Managing ProLiant servers with Linux

HOWTO

Abstract

This HOWTO provides instructions to help system administrators install, upgrade, and remove Version 8.1.0 (or later) of the following HP Linux management software:

- HP System Health Application and Command Line Utilities (hp-health)
- Insight Management SNMP Agents for HP ProLiant Systems (hp-snmp-agents)
- HP OpenIPMI Device Driver (hp-OpenIPMI)
- HP ProLiant Channel Interface Device Driver for iLO/iLO 2 (hp-ilo)
- The HP System Management Homepage (hpsmh)
- HP System Management Homepage Templates for Linux (hp-smh-templates)

This HOWTO also provides reference links to installation instructions for HP Systems Insight Manager and HP ProLiant Essentials Rapid Deployment Pack.

The HP ProLiant Support Pack (PSP) is a set of bundled software components for maintaining and deploying software on HP ProLiant servers and is available for download from http://h18004.www1.hp.com/products/servers/management/psp/index.html. For installing the complete set of Linux software drivers and management agents, see the appropriate PSP for Linux.

1 Software architecture

This section describes the features and architecture of the following systems:

- HP System Health Application and Command Line Utilities (hp-health)
- Insight Management SNMP Agents for HP ProLiant Systems (hp-snmp-agents)
- HP System Management Homepage (hpsmh)
- Descriptions for HP management consoles for Linux

1-1 System Health Application and Command Line Utilities (hp-health)

The System Health Application and Command Line Utilities (hp-health) package collects and monitors important operational data on ProLiant servers. Contained within the hp-health package are the following components:

- Health Monitor
- HP Integrated Management Logging (IML) utility (hplog)
- HP Unique Identifier utility (hpuid)
- HP ProLiant Boot Configuration Utility (hpbootcfg)
- HP Management Command Line Interface (hpasmcli)

ProLiant servers are equipped with hardware sensors and firmware to monitor certain abnormal conditions, such as temperature readings, fan failures, error correction coding (ECC) memory errors, and so on. The Health Monitor monitors these conditions and reports them to the administrator by printing messages on the console (preserved in /var/log/messages). The Health Monitor also logs the conditions to the ProLiant Integrated Management Log (IML). The IML is dedicated, Non-Volatile RAM (NVRAM) that can be viewed and maintained by the hplog application or iLO web interface.

ProLiant servers contain an Integrated Lights-Out (iLO) controller that, with optional software, allows secure remote management of the server including IML management and graphical remote console.

The System Health Application and Command Line Utilities (hp-health) package works with the HP ProLiant Channel Interface Device Driver for iLO/iLO 2 (hp-ilo) package to provide secure remote management of the server including IML management and graphical remote console.

hp-health Version 8.1.0 includes three applications (listed in Table 1). One of these modules is automatically selected at startup depending on the HP ProLiant Advanced System Management hardware available.

Note:
To determine the type of HP ProLiant Advanced System Management hardware installed, check the ProLiant server specifications located on www.hp.com.

Table 1: hp-health Version 8.1.0 applications

Application		Details
hpasmd		
	Location	/opt/hp/hp-health/bin/hpasmd
	Description	The hpasmd application automatically loads on ProLiant servers that have either the ASM or the legacy iLO hardware.
hpasmxld*		
	Location	/opt/hp/hp-health/bin/hpasmxld
	Description	The hpasmxld application automatically loads on ProLiant servers that have the HP Integrated Lights-Out 2 (iLO 2) management controller and the hp-OpenIPMI package is installed. The iLO 2 management controller contains an Intelligent Platform Management Interface (IPMI) Version 2.0 Base Management Controller (BMC) that replaces the operating system-based software management functionality provided by the legacy hpasmd application. The hpasmxld application is also dependent on the hp-OpenIPMI package. The hp-OpenIPMI package is a GNU GENERAL PUBLIC LICENSE (GPL) high performance enhancement of the IPMI device drivers that ship with standard Linux distributions. The hpasmxld package is automatically selected by the hpasm initialization script (/etc/init.d/hp-health) if the hp-OpenIPMI package is installed and the iLO 2 management controller is present. The corresponding hp-OpenIPMI package for ProLiant servers is available for download for select distributions at: http://h20000.www2.hp.com/bizsupport/TechSupport/Product.jsp?lang=en&cc=us&taskId=135&prodTypeId=15351&prodCatId=241435.
hpasmlited*		
	Location	/opt/hp/hp-health/bin/hpasmlited
	Description	The hpasmlited application automatically loads on HP ProLiant servers with the iLO 2 management controller and the hp-OpenIPMI package **not** installed. The hpasmlited application is designed to work with the standard IPMI device drivers that ship with the Linux distributions. The IPMI device drivers that ship with the Linux distributions are not as efficient as the hp-OpenIPMI drivers due to the constant polling method used for detecting system management events. The hpasmlited application has the ability to log raw IPMI messages (as does the hp-OpenIPMI package) to the /var/log/messages file to assist with debugging IPMI BMC integration issues.

* The hpasmxld application is more efficient than the hpasmlited application as a result of leveraging the high performance hp-OpenIPMI package, which includes support for IPMI 2.0 OEM message channels and messages.

Another source of information includes the following man pages provided with the hp-health package:

- hp-health
- hpasmcli
- hpuid
- hplog
- hpbootcfg

These man pages include detailed information on error messages and possible action that the administrator can take.

Additional information about the Insight Management SNMP Agents for HP ProLiant Systems is available at the following locations:

- www.hp.com/servers/manage
- http://h18000.www1.hp.com/products/servers/management/agents.html

1-1-1 Health Monitor

The Health Monitor augments the hardware features built into ProLiant servers. Basic features, such as temperature, fan, power supply, and memory monitoring are standard on almost all ProLiant servers. On some ProLiant servers, the Health Monitor supports features such as variable speed fans, server lights that give a visual indication of a possible error condition, and Advanced Memory Protection (AMP). The AMP feature allows the capability of reserving memory for fail over if a Single Bit Correctable Error (SBCE) threshold is exceeded.

Note:
On some ProLiant servers, the entire memory subsystem can be mirrored to survive an uncorrectable memory error. Without AMP, uncorrectable memory errors are always fatal and cause a kernel panic. AMP allows a server to continue execution until the faulty memory can be replaced. Mirrored AMP solutions usually allow removing the memory board with the faulty memory dual in-line memory module (DIMM) and replacing the faulty DIMM while the server continues execution. When the repaired AMP memory board is inserted back into the server, the AMP mirror automatically restores. This allows mission critical 7 X 24 applications to continue execution without interruption or downtime.

The following sections explain the features provided by the Health Monitor for the overall health of the ProLiant server.

1-1-1-1 System temperature monitoring

A ProLiant server can contain several temperature sensors. On ProLiant servers with intelligent temperature sensors, check the current and threshold temperatures by running hplog -t.

If the normal operating range is exceeded for any of these sensors, the Health Monitor does the following:

- Displays a message on the console stating the problem
- Makes an entry in the system health log and the operating system log

Additionally, on some servers, the fans gradually increase to full speed in an attempt to cool the server as the external environment temperature increases. If the server exceeds the normal operating range and does not cool down within 60 seconds, the operating system is, in most cases, shut down to close the file systems.

Tip:
On servers that do not have variable speed fans, the server is shut down unless the ROM-Based Setup Utility (RBSU) Thermal Shutdown feature is disabled. This feature is enabled by default. Use RBSU to control the shutdown option.

1-1-1-2 System fan monitoring

A ProLiant server can contain fan sensors. On ProLiant servers with intelligent fan sensors, check the status of the fans by running hplog -f.

If a cooling fan fails and there is no secondary redundant fan, the Health Monitor does the following:

- Displays a message on the console stating the problem
- Makes an entry in the system health log and the operating system log
- Shuts down the system (optionally) to avoid hardware damage

Use RBSU to control the shutdown option.

If a secondary or redundant fan is present when a fan fails, the Health Monitor does the following:

- Activates the redundant fan if not already running
- Displays a message on the console stating the problem
- Makes an entry in the system health log and the operating system log

1-1-1-3 Monitoring the system fault tolerant power supply

If the server contains a redundant power supply, the power load is shared equally between the power supplies. Check the status of the power supplies by running hplog -p. If a primary power supply fails, the server automatically switches over to a backup power supply. The Health Monitor does the following:

- Monitors the system for power failure and for physical presence of power supplies
- Reports when the power supplies experience a change in shared power load
- Displays a message on the console stating the problem
- Makes an entry in the system health log and the operating system log

1-1-1-4 ECC memory monitoring and advanced memory protection

If a correctable ECC memory error occurs, the Health Monitor logs the error in the health log, including the memory address causing the error. If too many errors occur at the same memory location, the driver disables the ECC error interrupts to prevent flooding the console with warnings (the hardware automatically corrects the ECC error).

On servers with AMP, the driver attempts to log an error if a memory board has been inserted, removed, or incorrectly configured, and optionally if an Online Spare Switchover or Mirrored Memory engaged event occurs.

The Health Monitor does the following:

- Displays a message on the console stating the problem
- Makes an entry in the system health log

This server feature is configured using RBSU. On ProLiant servers that do not support AMP mirroring, an uncorrectable (double bit) memory error causes the operating system to halt abruptly. Logging of the error might not be possible if the error occurs in memory used by the Health Monitor.

1-1-1-5 Automatic server recovery

Automatic Server Recovery (ASR) is configured using RBSU available during the initial boot of the server by pressing the **F9** key when prompted. This feature is implemented using a "heartbeat" timer that continually counts down. The Health Monitor frequently reloads the counter to prevent it from counting down to zero. If the ASR counts down to zero, it is assumed that the operating system has locked up and the system automatically attempts to reboot.

Events that can contribute to the operating system locking up include:

- A peripheral device, such as a Peripheral Component Interconnect Specification (PCI) adapter, generates numerous spurious interrupts when it fails.
- A high priority software application consumes all the available central processing unit (CPU) cycles and does not allow the operating system scheduler to run the ASR timer reset process.
- A software or kernel application consumes all available memory, including the virtual memory space (for example, swap). This can cause the operating system scheduler to cease functioning.
- A critical operating system component, such as a file system, fails and causes the operating system scheduler to cease functioning.
- Any event other than an ASR timeout causes a Non-Maskable Interrupt (NMI) to be generated.

The ASR feature is a hardware-based timer. If a true hardware failure occurs, the Health Monitor might not be called, but the server resets as if the power switch was pressed. The ProLiant ROM code might log an event to the IML when the server reboots.

The Health Monitor is notified of an ASR timeout through an NMI. If possible, the driver attempts to perform the following actions:

- Displays a message on the console stating the problem
- Makes an entry in the IML
- Attempts to gracefully shut down the operating system to close the file systems

There is no guarantee that the operating system will gracefully shutdown. This shutdown depends on the type of error condition (software or hardware) and its severity. The Health Monitor logs a series of messages when an ASR event occurs. The presence or absence of these messages can provide some insight into the reason for the ASR event. The order of the messages is important, since the ASR event is always a symptom of another error condition.

1-1-2 Console messages

When events occur outside of normal operations, the Health Monitor might display a console message or log a message to the IML. Operational messages, such as fan failures or temperature violations, are logged to the standard /var/log/messages file. Messages specific to device drivers (such as NMI type messages) can be viewed using dmesg, if the system is not completely locked up.

The hp-health man page documents how to interpret the messages produced by the Health Monitor.

1-1-3 HP Integrated Management Logging Utility (hplog)

The HP ProLiant Integrated Management Logging utility (hplog) allows system administrators to view IML pages. Commands are listed in Table 2.

Table 2: hplog options

Command	Description
hplog –t	Shows the current temperature and the threshold levels of all temperature sensors
hplog –f	Shows the status of all fans
hplog –p	Shows the status of all power supplies
hplog –t	Shows the current temperature and the threshold levels of all temperature sensors

1-1-4 HP Unique Identifier Utility (hpuid)

The HP Unique Identifier Utility (hpuid) allows local manipulation of the ProLiant Unique Identifier (UID) blue light on selected ProLiant servers. The hpuid utility allows the light to be turned on and off and displays the current status of the light (Table 3).

Table 3. hpuid options

Command	Description
hpuid –d	Disables the UID (blue) light
hpuid –e	Enables the UID (blue) light
hpuid –s	Shows the status of the UID (blue) light

1-2 Insight Management SNMP Agents for HP ProLiant (hp-snmp-agents)

The ProLiant Insight Management Agents provide proactive notification of server events through the HP Systems Insight Manager console. Alternatively, the ProLiant Insight Management Agents allow the status of the server to be monitored or checked using a standard Web browser. Insight Management Agents include the following:

- Server Agents (consist of Server Peer Agent, Host OS Agent, Threshold Agent, Standard Equipment Agent, and System Health Agent)
- Storage Agent (consists of IDA, IDE, SCSI, SAS, and FCA Agents, and Event Agent)
- Network Agent

1-2-1 Server Agent

A Server Agent consists of the sub-agent components listed in Table 4.

Table 4. Sub-agents of the Server Agent

Sub-agent	Description
Server Peer Agent	The Peer Agent extends the SNMP "enterprise" Management Information Base (MIB) to include HP specific data, specifically enterprise ID 232. The Peer Agent supports SNMP get, set, and trap operations on MIB branches under "enterprises.232." At SNMP agent startup, cmaX reads MIB information files referenced in the master file /opt/hp/hp-snmp-agents/mibs/cmaobjects.conf. These referenced MIB information files are /opt/hp/hp-snmp-agents/mibs/cmasvrobjects.conf and /opt/hp/hp-snmp-agents/mibs/cmafdtnobjects.conf. During installation, the Peer Agents are configured to start automatically when the SNMP agent is running and should be started after the SNMP agent snmpd is started and should be killed after snmpd is killed.
Host OS Agent	The Host OS Agent gathers data for the Host OS MIB, including: • Server/host name and operating system version number. • Linux file system information (for each mounted file system). • Software version information. The Host OS Agent executable is /opt/hp/hp-snmp-agents/server/bin/cmahostd.
Threshold Agent	The Threshold Agent implements the Threshold MIB. Users can set thresholds on counter- or gauge-type MIB variables. The Threshold Agent periodically samples each selected MIB variable at a rate defined by the user. MIB data values are compared to user-configured thresholds. If a configured threshold is exceeded, an alarm trap is sent to the configured SNMP trap destination and to Linux email (configurable through trapemail entries in /opt/hp/hp-snmp-agents/cma.conf file). User-configured alarm thresholds are permanently saved in the data registry until deleted by the user. The Threshold Agent executable is /opt/hp/hp-snmp-agents/server/bin/cmathreshd.

Sub-agent	Description
Standard Equipment Agent (cmastdeqd)	The Standard Equipment Agent gathers data for the Standard Equipment MIB. The data includes: • PCI slot information. • Processor and coprocessor information. • Standard peripheral information (serial ports, diskette drives, and so on). The Standard Equipment Agent executable is /opt/hp/hp-snmp-agents/server/bin/cmastdeqd.
System Health Agent (cmahealthd)	The System Health Agent gathers data for the Health MIB. The data collected includes critical (NMI) errors, correctable memory (ECC) errors, system hang/panic detection, temperature conditions, and fan failures. The System Health Agent then retrieves these errors from the Health Monitor. The System Health Agent executable is /opt/hp/hp-snmp-agents/server/bin/cmahealthd.

For more information on threshold configurations, see the HP Systems Insight Manager Help file. This guide can be found on the Management CD or on the HP website at www.hp.com/go/hpsim.

1-2-2 Storage Agent

The Storage agent consists of IDA, IDE, SCSI, SAS and FCA Sub-agents, and Event Agent components. The Storage agent collects information from the Fibre Channel, drive array, SCSI, SAS, and IDE subsystems at periodic intervals, makes the collected data available to the SNMP agent, and provides SNMP alerts.

Each Storage Data Collection Agent gathers and saves Storage MIB data to files in the Storage Data Registry. The Data Collection Agents periodically update MIB data at configurable poll intervals.

The agent responsible for managing the selected MIB data item performs SNMP set commands. Data Collection Agents generate SNMP trap commands.

The Storage data registry (/var/spool/compaq/hpasm/registry) is composed of standard Linux directories and associated files. Each file in the data registry is a logical object containing “n” related data items.

The -p poll_time command line argument, which can be used with the Storage Agents, specifies the number of seconds to wait between data collection intervals. The minimum allowed value is 1 second and the default value is 15 seconds.

Increasing the agent poll_time setting improves system performance but decreases the data collection rate. Conversely, decreasing the agent poll_time setting increases the data collection rate but may decrease system performance.

A Storage Agent consists of the sub-agent components listed in Table 5.

Table 5. Sub-agents of the Storage Agent

Sub-agent	Description
IDA Agent (cmaidad)	The IDA Agent gathers data for the IDA MIB. The data includes: • IDA controller information • IDA accelerator information • IDA logical drive information • IDA physical drive information The IDA Agent is located in /opt/hp/hp-snmp-agents/storage/bin/cmaidad. The suggested poll_time is 15 seconds (default). The minimum recommended poll_time is 5 seconds.

Sub-agent	Description
IDE Agent (cmaided)	The IDE Agent gathers data for the IDE MIB. The data includes: • IDE host controller information • ATA disk information • ATAPI device information The IDE Agent is located in /opt/hp/hp-snmp-agents/storage/bin/cmaided. The suggested poll_time is 15 seconds. The minimum recommended poll_time is 5 seconds.
FCA Agent (cmafcad)	The FCA agent gathers data for the FCA MIB. The data includes: • FCA host controller information • FCA array controller information • FCA array accelerator information • FCA logical drive information • FCA physical drive information • FCA storage system chassis information • FCA storage system power supply information • FCA storage system fan information • FCA storage system temperature information • FCA storage system backplane information The FCA Agent is located in /opt/hp/hp-snmp-agents/storage/bin/cmafcad. The suggested poll_time is 15 seconds (default). The minimum recommended poll_time is 5 seconds.
SCSI Agent (cmascsid)	The SCSI Agent gathers data for the SCSI MIB. The data includes: • SCSI host controller information • SCSI disk drive information • SCSI tape drive information The SCSI Agent is located in /opt/hp/hp-snmp-agents/storage/bin/cmascsid. The suggested poll_time is 15 seconds. The minimum recommended poll_time is 5 seconds.
SAS Agent (cmasasd)	The SAS Agent gathers data for the SAS MIB. The data includes: • SAS host controller information • SAS disk drive information • SAS tape drive information The SAS Agent is located in /opt/hp/hp-snmp-agents/storage/bin/cmasasd. The suggested poll_time is 15 seconds. The minimum recommended poll_time is 5 seconds.
Event Daemon (cmaeventd)	The Event Daemon gathers storage hardware events from the firmware and passes them on to other agents upon request. The Event Daemon is located in /opt/hp/hp-snmp-agents/storage/bin/cmaeventd.

1-2-3 NIC Agent (cmanic)

The NIC Agent collects information from network interface controllers at periodic intervals, makes the collected data available to the SNMP agent, and provides SNMP alerts. The NIC Agent gathers data for the NIC MIB from supported NIC device drivers. The data includes:

- Physical mapping and configuration data for each network interface.
- Network statistics for Ethernet interfaces. Information is provided for HP controllers. Limited information may be provided for third-party NICs.

1-2-4 Data Collection Agent

Data Registries are composed of standard Linux directories and associated files. Each file in the data registry is a logical object containing "n" related data items.

The MIB items supported by the Server Data Collection Agents are listed in the /opt/hp/hp-snmp-agents/mibs/cmafdtnobjects.conf and /opt/hp/hp-snmp-agents/mibs/cmasvrobjects.conf files.

During installation, each agent is configured to start automatically after the SNMP Agent (snmpd) is started and to stop after snmpd is stopped.

1-2-5 Lights Out Agent

A Lights Out Agent consists of the sub-agent components listed in Table 6.

Table 6. Sub-agents of the Lights Out Agent

Sub-agent	Description
Remote Insight/Integrated Lights-Out Agent (cmasm2d)	The Remote Insight/Integrated Lights-Out Agent (cmasm2d) gathers data for the Remote Insight/Integrated Lights-Out MIB. The data includes: • Configuration and statistical information for the Remote Insight Board or Integrated Lights-Out (RIB/RILOE/iLO). • Events logged to the RIB or iLO. • Configuration and statistical information for the Remote Insight/Integrated Lights-Out NIC.
Rack Agent (cmarackd)	The Rack Agent (cmarackd) monitors the rack health through the systems management microprocessor on the server, the microprocessor on the server enclosure, and the microprocessor on the power enclosure.
ProLiant Rack Infrastructure Interface Service (cpqriis)	The ProLiant Rack Infrastructure Interface Service (cpqriis) enables communication through the Integrated Lights-Out Management Component to the rack infrastructure. The HP ProLiant Rack Infrastructure Interface Service (cpqriis) opens and sustains communication with the Integrated Lights-Out management controller. This communication link is vital to obtain a connection to the ProLiant BL p-Class enclosure management controllers in the back of the rack. Without this connection, other applications like the Rack Upgrade Utility and Rack Agent do not work. The service also receives any type of alerts from the Rack Infrastructure and logs those into the OS logging facility.

1-2-6 Using the HP ProLiant BL Rack Upgrade Utility

The HP ProLiant BL Rack Upgrade Utility upgrades the firmware on the server blade and power management modules in the rack.

For iLO reflash and firmware upgrade information, see the Integrated Lights-Out User Guide located at http://h18013.www1.hp.com/manage/ilo-description.html.

```
cpqblru [-eql?]  [-a address1,address2,...]  [-c chassis1,chassis2,...]
```

Table 7. ProLiant BL Rack Upgrade Utility parameters

Parameter	Description
-a address1,address2,...	This optional parameter considers only enclosures with address1, address2, and so on. The list of addresses must be composed of 16-bit quantities separated by commas. The addresses can be obtained by running –q (see below). No white spaces are allowed in between the commas and the addresses. If a no comma-separated list is given, all possible addresses in the rack are considered.
-c chassis1, chassis2,...	This optional parameter considers only enclosures with positions chassis1, chassis2, and so on that are counted from the bottom. The list must be composed of small numbers that are legal positions in the rack. No white spaces are allowed in between the commas and the numbers. A list such as 1,2,5 signifies the bottom, second-to-bottom, and fifth-to-bottom enclosures.

Parameter	Description
-e	This parameter disregards the local enclosure (for example, the enclosure containing the server from which you flash) in the flashing. This parameter is given in conjunction with –a or –c.
-l	This parameter disregards anything but the local enclosure (for example, the enclosure containing the server from which you flash). This parameter should not be given with –a or –c.
-q	This parameter queries the chassis positions, their serial numbers, and their firmware status and returns their addresses.

The man page for this utility may be viewed by entering `man cpqblru` at the command prompt.

Note the following while upgrading ProLiant BL p-Class enclosure management controllers:

- During a flash upgrade, only the primary firmware image is reflashed. All controllers have a backup image. The backup image is used for recovery purposes when a flash upgrade is interrupted or otherwise fails. Restoring the backup firmware image is rarely needed and is covered in the Integrated Lights-Out User Guide located at http://h18013.www1.hp.com/manage/ilo-description.html.
- When updating enclosure management controllers in more than one enclosure, the new image must be transmitted twice (first to the local enclosure and second to the remote enclosures using broadcast mode). The update process can take 10 minutes or more. The update process notifies the user if the update succeeded or failed.
- The reflash operation consumes all bandwidth of the bus connecting the management controllers. Consequently, other software components, such as the ProLiant Rack Agent might not report up-to-date information during the flash upgrade.

1-3 HP OpenIPMI Driver (hp-OpenIPMI)

The hp-OpenIPMI device driver is a derivative work of the IPMI device driver that ships with the standard Linux kernel. This driver has been enhanced to include bug fixes in addition to supporting a PCI Base Management Controller (BMC), such as the one provided by the HP Integrated Lights-Out 2 (iLO 2) management controller. The file /opt/hp/hp-OpenIPMI/IPMI.txt is also a derivative of the Documentation/IPMI.txt file included with the standard Linux kernel. This file has been enhanced to document the additional parameters that can be passed to the ipmi_si.ko driver. The hp-OpenIPMI device driver enhancements are expected to be incorporated into the OpenIPMI device driver (www.openipmi.org) and subsequently, the standard Linux kernel. This driver can be used with other applications in addition to the HP Advanced System Management XL (hpasmxl) application.

1-4 HP ProLiant Channel Interface Device Driver for iLO/iLO2 (hp-ilo)

The HP ProLiant Channel Interface Device Driver for iLO/iLO2 (hp-ilo) enables iLO data collection and integration with the ProLiant Management Agents and the rack infrastructure interface service. The driver enables communication routing of SNMP traffic from the ProLiant Management Agents through the dedicated iLO management NIC.

For documentation on Integrated Lights-Out, which is supported by the iLO Management Interface Driver, visit http://h18013.www1.hp.com/products/servers/management/ilo2.

See the QuickSpecs for each product to determine the servers and operating systems supported.

1-5 HP System Management Homepage (hpsmh)

The HP System Management Homepage is a web-based interface that consolidates and simplifies single system management for HP servers running Linux operating systems. The System Management Homepage aggregates and displays data from Web Agents and other HP Web-enabled System Management Software that includes HP Insight Diagnostics, the Array Configuration Utility, and the HP Software Version Control Agents. The System Management Homepage enables IT administrators to view in-depth hardware configuration and status data, performance metrics, system thresholds, diagnostics, and software version control information using a single intuitive interface.

Additional information about Insight Management Agents is available at http://h18013.www1.hp.com/products/servers/management/agents/index.html.

Customers without automatic monitoring tools can view status information for servers that have the HP System Management Homepage, previously called ProLiant Management Agents, installed using a standard Web browser. The HP System Management Homepage responds to port 2381 (if the installed browser supports SSL encryption). For example, point the browser to https://192.1.1.20:2381 or https://localhost:2381 (the "https://" portion of the address is required).

The HP System Management Homepage allows you to view subsystem and status information from a Web browser, either locally or remotely.

Tip:
To install System Management Homepage (hpsmh), you must be logged in as "root." See the *hpsmh Installation Guide* for detailed information at http://bizsupport.austin.hp.com/bc/docs/support/SupportManual/c00293364/c00293364.pdf.

1-6 HP System Management Homepage Templates (hp-smh-templates)

The information that hp-snmp-agents makes available through SNMP can be viewed in the HP System Management Homepage. The HP System Management Homepage Templates (hp-smh-templates) package provides the necessary files to link the SNMP data to the HP System Management Homepage. hp-snmp-agents and hpsmh are prerequisites for installing hp-smh-templates.

1-7 Systems Insight Manager

HP System Insight Manager (HP SIM) combines the strengths of Insight Manager 7, HP Toptools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Linux and other operating systems. The core HP SIM software uses WBEM to deliver the essential capabilities required to manage all HP server platforms.

HP SIM can be extended to provide system management with plug-ins for HP clients, storage, power, and printer products. Plug-in applications for workload management, capacity management, virtual machine management, and partition management through the Integrity Essentials enable you to pick the value-added software required to deliver complete lifecycle management for your hardware assets.

For installation information, see the "Installing on Linux" section of the *HP Systems Insight Manager Installation and User Guide*, which is available for download at http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html.

2 Manual Installation

This section describes how to install, upgrade, and remove the packages for HP System Health Application and Command Line Utilities (hp-health) and Insight Management SNMP Agents for HP ProLiant Systems (hp-snmp-agents). The latest versions of this software can be downloaded from http://hp.com/go/proliantlinux.

2-1 Prerequisite: Installing package dependencies

The software described in this HOWTO is distributed in standard package formats that provide prerequisite information internally. If you attempt to install a component that does not have its prerequisites fulfilled, the installation will abort and you will be given a list of missing prerequisites. Any prerequisite packages not described in this HOWTO should have been provided as part of your operating system installation media. Consult the documentation provided by your Linux distribution for information on locating and installing the requested software, and then retry the installation.

For full functionality, the hpsmh package requires the following components:

- SNMP stack of the Linux distribution
- Java Virtual Machine Version 1.4.1 (or greater)

Note:
If you have installed earlier versions of ProLiant manageability software, such as the HP System Health Application and Insight Management Agents (hpasm), the HP Lights-Out Driver and Agents (hprsm), and NIC Agents (cmanic), see "Transitioning from hpasm, hprsm, and cmanic packages" on page 15.

2-1-1 Installing the HP OpenIPMI Driver (hp-OpenIPMI)

The Linux kernel .config file must have IPMI support enabled for rebuilds. This is not the default on some older Linux distributions. If a different Linux kernel, such as an errata kernel, is used in place of the supported version of Linux, the standard Linux kernel build environment must be installed. Error messages are displayed during the rebuild process indicating which Linux packages are missing.

If a previous version of the hp-OpenIPMI package has been installed, it must be removed before this package can be installed. To remove the previous version and any packages dependent on it, enter the following:

```
# /etc/init.d/hp-snmp-agents stop
# /etc/init.d/hp-health stop
# rpm -e hp-OpenIPMI
```

To install hp-OpenIPMI RPM, enter the following:

```
# rpm -Uvh hp-OpenIPMI-<version>.rpm
```

Upon startup, the hp-health service will detect and use the hp-OpenIPMI drivers instead of the distribution-provided drivers.

For more information about these components, see the online documentation by entering:

```
$ man hp-OpenIPMI
```

2-1-2 Installing the HP System Health Application and Command Line Utilities (hp-health)

To install hp-health, login as the root user, and then enter:

```
# rpm –Uvh hp-health-<version>.<distribution>.<platform>.rpm
```

Note:
The version number for the RPM file varies depending on the supported systems and functionality. The distribution refers to the Linux distribution supported by the RPM. The platform refers to the processor architecture the RPM was built to support. The RPM file has a binary compiled for the supported distribution with the default kernel.

After the installation process, the health service is configured to automatically start each time your system boots. To start the service without rebooting, enter:

```
# /etc/init.d/hp-health start
```

The health service can take more than 2 minutes to load, which is expected behavior. On systems with variable speed fans, the fans might start spinning more slowly if the temperature is reasonably low.

To check if the Health Monitor is loaded properly, enter the following command (which is only available when logged in as system administrator, super user, or root):

```
/etc/init.d/hp-health status
```

2-1-3 Installing the HP ProLiant Channel Interface Device Driver for iLO/iLO2 (hp-ilo)

To install hp-OpenIPMI RPM, enter the following:

```
# rpm –Uvh hp-ilo-<version>.rpm
```

This driver automatically loads upon system startup, or manually by entering:

```
# /etc/init.d/hp-ilo start
```

For more information about this component, see the online documentation by entering:

```
$ man hp-ilo
```

2-1-4 Installing the Insight Management SNMP Agents for HP ProLiant Systems

To install hp-snmp-agents, login as the root user, and then enter:

```
# rpm –Uvh hp-snmp-agents-<version>.<distribution>.<platform>.rpm
```

1. To configure and activate agents, execute the following command as root:

   ```
   # /sbin/hpsnmpconfig
   ```

2. Provide basic Simple Network Protocol (SNMP) information, when prompted. The drivers and agents are inserted immediately.
3. To check if the agents are loaded properly, enter the following command:

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

   For more information about these components, see the online documentation by entering:

   ```
   $ man hp-snmp-agents
   ```

2-2 Uninstalling drivers and agents

There are two options for preventing the drivers and agents from running, uninstalling, and starting or stopping drivers. For information on uninstalling or unloading drivers or agents, see "Starting and stopping agents and services" on page 17.

Table 8 lists the commands for uninstalling the entire contents of the hpasm, hprsm, and cmanic packages.

Table 8. Uninstall drivers and agents commands

Uninstall Command	Description
`# rpm -e hp-snmp-agents`	Removes the hp-snmp-agents package from your system
`# rpm -e hp-ilo`	Removes the hp-ilo package from your system
`# rpm -e hp-health`	Removes the hp-health package from your system
`# rpm -e hp-OpenIPMI`	Removes the hp-OpenIPMI package from your system

Caution:
If a service is running when the corresponding package is removed, it is automatically shut down during the removal process.

2-3 Transitioning from hpasm, hprsm, and cmanic packages

Prior to the 8.1.0 release, the functionality and files provided by hp-health and hp-snmp-agents were distributed in alternate packages.

If you have a version of the HP System Health Application and Insight Management Agent (hpasm), the HP Lights-Out Drivers and Agents (hprsm), or the NIC Agents (cmanic) installed, you must uninstall these components before installing the new RPM files.

Note:
If you have any local customizations to the /etc/hpasmrc file, save a copy of that file before removing the hpasm component. After hp-snmp-agents has been installed, you can make the same modifications to the file /etc/hp-snmp-agents.conf.

To determine if these components are loaded, enter the command listed in the To verify installation column in Table 9. To remove the component, enter the command shown in the To remove column.

Table 9. Loaded components

Component	To verify installation	To remove
HP System Health Application and Insight Management Agents	`$ rpm -q hpasm`	`#rpm -e hpasm`
HP Light-Out Drivers and Agents	`$ rpm -q hprsm`	`#rpm -e hprsm`
HP OpenIPMI Device Driver	`$ rpm -q hp-OpenIPMI`	`#rpm -e hp-OpenIPMI`

Component	To verify installation	To remove
NIC Agents	`$ rpm -q cmanic`	`#rpm -e cmanic`

Note:
Remove cmanic and hprsm before removing hpasm, because of driver dependencies.

If concurrent access on the RPM database is attempted, the following messages can result:

- rpmQuery: rpmdbOpen() failed
- cannot get shared lock on database
- rpmQuery: rpmdbOpen() failed

2-4 Updating drivers and agents

The following section provides information on updating the HP ProLiant Management Software for Linux. Note that these instructions are only appropriate when upgrading from software with a version greater than 8.1.0. For information on transitioning from pre-8.1.0 versions, see “Transitioning from hpasm, hprsm, and cmanic packages” on page 15.

RPM provides the -U option to upgrade a package. For example, to upgrade hp-health to a newer version you could use the command:

```
# rpm -Uvh hp-health-<version>.<distribution>.<platform>.rpm
```

See the rpm manpage in your Linux distribution for more information:

```
$ man rpm
```

3 Customization

This section includes advanced topics on data center customization.

3-1 Configuration files

The ProLiant Management Agents Configuration file /opt/hp/hp-snmp-agents/cma.conf is shared by all HP ProLiant Management Agents. Currently, exclude directives, taint directives, trap interface, trap email notification configuration, and base socket number (used by cmaX) are supported. The agents are capable of sending email notifications in addition to SNMP traps. The trapemail entries in /opt/hp/hp-snmp-agents/cma.conf configure the email commands, which are then read by the Peers software during their initialization.

The exclude directives allow customization of which agents to start automatically. Any drivers and agents included on this line will not be started by the run level scripts.

The exclude entries can be modified using the /sbin/hpsnmpconfig command.

If trapemail entries are edited, the Peers software must be restarted before the configuration modification is effective. The command to restart the SNMP agents is:

```
#/etc/init.d/hp-snmp-agents restart
```

The syntax of the trapemail lines is:

```
trapemail mail_command
```

The keyword "trapemail" indicates that the rest of the line is the command for sending trap email. In mail_command, you must provide the full path of your email command, the subject, and the recipients.

Multiple trapemail lines can be defined in /opt/hp/hp-snmp-agents/cma.conf. A default line is added during installation if none exists:

```
trapemail /bin/mail -s 'HP Insight Management Agents Trap Alarm' root
```

The mail_command can be any Linux command that reads standard input. For example, using trapemail /usr/bin/logger will log trap messages to the system log file (/var/log/messages).

The cmaXSocketBase entry in configuration file /opt/hp/hp-snmp-agents/cma.conf configures the starting socket port used for communications between cmaX and Peers. The entry is not needed unless the "bind() failed!" message displays in the Agents log file /var/spool/compaq/cma.log.

This entry should be listed in the configuration file as follows:

```
cmaXSocketBase 12345
```

The trapIf entry in configuration file /opt/hp/hp-snmp-agents/cma.conf can be used to configure the IP address used by the SNMP daemon when sending traps. For example, to send traps using the IP address of the eth1 interface you would add:

```
trapIf eth1
```

If the cmaXSocket Base entry is edited, the snmpd and Peers software must be restarted before the configuration modification is effective. You can do this by entering the following commands:

```
#/etc/init.d/snmpd restart
#/etc/init.d/hp-snmp-agents restart
```

You can also manipulate the /opt/hp/hp-snmp-agents/cma.conf file which contains one or more exclude directives. Any string after the exclude keyword is interpreted as an agent name that should not be started. Examples include:

```
exclude cmahealthd
exclude cmastdeqd
```

These two lines exclude two agents from the startup: the Health Agent (cmahealthd) and the Standard Equipment Agent (cmastdeqd).

3-2 Starting and stopping agents and services

After the initial installation, both the ProLiant Management Agents and the Health Monitor are loaded. Upon a reboot, the initscripts /etc/init.d/hp-health and /etc/init.d/hp-snmp-agents reload the Health Monitor and SNMP agents and drivers, even if a different kernel was used for the new run.

To start and stop the hp-health service at runtime, run:

```
# /etc/init.d/hp-health stop
# /etc/init.d/hp-health start
```

To start and stop the hp-snmp-agents at runtime, run:

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

You can also use distro-provided shortcuts for these commands.

For Red Hat and SuSE systems:

```
# service hp-health stop
# service hp-snmp-agents stop
```

3-3 Parameters

This section lists parameters for various agents and services.

Table 10 includes the command line arguments that can be passed to the NIC agents (cmanicd) from the /opt/hp/hp-snmp-agents/nic/etc/cmanicd script.

Table 10. Parameters for NIC agents

Parameter	Description
-p poll_time	This parameter specifies the number of seconds between data caching and poll intervals. NIC drivers are only queried when a request comes in and the cached information is older than the specified poll interval. The default value is 20 seconds. The minimum poll time is 10 seconds.
-s set_state	This parameter specifies whether SNMP set commands are allowed for this agent. A set_state of OK (default) means that SNMP set commands are allowed. A set_state of NOT_OK means that SNMP set commands are not allowed.
-t trap_state	This parameter specifies whether the NIC Agent is allowed to send traps or not. A trap_state of OK (default) indicates the NIC Agent can send SNMP traps. A trap_state of NOT_OK means that the NIC Agent is not allowed to send traps.

For example, to set the poll interval to 30 seconds and prevent traps, change PFLAGS= to PFLAGS="-p30 -t NOT_OK" in the /opt/hp/hp-snmp-agents/nic/etc/cmanicd script.

Traps are configured using the standard SNMP configuration file (snmpd.conf). See the snmpd.conf manual page for the most current configuration information. When the snmpd.conf or snmpd.local.conf configuration files are changed or when the SNMPCONFPATH environment variable is changed, the cmanic daemon must be restarted.

If your operating system has an active firewall configuration, external SNMP requests might be rejected by the system, which prevents remote management operation. Your system must be configured to allow udp connections on port 161 from any hosts that need to be able to send SNMP requests. There are significant security implications to configuring a firewall. Consider the iptables, ipchains, iptables-save, and iptables-restore man pages and the documentation for any firewall configuration application in use as mandatory reading before making any change to the firewall configuration.

The Rack Infrastructure Interface Service is contained in an executable called cpqriisd which resides in the /sbin directory. It can be invoked by using the commands in Table 11.

Table 11. Command options for the Rack Infrastructure Service

Option	Description
-F	This option will "daemonize" the process and start the daemon in a production level environment. Usage is recommended. An easier way to accomplish this task is to execute the hp-snmp-agents run-level script.
-D	This option starts the service in a debug environment. stdin and stdout go to the console; typing "e" will stop the daemon. Alerts are logged in to the same text console.
-V	This option enables the verbosity of the output. The default behavior is to output to both /var/log/messages and tty1 – tty10.
-?	This option reports the version of the service and informs the user of the other options described above.

Appendix A – Error messages

Messages logged if an ASR event occurs are listed in Table 12.

Table 12. Error messages

Message number	Details	
Message 1	NMI - Automatic Server Recovery timer expiration - Hour %d - %d/%d/%d	
	Description	This message indicates that the Health Monitor detected an ASR timeout and is attempting to gracefully shut down the operating system. Absence of this message can indicate a critical hardware failure (such as a non-correctable ECC error on a memory DIMM) or some other severe event. This is the first of a series of messages displayed to the console. This message is not be logged to the IML and most likely not be listed in any system logs.
	Recommended action	Review all the messages logged to the IML to see if any previous errors have been logged (for example, a corrected single-bit memory error might have been logged).
Message 2	ASR Lockup Detected: %s	
	Description	This message indicates that the Health Monitor detected an ASR timeout and is attempting to gracefully shut down the operating system. Absence of this ASR message can indicate a critical hardware failure (such as a non-correctable ECC error on a memory DIMM) or some other severe event. This is the first ASR message logged to the IML (if logging is possible).
	Recommended action	Review all the messages logged to the IML to see if any previous errors have been logged.
Message 3	casm: ASR performed a successful OS shutdown	
	Description	This ASR message indicates that the Health Monitor detected an ASR timeout and has gracefully shut down the operating system. Absence of this message can indicate a hardware failure (such as a non-correctable ECC error on a memory DIMM), a high priority process consuming all the available CPU cycles (software failure), or a device, such as a storage or network controller, flooding the system with interrupts. This is the second ASR message logged to the IML if logging is possible.
	Recommended action	This ASR message usually indicates a software error such as a high priority process consuming all the available CPU cycles. Linux tools, such as SAR (system activity report) can be used in conjunction with the ASR facility to locate the process causing the problem.
Message 4	ASR Detected by System ROM	
	Description	This message indicates that the ProLiant Server ROM detected an ASR timeout. This message is almost always present in the IML when an ASR timeout occurs. If this is the only ASR message logged to the IML, this can indicate a hardware failure (such as a non-correctable ECC error on a memory DIMM). The ASR feature on a ProLiant server resets the server when the timeout expires, with no software intervention required.
	Recommended action	If this is the only ASR message present, this usually indicates a hardware error (such as an unrecoverable memory error). Try moving the server memory DIMMs to different slots to see if more information can be logged. Review all IML messages that previously occurred to see if any other component has given an indication of failure or temperature limits that might have exceeded normal operating thresholds.

The cpqriisd service acts as an enabler for other ProLiant value-add software, such as the Rack Agent and the Rack Upgrade Utility. This service is only applicable for p-Class blade systems.

If the service goes away after a few seconds, there is a failure to initiate communication with the iLO management controller. The failure reason is logged in the message log. If the service is stopped, dependent applications like the Rack Firmware Upgrade Utility terminate as well.

Table 13 lists possible issues.

Table 13. cpqriisd messages

Message number	Details	
Message 1	Could not setup server semaphores Could not destroy server semaphores Up sem: Ioctl Failure ! Down sem: Ioctl Failure ! Down sem Down sem: Ioctl Failure ! Down sem get sem: Ioctl Failure ! set sem: Ioctl Failure !	
	Description	These messages indicate that synchronization objects, called "semaphores," cannot be set up correctly. This issue most likely occurs because the iLO driver is absent.
	Recommended action	Install the iLO driver.
Message 2	Warning: Shared Memory Segment exists Killing process %s pid %d pgid %d	
	Description	These messages indicate that the daemon encountered a shared memory segment that was not cleaned up properly.
	Recommended action	No action is required, since this message is informational. This warning will be removed in a later version of the Rack Infrastructure Interface Service.
Message 3	Multiple copies of this daemon may be running - exiting...	
	Description	This message indicates an issue with Version 1.0.0 of the Rack Infrastructure Interface Service, which disallows the starting of two copies of the service.
	Recommended action	Only one copy of the daemon should be running at any time.
Message 4	Setup Shared Memory failed!	
	Description	This message indicates that a common OS resource, "shared memory," is not available. This issue could be due to high utilization, but most likely a memory segment from an earlier version of this service was left behind erroneously.
	Recommended action	Install the latest version of this service.
Issue 5	Semaphore %s interrupted in %s Local Semaphore %s interrupted in %s	
	Description	This type of message will be logged if the service is terminated abruptly (for example, through the kill command).

Message number	Details	
	Recommended action	No action is required, since this message is informational.
Issue 6	Alert only seems to reach %d out of %d client applications	
	Description	The alerts coming from the infrastructure seem to be dispatched to a subset of registered clients only. Most likely, a client terminated suddenly without properly deregistering itself.
	Recommended action	This message does not indicate a problem with the Rack Infrastructure Interface Service; however, there might be a problem with the HP ProLiant Rack Daemon (cmarackd). Restart cmarackd. If the problem persists, contact your HP field service engineer.
Issue 7	ILO exceeded the number of allotted back offs, is it stuck?	
	Description	iLO responds with a backoff command indicating a busy state, which is a temporary condition. If this condition lasts too long (5000 tries), the message appears.
	Recommended action	Verify that iLO is not under extreme network load, such as a ping flood. Otherwise, contact your HP field service engineer.
Issue 8	Data returned is too short for any transaction	
	Description	Data corruption from iLO has occurred. The data received is ignored.
	Recommended action	Reboot iLO by navigating to the Network Settings tab in the iLO Web interface and clicking **Apply**. If you continue to see this message, contact your HP field service engineer.
Issue 9	watchdog sees no dispatch threads cpqci watchdog: close channel! cpqci watchdog: reopen channel!	
	Description	These messages indicate that iLO was reset and that the service is trying to reopen communication.
	Recommended action	No action is required, since this message is informational.
Issue 10	Problems setting up shared memory Problems setting up semaphores Problems setting up local semaphore Problems setting up watchdog thread Problems setting up IPMI channel Problems setting up dispatch thread Problems setting up secondary dispatch thread Problems setting up dispatch threads Did not receive initial handshake Problems pushing IPMI traffic over channel! Problems setting up dispatch data Problems setting up stats data Problems setting up dynamic mem allocator! Problems setting up hash table! Problems setting up communication with channel! Problems setting up watchdog thread!	

Message number	Details	
	Description	These messages indicate a problem that occurred during initialization of the service. The main reasons for failure include: • Absence of the iLO Driver. • iLO encountered problems and is in an undefined state. • The operating system is running out of resources (for example, memory, threads, semaphores, and so on).
	Recommended action	Verify that the iLO Driver is installed and reboot the server.
Issue 11	start failed. started and stopped. -- failed.	
	Description	This message indicates that the service terminated itself because of problems.
	Recommended action	Install Version 1.1.0-2 of the service. Verify that the iLO Driver is installed and reboot the server. If problems persist, contact your HP field service engineer.
Issue 12	Dispatcher still sees %d clients...	
	Description	A client does not respond properly to impending shut down. Consequently, the service waits for approximately 5 seconds, outputs this message, and exits.
	Recommended action	No action is required, since this message is informational. However, this message could also indicate that the HP ProLiant Rack Daemon (cmarackd) has died.
Issue 13	Checksum on SEEPROM %2.2x do not match for header (%2.2x)	
	Description	This message indicates that the EEPROMs in the infrastructure are corrupt.
	Recommended action	Contact your HP field service engineer for resolution.
Issue 14	Error: copy ipmb response with negative length %d Error: copy ipmb response with excessive length %d	
	Description	These messages indicate that a corrupt response from the infrastructure was received.
	Recommended action	Reboot the HP ProLiant Power Module.

Appendix B – Troubleshooting

This section describes common problems that might occur during installation and operation of the HP ProLiant Management Software for Linux.

Table 14 describes issues and workarounds for the hp-health and hp-snmp-agents packages. Any problems reported to HP should include the following files:

- /var/log/messages
- /var/log/boot.log (for Red Hat Linux distributions)
- /var/log/warn (for SuSE LINUX distributions)
- /var/spool/compaq/cma.log
- /var/spool/compaq/hpasmd.log

Table 14. Known issues for hp-health

Issue number	Details	
Issue 1	Non-certified machines	
	Symptom	When the hpasm RPM file is installed, the following message displays: `hpasm:  This driver is not supported on this system` The driver is not inserted into the list of modules.

	Cause	The Health Monitor cannot be initialized due to a conflict in ROM internal tables, or the server is not supported. This driver is only supported on servers that have the ProLiant Advanced Server Management (ASM) ASIC (PCI identifier 0x0e11a0f0 or the Integrated Lights-Out Management ASIC (PCI identifier 0x0e11b203)). No other ProLiant servers are supported.
		Verify that the appropriate ASM ASIC is present. Use the following commands to perform the check:
		`cat /proc/bus/pci/devices | grep –I 0e11a0f0`
		`cat /proc/bus/pci/devices | grep –I 0e11b203`
		One of these commands should succeed and return information. Also, check to see if a later ROM version is available for this server.

Issue 2	The hp-snmp-agents custom build does not work	
	Symptom	The hpasm_rebuild script logs messages to the console and exits.
	Cause	You must execute the custom build script as user name “root.” The RPM must be available to you and you should start the script with the version of the package that you installed (for example 6.30.0).
	Workaround	Install RPM and make sure it is available from your PATH variable.
Issue 3	No console messages	
	Symptom	No console messages appear on the text screens (for instance, Ctrl+Alt+F1), but the error messages get logged properly in /var/log/messages. If you run KDE or Gnome, xterms does not show the console messages originating from the Health Monitor.
	Cause	The syslogd daemon is configured somewhat differently than other distributions; the system messages do not appear on the lower digit terminals (tty1-9).

	Workaround	If you do not want the message to be logged on the system, configure it differently by modifying /etc/syslog.conf in the following way:
		`# Log all kernel messages to the console.`
		`# Logging much else clutters up the screen.`
		`kern.* /dev/console`
		`# Log anything (except mail) of level info or higher.`
		`# Don’t log private authentication messages!`
		`*.info;mail.none;news.none;authpriv.none /var/log/messages`
		After sending a HUP signal to syslogd process ID, you should see your kernel messages appearing on all consoles.
		“kill –1 <pid of syslogd>”

Issue 4	Superuser only	

Issue number	Details	

	Symptom	You experience the following problems:
		• Commands like insmod, modprobe, rmmod, or rpm are not available.
		• The RPM install fails because file permissions are being denied (see below).
		`"Failed to open //var/lib/rpm/packages.rpm`
		`error: cannot open //var/lib/rpm/packages.rpm"`

	Cause	Preparing a driver install necessitates access to system administrator rights.
	Workaround	Be sure to log in as "root" before you attempt the driver install.
Issue 5	The agents do not seem to expose their data through SNMP; my management console does not see any status.	
	Symptom	Through SNMP browsers or other management software, the servers appear dead. No SNMP traffic is available through them.
	Cause	This can be caused by many things. Here is a checklist of the most common problems: • SNMP is not running. • The agents and/or drivers have not started properly (see Issue 7). • The snmpd.conf file is misconfigured. – rwcommunity is undefined for either localhost or the management console. – -community string mismatches the one from the management console. – trapsink or trapcommunity is undefined. Trapcommunity may be undefined for localhost. • Firewalling software is enabled on the system and set up to block SNMP traffic. • The cmaX extension is absent from the snmp stack.

Table 15 describes common problems that might occur during installation and operation of the Host OS Agent, the Standard Equipment Agent, the SCSI Agent, the System Health Agent, the Threshold Agent, and the Peer Agents. In most cases, a workaround is available.

Table 15. Known issues for agents

Issue number	Details	
Issue 1	Cannot manage server from Systems Insight Manager, grayed-out utilization button, or missing file system space used information in the mass storage window	
	Workaround	To work around this issue, complete the following steps: 1. Check if the network is working by pinging the server from the system running Systems Insight Manager. 2. Be sure that Systems Insight Manager is using the correct community string, which is defined in the server's snmpd.conf file. 3. Be sure that post-installation configurations have been performed properly, if needed. 4. Check the Host OS Agent status with the Linux command ps –ef | grep cmahostd. If the agent is not running, start the Host OS Agent manually using the following command: `#/opt/hp/hp-snmp-agents/server/etc/cmahostd start` If the Host OS Agent is running but not reporting data, or if it was correctly started but is no longer running, check the file /var/spool/compaq/cma.log for error messages. You must be logged in as "root" to access this file.
Issue 2	Grayed-out system board, expansion boards, or configuration buttons	

Issue number	Details	
	Workaround	Check the Standard Equipment Agent status with the Linux command `ps -ef | grep cmastdeqd`. If the agent is not running, start the Standard Equipment Agent manually using the following command: `#/opt/hp/hp-snmp-agents/server/etc/cmastdeqd start` If the agent is running but not reporting data, or if the agent was correctly started but is no longer running, check the file `/var/spool/compaq/cma.log` for error messages. You must be logged in as "root" to access this file.
Issue 3	Missing SCSI drive information in the mass storage window	
	Workaround	Check the SCSI Agent status with the command `ps -ef | grep cmascsid`. If the agents are not running, they must be started (see the start/stop documentation for the appropriate agent). If the agent is running but not reporting data or, if it was correctly started but is no longer running, check the file /var/spool/compaq/cma.log for error messages. You must be logged in as "root" to access this file.
Issue 4	Added SCSI devices do not appear	
	Workaround	To minimize system overhead, the cmascsid process does not search for new hardware every poll_time. There is a delay of up to 32 times the poll interval, which is normally every 30 seconds, up to 16 minutes in the default case, before new SCSI devices are discovered by cmascsid and reported to the ProLiant Management Console. Once the hardware has been discovered, its status is checked each poll_time and reported to ProLiant Management Console when it has changed.
Issue 5	Missing or 0-value SCSI hard drive serial number or capacity	
	Workaround	Most SCSI hard drives do not make this information available to the host when the drive media is not spinning. Hot-pluggable drives do not start spinning until the operating system attempts to open them. Obtaining this information requires access to the drive. After the drive is first opened, to minimize system overhead, there can be a delay of up to 32 times the poll_time of the cmascsid process before updated information is available to the ProLiant Management Console.
Issue 6	Grayed-out button for a SCSI controller	
	Workaround	Information about the configuration of the device indicates that a SCSI controller is installed, but no further information is available. Several conditions result in a grayed-out button: • The SCSI agent process "cmascsid" might not be running. • The SCSI controller might have been disabled by the System Configuration Utility. • This might be an unsupported controller.
Issue 7	Missing or grayed-out storage controllers in the mass storage window	
	Workaround	Check the Mass Storage Agent status with the Linux command ps -ef | grep cma. See the entries for cmaidad, cmafca, cmascsid, cmasasd, and cmaided. • If the agent is not running, it must be started (see the start/stop documentation for the appropriate agent). • If the agent is running but not reporting data, or if it was correctly started but is no longer running, check the file /var/spool/compaq/cma.log for error messages. You must be logged in as "root" to access this file.
Issue 8	Grayed-out recovery button in the device view window, grayed-out auto recovery button in the recovery window, or grayed-out environment button in the recovery window	

Issue number	Details	
	Workaround	To work around this issue, complete the following steps: 1. Be sure your system supports the System Health Agent features. These features are supported only on HP ProLiant servers. 2. Check the System Health Agent status with the Linux command `ps -ef | grep cmahealthd`. If the agent is not running, it must be started (see the start/stop documentation for the System Health Agent).
Issue 9	Grayed-out Remote Insight button in the recovery window	
	Workaround	A grayed-out Remote Insight button can be caused by one of the following: • The Remote Insight Controller might not be configured properly. • The Remote Insight Driver might not be installed. • The Remote Insight Agent cmasm2d might not be running.
Issue 10	Unable to change any values on the managed server or no SNMP traps/alarms are received	

	Workaround	To work around this issue, complete the following steps:
		1. Be sure that the SNMP Agent, the Peer agent, and the agent processing the set are all running.
		2. Check the agent command line arguments in the agent start script files.
		3. Verify that either the argument -s OK is present or that default set_state is OK for the agent. This process enables SNMP sets for this agent only.
		4. Verify that the server SNMP community string defined in your snmpd.conf (using rwcommunity keyword) matches the community string defined at the management console.
		If you are using Systems Insight Manager, the community string can be set in the Device Setup window. For more information, see the section on community strings in the *Systems Insight Manager User Guide Help* file.
		If you changed the snmpd.conf files, you need to refresh snmpd and agents with the following commands:
		`#/etc/init.d/snmpd restart`
		`#/etc/init.d/hp-snmp-agents restart`
		5. Test the traps by setting a threshold on an item that will cause a trap using the Set Threshold feature of Systems Insight Manager. See the section "Set Threshold" in the *Systems Insight Manager User Guide* for more information.
		If traps still do not function, have your Linux device send traps to itself. Run the Linux SNMP trap receiving utility snmptrapd –P.
		Next, generate a trap to localhost using the Linux snmptrap utility. The Linux command `snmptrapd –f -Le` should display the trap. Note that recent versions of snmptrapd will not accept incoming notifications by default. See snmptrapd.conf(5) for information on configuring access control settings to enable incoming notifications.

Issue 11	Unable to set thresholds on MIB items or no user-defined SNMP traps are received	

Issue number	Details	

	Workaround	Check the Threshold Agent status with the Linux command: `ps -ef | grep cmathreshd`. If the agent is not running, start the Threshold Agent using following command:
		`#/opt/hp/hp-snmp-agents/server/etc/cmathreshd start`
		If the agent is running but not reporting data, or if it was correctly started but is no longer running, check the file `/var/spool/compaq/cma.log` for error messages. You must be logged in as "root" to access this file. Verify that the server SNMP community string defined in your `snmpd.conf` (using rwcommunity keyword) matches the community string defined at the management console. If you are using Systems Insight Manager, the community string can be set in the Device Setup window. For more information, see the section on community strings in the *Systems Insight Manager User Guide Help* file.
		If sets still do not work, perform the following procedure:
		1. Stop the Threshold Agent and delete previous alarm threshold files using the following command:
		`# /opt/hp/hp-snmp-agents/server/etc/cmathreshd stop`
		2. Start the Threshold Agent using the following command:
		`# /opt/hp/hp-snmp-agents/server/etc/cmathreshd start`

Issue 12	Disabling SNMP sets for a specific agent	
	Workaround	Stop the agent associated with the desired MIB. Change the agent command line argument set switch to -s NOT_OK in the corresponding /opt/hp/hp-snmp-agents/<agent>/etc/<subagent> file. This disables SNMP sets for this agent only. Restart the agent.
Issue 13	Disabling SNMP traps for a specific agent	
	Workaround	Stop the agent. Change the agent command line argument trap switch to -t NOT_OK in the /opt/hp/hp-snmp-agents/<agent>/etc/<subagent> file. This disables SNMP traps for this agent only. Restart the stopped agent.
Issue 14	Disabling remote reboot	
	Workaround	Stop the Server Standard Equipment Agent using following command: `#/opt/hp/hp-snmp-agents/server/etc/cmastdeqd stop` Edit /opt/hp/hp-snmp-agents/server/etc/cmastdeqd and change the cmastdeqd agent command line reboot switch to -r NOT_OK. This disables SNMP reboots for this device only. Restart the Standard Equipment Agent.
Issue 15	Peer Agents will not run	

	Workaround	Check the /var/spool/compaq/cma.log file for messages. If it is caused by not running snmpd, then configure snmpd to start automatically during boot. If you changed the snmpd.conf files, you must refresh snmpd and agents with the following commands:
		`#/etc/init.d/snmpd restart`
		`#/etc/init.d/hp-snmp-agents restart`

Appendix C – hp-snmp-agents command lines and arguments

Table 16 lists the command lines and Table 17 lists the command arguments for hp-snmp-agents.

Table 16. Command lines for hp-snmp-agents

Component	Description	Command
Server Agents		
cmahostd	Host daemon to collect data about installed software, firmware, and agent conditions	/opt/hp/hp-snmp-agents/server/etc/cmahostd
cmapeerd	Host daemon collected data made available to SNMP requesters	/opt/hp/hp-snmp-agents/server/etc/cmapeerd
cmathreshd	Daemon to monitor MIB items to exceed a certain threshold	/opt/hp/hp-snmp-agents/server/etc/cmathreshd
cmahealthd	Host daemon to collect temperature	/opt/hp/hp-snmp-agents/server/etc/cmahealthd
cmastdeqd	Host daemon to collect PCI/EISA slot information	/opt/hp/hp-snmp-agents/server/etc/cmastdeqd
cmaperfd	Daemon to collect performance data for CPU	/opt/hp/hp-snmp-agents/server/etc/cmaperfd
cmasm2d	Agent to collect data from iLO/RILOE	/opt/hp/hp-snmp-agents/server/etc/cmasm2d
cmarackd	Agent to collect data from the ICE infrastructure	/opt/hp/hp-snmp-agents/server/etc/cmarackd
Storage Agents		
cmaidad	Agent to collect data from cciss/cpqarray drivers	/opt/hp/hp-snmp-agents/storage/etc/cmaidad
cmaided	Agent to collect data from IDE devices	/opt/hp/hp-snmp-agents/storage/etc/cmaided
cmafcad	Agent to collect data from the cpqfc driver	/opt/hp/hp-snmp-agents/storage/etc/cmafcad
cmascsid	Agent to collect data from SCSI storage devices	/opt/hp/hp-snmp-agents/storage/etc/cmascsid
cmasasd	Agent to collect data from SAS storage devices	/opt/hp/hp-snmp-agents/storage/etc/cmasasd
Network Agents		
cmanicd	Agent to collect data from network interfaces	/opt/hp/hp-snmp-agents/nic/etc/cmanicd

Note: All agents support -p, -s, -t as startup parameters.

Note: Each agent has an associated run level script which is located in /opt/hp/hp-snmp-agents/<agent>>/etc/<subagent>. All important settings such as poll time arguments are contained in these individual scripts.

Table 17. Command arguments for hp-snmp-agents

Command line argument	Description
-p poll_time	Specifies the number of seconds to wait between data collection intervals. The minimum allowed value is 1 second and the default value is 60 seconds.
-s set_state	Specifies whether SNMP set commands are allowed for this agent. A set_state of OK (default) means that SNMP set commands are allowed. A set_state of NOT_OK means that SNMP set commands are not allowed.
-t trap_state	Specifies whether SNMP trap commands are allowed for this agent. A trap_state of OK (default) means that SNMP trap commands are allowed. A trap_state of NOT_OK means that SNMP trap commands are not allowed.

Call to action

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

© Copyright 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Linux is a U.S. registered trademark of Linus Torvalds.

501165-001, August 2008