Replicate Agent Settings	A tool that can be used to copy web-based agent settings to a group of systems.

repository A directory containing ProLiant and Integrity Support Packs, Integrity Support Packs and Smart Components or Support Pack for ProLiant.

Resource Partition A subset of the resources owned by an operating system instance. The use of those resources is controlled through technologies such as the Fair Share Scheduler, pSets, and Memory Resource Groups.

A resource partition also has a set of processes associated with it, and only those processes can use the resources within the resource partition. Policies established by tools such as Process Resource Manager (PRM), Workload Manager (WLM), or Global Workload Manager (gWLM) control how resources are allocated to the set of resource partitions within an operating system instance.

resource pool A group of physical and virtual resources managed by HP Virtual Server Environment. An administrator controls resource utilization by allowing users access to resource pools.

role *See* toolbox.

rule set Conditions, policies, or criteria applied to system information to determine what it is.

SAN A storage area network (SAN) is a network (or subnetwork) that connects data storage devices with associated data servers. A storage area network is typically part of an overall network of computing resources.

search criteria A set of variables (information) used to define a requested subset of information from the HP Systems Insight Manager database.

Secure HTTP An extension to the HTTP protocol that supports sending data securely over the web.

Secure Shell A program to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

Secure Sockets Layer A standard protocol layer that lies between HTTP and TCP and provides privacy and message integrity between a client and server. A common usage of SSL is to provide authentication of the server, so clients can be assured they are communicating with the server it claims to be. It is application protocol independent.

secure task execution A feature of HP Systems Insight Manager that securely executes a task from a managed system. STE ensures that the user requesting the task has the appropriate rights to perform the task, and encrypts the request to protect data from snooping.

security roles A feature that enables administrators to restrict system access and manage access on a per-user or per-group basis. This capability enables systems administrators to delegate tasks to junior staff without providing access to advanced or dangerous features. It also enables systems administrators to delegate management of systems to specific organizations or customers without providing access to systems owned by other organizations or customers.

self-signed certificate A certificate that is its own Certificate Authority (CA), such that the subject and the CA are the same.
See also certificate, certificate authority.

server blade Typically a very dense server system 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.
See also enclosure.

server blade visual locator A feature designed to provide visual representation of ProLiant BL e-Class, p-Class and c-Class servers within their respective enclosures and racks.
See also enclosure.

Service Advertising Protocol A NetWare protocol used to identify the services and addresses of servers attached to the network.

set disk thresholds A task provided by HP Systems Insight Manager to set a disk threshold for systems in an associated collection. This threshold is set on all disk volumes on the target systems.

Shared Resource Domain A collection of compartments—all of the same type—that share system resources. The compartments can be nPartitions, virtual partitions, processor sets (pSets), or Fair Share Scheduler (FSS) groups.

	A server containing nPartitions can be an SRD—as long as nPartition requirements are met. A server or an nPartition divided into virtual partitions can be an SRD for its virtual partition compartments. Similarly, a server, an nPartition, or a virtual partition containing pSets can be an SRD for its pset compartments. Lastly, a Server, an nPartition, or a virtual partition containing FSS groups can be an SRD for its FSS group compartments. A complex with nPartitions can hold multiple SRDs. For example, if the complex is divided into nPartitions, named Par1 and Par2, Par1's compartments could be virtual partitions, while Par2's compartments are pSets. Each compartment holds a workload. gWLM manages the workload by adjusting the compartment's resource allocation.
Short Message Service	A convenient way to send brief text messages directly to a wireless phone. There is a maximum message length of 140 characters.
Simple Network Management Protocol	One management protocol supported by HP Systems Insight Manager. Traditional management protocol used extensively by networking systems and most servers. Management Information Base for Network Management of TCP/IP-based internets (MIB-II) is the standard information available consistently across all vendors.
Simple Object Access Protocol	A lightweight protocol for exchange of information in a decentralized, distributed environment.
Single Sign On	Permission granted to an authenticated user browsing to HP Systems Insight Manager to browse to any of the managed systems from within HP Systems Insight Manager without re-authenticating to the managed system. HP Systems Insight Manager is the initial point of authentication, and browsing to another managed system must be from within HP Systems Insight Manager.
single-system aware	A run type that does not support multi-system operations. Tools with this run type are only aware of the system on which they are running.
SMI CIMOM	*See* common information model object manager.
SMI-S provider	An industry-standard WBEM provider that implements a well defined interface for storage management. The manufacturers of host bus adapters (HBAs), switches, tape libraries, and storage arrays can integrate SMI-S providers with their systems, or provide them as separate software packages. *See also* Web Based Enterprise Management.
SNMP communication setting	Default SNMP community string used when communicating with systems supporting SNMP communications.
SNMP trap	Asynchronous event generated by an SNMP agent that the system uses to communicate a fault.
Software Distributor	The HP-UX administration tool set used to deliver and maintain HP-UX operating systems and layered software applications.
software inventory	A listing of the HP software installed on the system where the Version Control Agent is installed.
software update	A task to remotely update software and firmware.
spoofing	The act of a website posing as another site to gather confidential or sensitive information, alter data transactions, or present false or misleading data.
standard error	The default place where the system writes error messages. The default is the terminal display.
standard output	The default place to which a program writes its output. The default is the terminal display.
status message list	A list created by Cluster Management Resources to collect entries found in the bottom left area of the **Cluster Monitor** page to bring your attention to cluster attributes that are in an abnormal state.
status message summary header	The list header summary of the total number of status messages in the list and, in parentheses, the number of status messages that have not been examined.
status type	The classification of status messages (for example, Critical, Major, Minor, Normal, Warning, and Unknown).

Storage Management Initiative Specification

A standard management interface developed by the Storage Networking Industry Association (SNIA). SMI-S provides a common interface and facilitates the management of storage devices from multiple vendors. SMI-S uses industry-standard common information model and Web Based Enterprise Management technology.

storage systems

SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters).

subnet

On TCP/IP networks, subnets are all systems whose IP addresses have the same prefix. For example, all systems with IP addresses that start with 10.10.10. would be part of the same subnet.

Survey Utility

An agent (or online service tool) that gathers and delivers hardware and operating system configuration information. This information is gathered while the server is online.

symmetric key

A common key that both the server and receiver of a message share and use to encrypt and decrypt a message.

system

Systems on the network that communicate through TCP/IP. To manage a system, some type of management protocol (for example, SNMP, or WBEM) must be present on the system. Examples of systems include servers, workstations, desktops, portables, routers, switches, hubs, and gateways.

system group

A group of systems based on a system collection; a static snapshot of the source collection at the time the system group was created. Used for authorizations.

system health status

This is aggregate status all of the status sources (which can be SNMP, WBEM, and HTTP) that are supported on a target system, with the most critical status being displayed. The following are the different system health statuses that can be displayed:

- **Critical**

  HP Systems Insight Manager can no longer communicate with the system. The system was previously discovered but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems.

- **Major**

  A major problem exists with this system. It should be addressed immediately. For systems running an Insight Management Agents, some component has failed. The system might no longer be properly functioning, and data loss can occur.

- **Minor**

  A minor problem exists with this system. For systems running Insight Management Agents, some component has failed but the system is still functioning.

- **Warning**

  The system has a potential problem or is in a state that might become a problem.

- **Normal**

  The system is functioning correctly.

- **Disabled**

  The system is disabled from monitoring but is not necessarily turned off.

- **Unknown**

  HP Systems Insight Manager cannot obtain management information about the system.

- **Informational**

  The system might be in a transitional or non-error state.

system identification

Identifying information about systems. This information is stored in the database. The following information is identified:

- Type of management protocol on the system (SNMP/SNMP v3, WBEM, HTTP, and SSH)
- Type of HP system (server, client, switch, router, and so on)
- Network name of system

system information Information that is provided on the **System Page** under the **System** tab. The system information includes:

- Network address
- Network name
- Description
- Contact
- Location
- System links

system information using SNMP Agents that conform to SNMP MIB-2 standards.

system links A summary information page for a specific system that has a management agent.

System Management Homepage An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software.

system overview report A report indicating the state of systems that is available at the time that HP Systems Insight Manager is first opened. A system search result contains the number of systems that are registered with the HP Systems Insight Manager databases. Systems are grouped by their status conditions. Each number in a column is a hyperlink to a more detailed list of systems, which displays the systems that correspond to the number in the overview.

system properties properties can be set for a single system or for multiple systems at the same time and include options such as system name, system type, system sub-type, operating system version, asset number, contact information, and whether or not the system properties can be changed or updated by the discovery process.

system search Logical grouping of systems into a collection based on information in the HP Systems Insight Manager database. After a search is defined, you can display the results from the system view page or associate it with a management task.

system search results The result of a system search.

system status panel The section of the GUI on the left of the screen that displays status information and system or event alarms.

system type One of 12 supplied types. You can add your own based on one of these types. For example, use Server type to create MyServer type. It is still a server and is reported on in the same way, but it has your designation.

System Type Manager A utility that enables users to set certain attributes for those systems that are discovered as Unknown by SIM. Using this utility, user can configure SNMP rules based on system object identifier and set system type, subtype and user defined model based on the response from SNMP. HP Systems Insight Manager discovers and identifies the system and applies the new information when an Unknown system matches a rule set that you specify as the primary rule set. Furthermore, creating the new system type provides a **System Link** page for viewing the information returned from the system agent or from the communication protocol of SNMP.

task An executed instance of an HP Systems Insight Manager tool, on one or more systems, with a specific set of arguments.

task scheduling A master scheduling tool for the scheduling of polling, control, and notification tasks.

template A tool that specifies the requirements for an infrastructure service in terms of server groups, networks, storage, and contain customization points that use HP Operations Orchestration workflows during the execution of request.

template files Template files are a concept that was used before HP Systems Insight Manager had multiple automatic discovery tasks. Template files should no longer be used. However, a template file enables you to create the same data range (IP ranges, and so on) that would be entered in a discover IP inclusion range. The automatic discovery task can have as input one or more template files. However, template files cannot be nested.

threshold A preset limit that produces an event when the limit is reached or exceeded.

Tomcat An open source implementation of Java Servlet and JavaServer Pages technologies that is used by HP Systems Insight Manager as a web server.

tool An application, command, or script that can be executed by HP Systems Insight Manager on one or more systems to perform a task.

toolbox A defined set of tools that a user might need for a particular task, such as database administration or software management. Each HP Systems Insight Manager toolbox is associated with a set of tools and authorizations.

trap An unsolicited message generated by a management agent that indicates that an event has occurred. For example, a monitored item has exceeded a set threshold or changed status. Previously called alarm.
See also event.

trap categories Event collection systems found by event type. SNMP/SNMP v3 traps categorized by HP Systems Insight Manager into logical groups according to their functions.

trap forwarding address The IP address of a system that has been specified to receive trap notifications forwarded by the HP Systems Insight Manager systems.

type The classification of a system, which identifies it as a standard system type. The system types are client, cluster, portable, printer, remote access device, repeater, router, server, switch, unknown, workstation, and other.

uncleared event status Events that have a Critical, Major, Minor, Normal, or Informational severity and have not been cleared or deleted from the database. Events can be cleared without being deleted from the database by using the **Clear events** menu option.

- **Critical.**
  A failure has occurred, and immediate attention is required.
- **Major.**
  A failure is impending.
- **Minor.**
  A warning condition exists that can escalate into a more serious problem.
- **Normal.**
  These events are not a problem.
- **Informational.**
  No attention required. This status is provided as useful information

unknown status HP Systems Insight Manager cannot obtain management information about the system using SNMP/SNMP v3. Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting.

user A network user with a valid login on the Central Management Server that has been added to HP Systems Insight Manager.

user accounts Accounts used to sign-in to HP Systems Insight Manager. These accounts associate a local Windows user account or a domain account with privilege levels and paging attributes inside HP Systems Insight Manager.

user group A group of users defined on the Central Management Server operating system that has been added to HP Systems Insight Manager. Members of the user group in the operating system can sign-in to HP Systems Insight Manager.

user rights user A user who cannot configure the Central Management Server. However, the user can view and run predefined reports on the Central Management Server and all managed systems.

version control Referred to as the Version Control Repository Manager installed on a Windows system for Windows and Linux ProLiant systems, and Software Distributor on HP-UX operating systems. Provides an overview of the software status for all managed ProLiant or Integrity systems and can update system software and firmware on those systems programmatically using predetermined criteria. Version control identifies systems that are running out-of-date system software, indicates if an upgrade is available, and provides reasons for upgrading. For HP-UX systems, Software

	Distributor can be launched from an HP Systems Insight Manager Central Management Server against one or more installed HP-UX systems.
Virtual Server Environment	An integrated server virtualization offering for HP-UX, Linux, and Windows servers that provides a flexible computing environment maximizing usage of server resources. VSE consists of a pool of dynamically sizeable virtual servers; each can grow and shrink based on service level objectives and business priorities. For more information, see http://h71028.www7.hp.com/enterprise/cache/258348-0-0-101-121.html.
WBEM Services	HP WBEM Services for HP-UX is an HP product that uses WBEM and DMTF standards to manage HP-UX system resources.
Web Based Enterprise Management	This industry initiative provides management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to software and hardware data that is readable by WBEM client applications.
Web-Based Enterprise Services	A tool suite that is aimed at preventing or reducing the downtime of a system.
Web-launch aware	A run type for tools that are launched in a web browser using a web server. WLA tools can be designed to deal with multiple systems.
Windows Management Instrumentation	An API in the Windows operating system that enables you to manage and control systems in a network.
workspace	The section of the GUI where tools appear.
X client	An application or tool that appears on an X server. X clients can also be called X applications.
X server	A local application that accepts X client requests and acts on them.
X Window System	A cross-platform windows system that uses the client/server model to distribute services across a network. It enables applications or tools to run on a remote computer.
XML document	A collection of data represented in XML.

Index

A

active time-out, 46
audit log
  configure, 47

C

Central Management Server
  Linux system preparation, 26
central management server
  installing HP SIM on Linux, 27
  requirements, 5
configuration
  audit log, 47
  data collection CPU utilization, 46
  lifetimes for Task Result entries, 48
  managed system, 35
  time-out policy, 46
configuration options, 46
configuring
  first time wizard, 38
  HP Systems Insight Manager, 38
  managed systems, 38
CPU utilization, 46
customization options, 46

D

data collection
  performance, 46
database
  remote for improved performance, 46
default time-out period, 46

F

first setup *see* initial setup
First Time Wizard, 38
frequently scheduled task lifetimes, 48

G

getting started, 35

I

initial setup, 35
  managed systems, 35
install
  central management server requirements, 5
  managed system requirements, 8
  process overview, 5
installing HP SIM
  Linux CMS, 27

L

last result task lifetimes, 48
lifetimes for Task Result entries, 48
Linux CMS
  installation and configuration, 27
  removing HP SIM, 45
  system preparation, 26

M

managed environment
  first time wizard, 38
managed node *see* managed system
managed system
  requirements, 8
  setup, 35
monitor time-out, 46

N

node *see* managed system

P

parameter
  DataCollectionThreadCount, 46
  EnableSessionKeepAlive, 46
  LOG, 47
  MX_JOB_MAX_COMPLETED_JOB_AGE, 48
  MX_JOB_MAX_COMPLETED_JOBS_PER_TASK, 48
  MX_JOB_MIN_COMPLETED_JOBS_PER_TASK, 48
  MX_LOG_FILEEXT, 47
  MX_LOG_FILENAME, 47
  MX_LOG_FILESIZE, 47
  MX_LOG_QUEUESIZE, 47
  MX_LOG_ROLLFILEEXT, 47
  session-timeout, 46

R

removing HP SIM
  Linux CMS, 45
requirements
  central management server, 5
  managed system, 8

S

setup
  initial, 35
  managed systems, 35
short and long task lifetimes, 48
Storage Management Initiative Specification
  storage, 35

T

Task Results Page
  entry lifetime configuration, 48
time-out policy
  configuration, 46
troubleshooting, 50
typographic conventions, 55

U

Uninstall Central Management Server
  removing HP SIM on Linux, 45

upgrading HP SIM
overview, 42
process, 42