

HP ProLiant and SecurePlatform Management

**OPSEC Engineering
May 2008**

**If you have any questions about this document contact us at
<http://www.opsec.com/contact.html>**

HP ProLiant Servers

ProLiant servers have long been known for reliability. In addition to unsurpassed product reliability, HP innovations provide platforms and solutions that improve data center efficiency while helping customers manage complexity and risk. The ProLiant management infrastructure creates an environment for life cycle management that optimizes data center efficiency and lowers TCO.

The HP Advanced Server Management Agents included in the ProLiant Support Pack collect and monitor important operational data on ProLiant servers is compatible with Check Point SecurePlatform.

SecurePlatform

The SecurePlatform Pro prehardened operating system enables administrators to install Check Point's market-leading VPN-1® gateways, SmartCenter™ management servers, and other products within five minutes on Intel or AMD based open servers. It eliminates the need for administrators to uninstall or reconfigure portions of the operating system or to apply fixes manually whenever a new vulnerability is found. Instead, SecurePlatform Pro provides a preconfigured, prehardened operating system that meets the requirements of the most demanding network environments.

The HP Health Application and Insight Management Agents for Red Hat Enterprise Linux 3 available in the ProLiant Support Pack that ship with HP ProLiant systems can be installed on SecurePlatform.

Check Point products that are compatible with Red Hat Enterprise Linux 3 packages

Product	Version
VPN-1	R60 and later including SecurePlatform 2.6 R65
Provider-1	R61 and later including SecurePlatform 2.6 R65
Integrity Server	R61 and later including EndPoint 7.0
Connectra	R61 and later

The Combined HP and Check Point Management Advantage

Security Management Architecture (SMART) Architecture	
Feature	Description
Central Management	SmartView Monitor - SmartView Monitor™ provides real-time

	monitoring of security, network, VPN tunnel, and user activity via a central console.
Configuration Management	SmartUpdate - SmartUpdate automatically distributes software applications and updates to Check Point products and manages product licenses. It provides a centralized means to guarantee that security throughout the network is always up to date.

Getting the status of the ProLiant Server

There are multiple ways to get the operational status of the ProLiant server. The ideal way is to load the Insight Manager agents and use a tool such as HP OpenView or Insight Manager to monitor the status of all the ProLiant servers. HP Systems Insight Manager provides hardware fault, asset, and configuration management for all of your HP Systems.

ProLiant Essentials Server Plug-Ins	
Feature	Description
Central Management	HP Systems Insight Manager System Health Application and Insight Management Agents - collects and monitors important operational data on ProLiant servers.
Configuration Management	Integrated Lights-out Advanced Pack - Control ProLiant servers remotely through a web-browser Intelligent Networking Pack ¹ - Minimize the risk of outages due to network failures or virus attacks Performance Management Pack ¹ - Identify systems with performance bottlenecks Rack and Power Manager ¹ - Grow with your datacenter demands for power protection and rack space
Software Deployment	HP BladeSystem Integrated Manager ¹ - Access all tools needed to configure and manage an HP BladeSystem environment System Management Homepage - Review in-depth system hardware configuration and status data, performance

	<p>metrics, system thresholds and software version control information</p> <p>Rapid Deployment Pack¹ - Automate unattended deployment of HP Bladesystem and ProLiant hardware</p> <p>Vulnerability and Patch Management Pack¹ - Identify and close security vulnerabilities before they result in unplanned downtime</p>
--	--

¹ – Not supported on SecurePlatform

HP Integrated Lights-Out

Integrated Lights-Out allows browser access to ProLiant servers through a seamless, hardware-based graphical Remote Console, Virtual Power Button, and Virtual Floppy. This functionality does not require an OS driver.

The iLO Management Interface Driver 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.

The Rack Agent monitors the rack through the systems management microprocessor on the server, the microprocessor on the server enclosure, and the microprocessor on the power enclosure.

The ProLiant Rack Infrastructure Interface Service enables communication through the Integrated Lights-Out Management Component to the rack infrastructure.

HP Lights-Out Drivers and Agents (hprsm)

The HP Lights-Out Drivers and Agents package contains the following drivers and agents:

- Remote Insight Driver (cpqrid)
- iLO Management Interface Driver (cpqci)
- Remote Insight/Integrated Lights-Out Agent (cmasm2d)
- Rack Agent (cmarackd)
- Rack Infrastructure Interface Service (cpqriisd)
- Compaq BL Rack Upgrade utility (cpqblru)

Note: These modules route data from the OS to the iLO interface. For instance the Remote Insight Driver (cpqrid) enables the routing of SNMP traffic out of the Remote Insight Lights-Out Edition and Remote Insight Lights-Out Edition II adapters. These

adapters are equipped with an integrated network interface card (NIC) that is used to manage the card through its Web interface or through Systems Insight Manager. These drivers are not supported on SecurePlatform.

NIC Agents

The NIC Agents collect information from network interface controllers at periodic intervals, make the collected data available to the UCD SNMP agent, and provide SNMP alerts. The NIC Agents gather data for the NIC MIB from NIC device drivers supporting the /proc file system reporting format. 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.

The HP System Health Application and Insight Management Agents

The HP System Health Application and Insight Management Agents included in the ProLiant Support Pack (hpsm) package collect and monitor important operational data on ProLiant servers. Contained within the hpsm package are the following:

- Health Monitor
- Integrated Management Log (IML) Viewer Application
- Foundation Agents
- Health Agent
- Standard Equipment Agent
- Server Peer Agent
- Storage Agents

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

The ProLiant Management Agents are included to provide proactive notification of server events through the HP Systems Insight Manager console. Some 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.

There are three binary modules that are bundled in the hpsm package. These will automatically be selected depending on the HP ProLiant Advanced System Management hardware available.

`/opt/compaq/hpasm/bin/hpasm`

The "hpasm" application will automatically load on HP ProLiant servers that have either the Advanced System Management (ASM) or the legacy Integrated Lights-Out (iLO) hardware.

Note: Early hpasm packages relied on a cpqasm.o health driver and required a build environment on non-standard Linux distributions. In August 2004 the health driver was converted to a user space application. The early packages that rely on the cpqasm.o health driver are not supported on SecurePlatform. Otherwise SecurePlatform supports the hpasm binary and iLO hardware.

`/opt/compaq/hpasm/bin/hpasmxld`

The "hpasmxld" application will automatically load on HP ProLiant servers that have Integrated Lights-Out 2 (iLO 2) management controller and the "hp-OpenIPMI" package is installed. The iLO 2 management controller contains an Intelligent Platform Interface (IPMI) version 2.0 Base Management Controller (BMC) that replaces the OS based software management functionality provided by the legacy "hpasm" 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 will be automatically selected by the hpasm initialization scripts (`/etc/init.d/hpasm` and `/opt/compaq/hpasm/etc/hpasm`) if the hp-OpenIPMI package is installed and the iLO 2 management controller is present. The corresponding hp-OpenIPMI package is available under catalog "Driver - System Management" and then click on "HP OpenIPMI Device Driver for Red Hat Enterprise Linux 3 (x86)" to download.

Note: The SecurePlatform kernel is not a standard Linux kernel and does not include a build environment so installation of the above hp-OpenIPMI package is not supported.

`/opt/compaq/hpasm/bin/hpasmlited`

The "hpasmlited" application will automatically load on HP ProLiant servers that have the Integrated Lights-Out 2 (iLO 2) management controller and the "hp-OpenIPMI" package is 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.

Note: Check Point products running on a SecurePlatform 2.4 kernel include an ipmi_kcs_drv.o module, but not the ipmi_si_drv.o module. SecurePlatform 2.6 includes the ipmi_si.ko module. Modified OpenIPMI init scripts are included in the splat_hpsm_support_files.tgz that enables the hpsm hpsmlited binary to work with these modules.

To determine if your server has an iLO 2 management controller see the [support matrix](http://h18013.www1.hp.com/products/servers/management/remotemgmt/supported-servers.html).
<http://h18013.www1.hp.com/products/servers/management/remotemgmt/supported-servers.html>

Peer Agents

The Peer Agents extend the SNMP "enterprise" Management Information Base (MIB) to include Foundation and Server MIB data. The Peer Agents support SNMP get, set, and trap operations on data items defined in the Host and Threshold MIBs. At SNMP agent startup, the Host and Threshold MIBs in /opt/compaq/foundation/etc/cmafdtnobjects.conf are read by cmaX and registered with the SNMP agent. The Health, Standard Equipment, and Remote Insight MIBs in the file /opt/compaq/server/etc/cmasvobjects.conf are also read by cmaX and registered with the SNMP agent. During installation, each agent is configured to start automatically after SNMP Agent (snmpd) is started and to stop after snmpd is stopped.

Data Collection Agents

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

Host OS Agent

The Host OS Agent gathers data for the Host OS MIB, including:

- Server/host name and operating system version number
- Processor utilization information (for each processor) over 1-minute, 5-minute, 30-minute, and 60-minute intervals
- Linux file system information (for each mounted file system)
- Software version information

The Host OS Agent executable is /opt/compaq/foundation/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/compaq/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/compaq/foundation/bin/cmthreshd.

System Management Homepage

The System Management HomePage runs as a daemon and converts SNMP information into HTML format so that it can be viewed from a Web browser. The Web Agent provides Web pages containing management information about HP servers. The Web Agent allows users to view subsystem and status information of HP servers from a Web browser, either locally or remotely.

The System Management Homepage is a separate optional package (hpsm) controlled by /etc/init.d/hpsmhd.

Standard Equipment Agent

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/compaq/server/bin/cmastdeq.

System Health Agent

The System Health Agent gathers data for the Health MIB. The data collected include 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/compaq/server/bin/cmahealthd.

Storage Data Collection Agents

The Storage Agents collect information from Fibre Channel, drive array, SCSI, and IDE subsystems at periodic intervals, make the collected data available to the UCD SNMP agent, and provide 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.

Event daemon

The Event Daemon gathers storage hardware events from firmware and passes them on to other agents upon request.

IDA Agent

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/compaq/storage/bin/cmidad`.

FCA Agent

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/compaq/storage/bin/cmafcad`.

IDE Agent

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/compaq/storage/bin/cmaided`.

SCSI Agent

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/compaq/storage/bin/cmascsid`.

Note: An additional library file is needed for the storage agents to run on SecurePlatform. See the configuration section below.

Test Configuration

Check Point Software

- SecurePlatform 2.6 VPN-1 NGX R65
- SecurePlatform VPN-1 NGX R65
- SecurePlatform VPN-1 NGX R62
- SecurePlatform VPN-1 NGX R61
- SecurePlatform VPN-1 NGX R60 HFA_03
- SecurePlatform Connectra R62
- SecurePlatform Provider-1 R65

HP Software

- Insight Manager v5.3 on Windows 2003 SP1
- hpsasm-7.8.0-97.rhel3.i386.rpm
- cmanic-7.7.0-5.rhel3.linux.rpm
- hpsmh-2.1.8-177.linux.i386.rpm

Hardware Tested

HP DL360 G3

- 2 Xeon 3.6 GHz CPUs
- 4 GB RAM
- 2 Intel 82541GI Gigabit NICs
- Perc 4e/Si Storage Controller
- 2 Seagate ST373207LC SCSI 68 GB HDD (configured in a RAID 1 array)
- Integrated Lights-Out iLO - lspci -nm output:
 - 00:05.0 "Class 0880" "0e11" "b203" -r01 "b203" "b206"
 - 00:05.2 "Class 0880" "0e11" "b204" -r01 "b204" "b206"

HP DL320 G5

- 1 Celeron 3.2 GHz
- 1 GB RAM
- 1 HP NC324i Integrated PCIe Dual Port Gigabit Server Adapter
- P400 SmartArray Controller
- 2 68 GB SAS DF072ABAA8 HDDs (configured in a RAID 1 array)
- Integrated Lights-Out 2 iLO 2 - lspci -nm output
 - 01:04.0 "Class 0880" "0e11" "b203" -r03 "b203" "3305"
 - 01:04.2 "Class 0880" "0e11" "b204" -r03 "b204" "3305"
 - 01:04.4 "Class 0c03" "103c" "3300" "3300" "3305"
 - 01:04.6 "Class 0c07" "103c" "3302" -p01 "3302" "3305"

Note: Testing of every hardware configuration is beyond the scope of this document. Consult the HP supported servers matrix and the readme for specific hardware and software requirements.

Managed System Requirements

- Firewall rules
 - src Insight Manager host, dst SecurePlatform, UDP 161 (SNMP)
 - src Insight Manager host, dst SecurePlatform, ICMP
 - src SecurePlatform, dst Insight Manager host, UDP 162 (SNMP trap)
 - src Insight Manager host, dst SecurePlatform, TCP 2381 (System Management Homepage https - optional)
 - src Insight Manager host, dst SecurePlatform, TCP 2301 (System Management Homepage http - optional)
- SNMP configuration
- Additional library for the storage agents and init scripts for IPMI for iLO 2 hardware included in splat_hpsm_support_files.tgz available at <http://www.opsec.com/solutions/partners/hpsm.html>

Installation

Prerequisites

Determine if your server includes an iLO 2 management controller. See the [support matrix](#) at; <http://h18013.www1.hp.com/products/servers/management/remotemgmt/supported-servers.html>

Note: Systems with iLO 2 support will need the init scripts included in the splat_hpsm_support_files.tgz support files.

Download the latest Red Hat EL 3 hpsm (System Health Application and Insight Management Agents), cmanic (HP NIC agent), and the optional hpsmh (System Management Homepage) packages from www.hp.com for your hardware.

Download the splat_hpsm_support_files.tgz support files from <http://www.opsec.com/solutions/partners/hpsm.html>

Installing System Management Homepage (optional)

Login as expert on the SecurePlatform managed system and create the /etc/redhat-release file with the following contents.

```
[Expert@opsec-81]# echo "Red Hat Enterprise Linux ES release 3 (Taroon)" >
/etc/redhat-release
[Expert@opsec-81]# cat /etc/redhat-release
Red Hat Enterprise Linux ES release 3 (Taroon)
```

Install the hpsmh package.

```
[Expert@opsec-81]# rpm -ivh hpsmh-2.1.-177.linux.i386.rpm
Preparing... ##### [100%]
Detected Red Hat Enterprise Linux AS/ES/WS 3
Creating hpsmh user and group...
 1:hpsmh ##### [100%]

*****
* System Management Homepage installed successfully with *
* default configuration values. To change the default *
* configuration values, type the following command at *
* the root prompt: *
* * *
* perl /usr/local/hp/hpSMHSetup.pl *
* * *
*****

Stopping hpsmhd:
Starting hpsmhd:
```

Note: SecurePlatform does not support changing the configuration values using perl.

Note: If you install hpsmh after installing hpasm, then the uid and gid of some files may not be correct. HP recommends running "/etc/init.d/hpasm reconfigure" in this case.

Installing Support Files for HPASM

Copy the splat_hpasm_support_files.tgz to the SecurePlatform system and extract the files in the package.

```
[Expert@opsec-81]# tar xzvf splat_hpasm_support_files.tgz splat_hpasm
splat_hpasm/
splat_hpasm/libstdc++-3-libc6.2-2-2.10.0.so
splat_hpasm/init_scripts/
splat_hpasm/init_scripts/2.4_init_ipmi
splat_hpasm/init_scripts/sysconfig_ipmi
splat_hpasm/init_scripts/2.6_init_ipmi
```

Custom OpenIPMI init Scripts

If your system has an iLO 2 management controller, then copy the IPMI sysconfig file to the /etc/sysconfig directory. Ensure that is named ipmi.

```
[Expert@opsec-81]# cp splat_hpasm/init_scripts/sysconfig_ipmi
/etc/sysconfig/ipmi
```

Copy the IPMI init script that matches the SecurePlatform kernel to the /etc/init.d directory. Here is an example from SecurePlatform 2.4 install. Ensure that is renamed to ipmi.

```
[Expert@opsec-81]# uname -r
2.4.21-21cp
[Expert@opsec-81]# cp splat_hpasm/init_scripts/2.4_init_ipmi /etc/init.d/ipmi
```

Additional Library for Storage Agents

The Foundation and Server agents of hpasm function without any additional configuration, but the Storage agents requires an additional lib file that is not included in SecurePlatform. This is from the compat-libstdc++-8-3.3.4.2.i386.rpm package.

Copy the libstdc++-3-libc6.2-2-2.10.0.so file to /usr/lib and set up a link libstdc++-libc6.2-2.so.3.

```
[Expert@opsec-81]# cp libstdc++-3-libc6.2-2-2.10.0.so /usr/lib
[Expert@opsec-81]# cd /usr/lib
[Expert@opsec-81]# ln -s libstdc++-3-libc6.2-2-2.10.0.so libstdc++-libc6.2-
2.so.3
[Expert@opsec-81]# chmod 755 libstdc++-3-libc6.2-2-2.10.0.so
```

Configure SNMP

The net-snmp agent on SecurePlatform is installed, but disabled by default. Enable it using the SecurePlatform “snmp service enable” command.

```
[Expert@opsec-81]# snmp service enable
Starting snmpd: [ OK ]
```

Install HPASM

Download the hpasm and cmanic RPMs to a directory on your hard drive and change to that directory.

If a previous version of the Health Driver or Insight Management agents has been installed, they must be removed before this package can be installed. Any packages dependent on the Health Driver must also be removed. To check which version of the Health Driver (if any) is on the system, type:

`rpm -q hpasm`

The `rpm -q` command may also be used to check for the existence of dependent packages. There is no need to uninstall packages that are not present on the system.

To remove the previous version and any packages dependent on it, type the following, in order:

- `rpm -e hponcfg` (if installed)
- `rpm -e cmanic` (if installed)
- `rpm -e hprsm`
- `rpm -e hpasm`

To install the `hpasm` package, type:

`rpm -ivh hpasm-< version >.rpm`

```
[Expert@opsec-81]# rpm -ivh hpasm-7.8.0-97.rhel3.i386.rpm
Preparing...
Please read the Licence Agreement for this software at

    /opt/compaq/hpasm/hpasm.license

By not removing this package, you are accepting the terms of the "License for
HP Value Added Software".
=====
NOTE: In order to activate the software contained in this package, you must
type 'hpasm activate' as 'root' user.
You may subsequently reset your agent configuration by typing
'/etc/init.d/hpasm configure' or '/etc/init.d/hpasm reconfigure'.
=====
The hpasm RPM has installed successfully.
```

The NIC Agents must be downloaded and installed separately.

```
[Expert@opsec-81]# rpm -ivh cmanic-7.7.0-5.rhel3.linux.rpm
Preparing...                               ##### [100%]
 1:cmanic                                   ##### [100%]
cmanic installation: snmpd Start script is detected at runlevels
cmanic installation: cmanic Start script is installed at runlevels 2 3 4 5
```

Running the health driver: Once installed, the health driver will be automatically loaded every time the server boots. Several `/proc` entries are available when the driver is running.

Additional information and help is available at;
[Managing ProLiant Servers With Linux](#)

Configuration

After the installation process, type `hpasm activate` to configure and activate the agents. Provide basic Simple Network Protocol (SNMP) information, when prompted. This modifies `/etc/snmp/snmpd.conf` and `/opt/compaq/cma.conf`. You may subsequently reset your agent configuration by typing;

```
/etc/init.d/hpasm configure' or '/etc/init.d/hpasm reconfigure'
```

First Time Configuration

```
[Expert@secureplatform]# hpasm activate
```

```
Welcome to the hp System Health Application and Insight Management
Agent(hpasm) package installation. This package contains the hp Advanced
Server Management Application(hpasmd) and hp's SNMP agents. This package is
intended to only function on hp servers with either the ProLiant ASM
(0x0E11A0F2) ASIC or the ProLiant iLO Advanced Server Management (0x0E11B203)
ASIC.
```

```
Do you wish to continue? <y/n> (blank is y) y
```

```
=====
NOTE: Your SNMP stack can load the 32-bit hp ProLiant Management Extension.
      Problems may result from using your distribution's SNMP stack.
      See hp Documentation (HOWTO, agent manual) for more details.
=====
```

```
Press any key to continue...<press Enter>
```

```
The startup scripts in this package also control the loading of modules in
this and other hp management packages(i.e. hprsm). Some of those management
modules are distributed under a non-GPL license. When these non-GPLed modules
are loaded the kernel's tainted flag (see /proc/sys/kernel/tainted) may be
set. If you choose not to load them, some management functionality will be
lost.
```

```
Do you want to load the hp modules even though they may "taint" your kernel?
<y/n> (Blank is y) n
```

(Note: The hprsm package is not supported on SecurePlatform.)

```
This package contains data gathering agents that provide data to clients via
SNMP. This SNMP data may be used by other hp management software. If you
```

choose not to start these agents that data may not be provided. Answer 'y' to this question to start the base set of agents. You will be prompted for the more specialized Storage and Performance agents.

Agent Startup Policy

Do you require SNMP agents (y/n) ? (Blank is y): **y**

Storage Agent Startup Policy

Do you require Storage Agent support (y/n) ? (Blank is y): **y**

Performance Agent Startup Policy

Do you require performance agent support (y/n) ? (Blank is y): **y**

This configuration script will configure SNMP to integrate with the HP SIM and the HP System Management Homepage. The HPASM can also exist in a more secure SNMP environment (e.g. VACM) that you have previously configured. See the hpasm(4) man page for specific details on how to configure the VACM entries in the 'snmpd.conf' file. You may press <ctrl+c> now to exit now if needed.

Do you wish to use an existing snmpd.conf (y/n) (Blank is n): **n**

Enter the localhost SNMP Read/Write community string

(one word, required, no default): *********

Re-enter the same input to confirm: *********

ACCEPTED: inputs match!

Enter localhost SNMP Read Only community string

(one word, Blank to skip): *********

Re-enter the same input to confirm: *********

ACCEPTED: inputs match!

Enter Read/Write Authorized Management Station IP or DNS name

(Blank to skip): **10.133.2.150**

Enter SNMP Read/Write community string for Management Station "10.133.2.150"

(one word, required, no default): *********

Re-enter the same input to confirm: *********

ACCEPTED: inputs match!

Enter Read Only Authorized Management Station IP or DNS name (Blank to skip):

10.133.2.150

Enter SNMP Read Only community string for Management Station "10.133.2.150"

(one word, required, no default): *********

Re-enter the same input to confirm: *********

ACCEPTED: inputs match!

Enter default SNMP trap community string

(One word; Blank to skip):

Enter SNMP trap destination IP or DNS name

(One word; Blank to skip): **10.133.2.150**

Enter trap community string for trap destination "10.133.2.150"

```
(One word; Blank to skip):
Enter system contact information
(Name, phone, room, etc; Blank to skip): Manager@example.com
Enter system location information
(Building, room, etc; Blank to skip): A-bldg, rm-111
```

This configuration script will add user 'hpsmh' and group 'hpsmh' to integrate with the HP SIM and the HP System Management Homepage (hpsmh). The default selection is to enable hpsmh support.

```
Do you wish to disable hpsmh support (y/n) (Blank is n): n
```

```
=====
NOTE: New cma.conf entries were added to the top of /opt/compaq/cma.conf
=====
```

```
The hpsmh group already exists...doing nothing
The hpsmh user already exists...doing nothing
Changing Owner and Group of '/opt/hp/hpsmh/data' to 'hpsmh:hpsmh' ...
Going to apply the permissions...
```

```
=====
NOTE: New snmpd.conf entries were added to the top of /etc/snmp/snmpd.conf
=====
```

```
Starting HP Server Management Drivers and Agents, please wait ...
/lib/modules/2.4.21-21cp/kernel/drivers/char/ipmi/ipmi_si_drv.o:
/lib/modules/2.4.21-21cp/kernel/drivers/char/ipmi/ipmi_si_drv.o: No such file
or directory
```

Note: If this is SecurePlatform 2.4 on a system with an iLO 2 controller there is an error about the missing ipmi_si_drv.o, but hpsmslited runs and connects to the ipmi_kcs_drv.o module.

Note: The default trapemail setting in /opt/compaq/cma.conf is set to send emails, but the mail package isn't supported on SecurePlatform.

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

This can be changed to send the logs to /var/log/messages. Change "/bin/mail" to /usr/bin/logger" or use the Check Point sendmail binary, "/opt/CPsuite-R60/fw1/bin/sendmail". The location may be different depending upon the Check Point product installed. If you choose to use sendmail, then cd to the /opt/compaq/hpasm/etc directory and edit the hpasm file. Change;

```
unset LD_LIBRARY_PATH
```

```
to;
```

```
# unset LD_LIBRARY_PATH
```

and restart hpsasm. Otherwise the trapemail command fails with the error “/opt/CPsuite-R65/fw1/bin/sendmail: error while loading shared libraries: libcprod50.so: cannot open shared object file: No such file or directory”.

SNMP Changes

After configuring hpsasm the /etc/snmp/snmpd.conf is modified and /etc/snmp/snmpd.users.conf is renamed to /etc/snmp/snmpd.users.conf.bak. The SecurePlatform snmp command writes to /etc/snmp/snmpd.users.conf. If you wish to use the SecurePlatform snmp command copy snmpd.users.conf.bak to snmpd.users.conf and modify /etc/snmp/snmpd.conf so that the rocommunity entries don't conflict. The SecurePlatform snmp command only supports read-only entries.

Here is an example of the additions to /etc/snmpd.conf.

```
# Following entries were added by HP Insight Management Agents at
#      Fri May  5 11:37:12 GMT-7 2008
dlmod cmaX /usr/lib/libcmaX.so
rwcommunity private 127.0.0.1
rocommunity public 127.0.0.1
rwcommunity private 10.133.2.150
rocommunity public 10.133.2.150
trapcommunity
trapsink 10.133.2.150
# ----- END -----
```

SNMP Considerations

The above configuration enables write access. This is a change from the default Check Point net-snmp configuration which doesn't allow write access. The default limits some functionality, i.e. clearing the IML log, specifying a reboot, changing the polling cycle, etc. It is possible to limit the SNMP agent to respond to "localhost" writes which is all the Insight agents require (as they are running locally).

HP agents require that snmpd be enabled for interprocess communication between the agents. This can be set using the following configuration.

```
rwcommunity private 127.0.0.1
rocommunity public 127.0.0.1
```

Then you could allow only snmp-read requests to the HP System Insight Manager server. For example;

rocommunity public 10.133.2.150

Testing the Configuration

Check the Status of hpasm

Without an iLO Controller

```
[Expert@secureplatform]# /etc/init.d/hpasm status
hpasmd is running...
Status of Foundation Agents (cmafdtn): cmathreshd cmahostd cmapeerd
cmathreshd is running...
cmahostd is running...
cmapeerd is running...
Status of Server Agents (cmasvr): cmastdeqd cmahealthd cmaperfd
cmastdeqd is running...
cmahealthd is running...
cmaperfd is running...
Status of Storage Agents (cmastor): cmaeventd cmaidad cmafcad cmaided
cmascsid cmasasd
cmaeventd is running...
cmaidad is running...
cmafcad is running...
cmaided is running...
cmascsid is running...
cmasasd is stopped...
```

With an iLO 2 Controller on SecurePlatform 2.4

Note: There is an error about the missing ipmi_si_drv.o, but hpasm-lite runs and connects to the ipmi_kcs_drv.o module.

```
[Expert@opsec-81]# /etc/init.d/hpasm status
/lib/modules/2.4.21-21cp/kernel/drivers/char/ipmi/ipmi_si_drv.o:
/lib/modules/2.4.21-21cp/kernel/drivers/char/ipmi/ipmi_si_drv.o: No such file
or directory
    Using standard Linux IPMI device driver and hpasm-lite

ipmi_msghandler module loaded.
ipmi_kcs_drv module loaded.
ipmi_devintf module loaded.
/dev/ipmi0 exists.

    hpasm-lite is running...
Status of Foundation Agents (cmafdtn): cmathreshd cmahostd cmapeerd
```

```
cmathreshd is running...
cmahostd is running...
cmapeerd is running...
Status of Server Agents (cmasvr): cmastdeqd cmahealthd cmaperfd
cmastdeqd is running...
cmahealthd is running...
cmaperfd is running...
Status of Storage Agents (cmastor): cmaeventd cmaidad cmafcad cmaided
cmascsid cmasasd
cmaeventd is running...
cmaidad is running...
cmafcad is running...
cmaided is running...
cmascsid is running...
cmasasd is stopped...
```

With an iLO 2 Controller on SecurePlatform 2.6

```
[Expert@opsec-81]# /etc/init.d/hpasm status
```

```
Using standard Linux IPMI device driver and hpasm-lite
```

```
ipmi_msghandler module loaded.
ipmi_si module loaded.
ipmi_devintf module loaded.
/dev/ipmil exists.
```

```
hpasmlited is started...
Status of Foundation Agents (cmafdtn): cmathreshd cmahostd cmapeerd
cmathreshd is running...
cmahostd is running...
cmapeerd is running...
Status of Server Agents (cmasvr): cmastdeqd cmahealthd cmaperfd
cmastdeqd is running...
cmahealthd is stopped...
cmaperfd is running...
Status of Storage Agents (cmastor): cmaeventd cmaidad cmafcad cmaided
cmascsid cmasasd
cmaeventd is running...
cmaidad is running...
cmafcad is running...
cmaided is running...
cmascsid is running...
cmasasd is stopped...
```

Note: In my test configuration cmaeventd ran normally until the P400 firmware was updated to version 4.12. This also occurs on the same hardware with RHEL 3 update 8 and the same hpasm agents installed so it doesn't seem to be an issue specific to SecurePlatform.

Insight Manager Considerations

Insight Manager includes the ability to execute commands remotely via a secure ssh connection, e.g. ls or ps. This requires that the key be exchanged using the mxagentconfig utility or using Repair Agents in Insight Manager.

Note: This may be because SecurePlatform doesn't support a sftp-server connections to exchange the key. More investigation needs to be done if this is feature is needed.

Connecting to the System Management Homepage

If the hpsmh package is installed connect to <http://<secureplatform>:2301> or <https://<secureplatform>:2381>. Login using a SecurePlatform Web Administrator username and password and ensure that the system data is being polled correctly.

The following limitations exist.

- Home -> System -> System Info identifies the Operating System as Linux - Oracle rather than SecurePlatform.
- Modifying the SecurePlatform SNMP settings via Settings -> SNMP Webagent ->SNMP Configuration is not supported.
- Generation of a local server certificate via Settings -> System Management Homepage -> Security ->Local Server Certificate is not supported.
- Limiting user access via Settings -> System Management Homepage -> Security ->User Groups is not supported.

hp System Management Homepage for opsec-81 System Model: **ProLiant DL320 G5**
[Support](#) | [Forums](#) | [Help](#) Current User: **admin**
[logout](#)

Home **Settings** Tasks Logs

home

Integrated Agents
[HP Foundation Agent](#)
[HP Server Agent](#)
[HP Storage Agent](#)
[HP NIC Agent](#)

Other Agents
 none

Management Processor
 none

Other Software
[HP Essentials Software](#)

KEY: ✓ OK
 ⚠ Degraded
 ✖ Failed
 ? Unknown

Thursday, May 08, 2008 3:33:02 PM
[refresh](#): manual

Overall System Status

▼ [Logs -> Integrated Management Log](#)

✓ **NIC**

- ✓ [HP NC324i Integrated PCIe Dual Port Gigabit Server Adapter Mem FDDD0000 Port 2](#)
- ✓ [HP NC324i Integrated PCIe Dual Port Gigabit Server Adapter Mem FDDF0000 Port 1](#)
- ? [Virtual interface 1](#)

✓ **Recovery**

- ✓ [Autorecovery](#)
- ✓ [Environment](#)
- ? [Power Supply](#)

✓ **Storage**

- ✓ [File System Space Used](#)
- ✓ [Smart Array P400 Controller in Slot 1](#)
- ✓ [Standard IDE Controller on System Board](#)

✓ **System** [Utilization](#)

Troubleshooting Problems

For problems with the hpsasm agents check the cma.log and hpsasm.log files in the /var/spool/compaq directory.

For problems with the hpsmh package check log files in the /var/spool/opt/hp/hpsmh/logs/ directory.

Trademarks and Copyrights

TRADEMARKS:

©2003-2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, the Check Point logo, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, Integrity, OPSEC, Provider-1, SecureKnowledge, SecurePlatform, SmartCenter, SmartConsole, SmartDashboard, SmartUpdate, SmartView, SmartView Monitor, VPN-1, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications. For third party notices, see: THIRD PARTY TRADEMARKS AND COPYRIGHTS.

THIRD PARTY TRADEMARKS AND COPYRIGHTS

Trademarks used in this text: *HP*, *ProLiant*, and *OpenView* are trademarks of HP; *Red Hat* and *Red Hat Enterprise Linux* are registered trademarks of Red Hat, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products.