HP Operations Manager on Linux

Administrator's Reference

Software Version: 9.01

for the Red Hat Enterprise Linux operating system

Manufacturing Part Number: None

Date: September, 2009

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

Trademark Notices.

Adobe® is a trademark of Adobe Systems Incorporated.

Intel®, Itanium®, and Pentium® are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Contents

Contents

Contents

C. HPOM Audits

D. Reference Pages

Printing History

The printing date and part number of the manual indicate the edition of the manual. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The part number of the manual will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

Edition	Publish Date
First	September 2009

Conventions

The following typographical conventions are used in this manual:

Table 1 Typographical Conventions

Font	Meaning	Example
Italic	Book titles and names of reference pages	Refer to the *HPOM Administrator's Reference* and the *opc(1M)* reference page for more information.
	Emphasis	You *must* follow these steps.
	Variable that you must supply when entering a command	At the prompt, enter **`rlogin`** ***`username`***.
	Parameters to a function	The *`oper_name`* parameter returns an integer response.
Bold	New terms	The **HTTPS agent** tracks...
`Computer`	Text and other items on the computer screen	The following system message displays: `Are you sure you want to remove current group?`
	Command names	Use the `grep` command ...
	Function names	Use the `opc_connect()` function to connect...
	File and directory names	`/opt/OV/bin/OpC/`
	Process names	Check to see if `opcmona` is running.
	Window names	In the `Add Logfile` window...
	Menu name followed by a colon (`:`) means that you select the menu, then the item. When the item is followed by an arrow (`->`), a cascading menu follows.	Select `Actions: Filtering -> All Active Messages` from the menu bar.

Table 1 Typographical Conventions (Continued)

Font	Meaning	Example
`Computer Bold`	Text that you enter	At the prompt, enter **`ls -l`**
Keycap	Keyboard keys	Press **Return**.
`[Button]`	Buttons in the user interface	Click `[OK]`.

Documentation Map

HP Operations Manager (HPOM) provides a set of manuals and online help that help you to use the product and to understand the concepts underlying the product. This section describes what information is available and where you can find it.

Electronic Versions of the Manuals

All the manuals are available as Adobe Portable Document Format (PDF) files in the documentation directory on the HPOM product CD-ROM.

With the exception of the *HPOM Software Release Notes*, all the manuals are also available in the following HPOM web-server directory:

`http://<management_server>:3443/ITO_DOC/<lang>/manuals/*.pdf`

In this URL, <*management_server*> is the fully qualified hostname of your management server, and <*lang*> stands for your system language, for example, `C` for the English environment.

Alternatively, you can download the manuals from the following website:

`http://support.openview.hp.com/selfsolve/manuals`

Watch this website regularly for the latest edition of the *HPOM Software Release Notes*, which is updated every two to three months with the latest news (for example, additionally supported operating system versions, the latest patches and so on).

HPOM Manuals

This section provides an overview of the HPOM manuals and their contents.

Table 2 HPOM Manuals

Manual Title	Description	Media
HPOM Installation Guide for the Management Server	Designed for administrators who install HPOM software on the management server and perform the initial configuration. This manual describes the following: • Software and hardware requirements • Software installation and removal instructions • Configuration defaults	PDF only
HPOM Concepts Guide	Provides you with an understanding of HPOM on two levels. As an operator, you learn about the basic structure of HPOM. As an administrator, you gain an insight into the setup and configuration of HPOM in your own environment.	PDF only
HPOM Administrator's Reference	Designed for administrators who install HPOM on the managed nodes and are responsible for HPOM administration and troubleshooting. Contains conceptual and general information about the HPOM managed nodes.	PDF only
HPOM HTTPS Agent Concepts and Configuration Guide	Provides platform-specific information about each HTTPS-based managed node platform.	PDF only
HPOM Reporting and Database Schema	Provides a detailed description of the HPOM database tables, as well as examples for generating reports from the HPOM database.	PDF only
HPOM Java GUI Operator's Guide	Provides you with a detailed description of the HPOM Java-based operator GUI and the Service Navigator. This manual contains detailed information about general HPOM and Service Navigator concepts and tasks for HPOM operators, as well as reference and troubleshooting information.	PDF only

Table 2 HPOM Manuals (Continued)

Manual Title	Description	Media
Service Navigator Concepts and Configuration Guide	Provides information for administrators who are responsible for installing, configuring, maintaining, and troubleshooting the HP Operations Service Navigator. This manual also contains a high-level overview of the concepts behind service management.	PDF only
HPOM Software Release Notes	Describes new features and helps you: • Compare features of the current software with features of previous versions. • Determine system and software compatibility. • Solve known problems.	PDF only
HPOM Firewall Concepts and Configuration Guide	Designed for administrators. This manual describes the HPOM firewall concepts and provides instructions for configuring the secure environment.	PDF only
HPOM Web Services Integration Guide	Designed for administrators and operators. This manual describes the HPOM Web Services integration.	PDF only
HPOM Security Advisory	Designed for administrators. This manual describes the the HPOM security concepts and provides instructions for configuring the secure environment.	PDF only
HPOM Server Configuration Variables	Designed for administrators. This manual contains a list of the HPOM server configuration variables.	PDF only

Additional HPOM-Related Products

This section provides an overview of the HPOM-related manuals and their contents.

Table 3 Additional HPOM-Related Manuals

Manual	Description	Media
HP Operations Manager on Linux Developer's Toolkit If you purchase the HP Operations Manager on Linux Developer's Toolkit, you receive the full HPOM documentation set, as well as the following manuals:		
HPOM Application Integration Guide	Suggests several ways in which external applications can be integrated into HPOM.	PDF
HPOM Developer's Reference	Provides an overview of all the available application programming interfaces (APIs).	PDF

HPOM Online Information

The following information is available online.

Table 4 HPOM Online Information

Online Information	Description
HPOM Administrator GUI Online Help	The online help for the HPOM administrator GUI provides context-sensitive information about individual pages, menus, and options displayed in the administrator's graphical user interface. Menus and menu options differ according to the data context in which you are working. Start the HPOM administrator's user interface by entering the following URL in a supported Web browser: • Standard Connection: **`http://<hostname>:9662`** • Secure Connection: **`https://<hostname>:9663`**
HPOM Java GUI Online Information	HTML-based help system for the HPOM Java-based operator GUI and Service Navigator. This help system contains detailed information about general HPOM and Service Navigator concepts and tasks for HPOM operators, as well as reference and troubleshooting information.
HPOM reference pages	Reference pages available online for HPOM. Reference pages are also available in HTML format. To access these pages, enter the following location (URL) in your web browser: **`http://<management_server>:3443/ITO_MAN`** In this URL, the variable <*management_server*> is the fully qualified hostname of your management server. Note that the reference pages for the HP Operations HTTPS agents are installed on each managed node. For more information about the HPOM reference pages, see "Reference Pages" on page 517.

1 Agent Installation on HPOM Managed Nodes

In this Chapter

This chapter gives general instructions on how to install the HP Operations Manager (HPOM) agent software on the supported managed nodes. The information in this section covers the following topics:

❏ "Installation Requirements" on page 27

❏ "Installation Tips" on page 29

❏ "Automatic Installation or Update of HPOM Software" on page 35

❏ "Secure Shell Installation" on page 38

❏ "HPOM Software Removal on the Managed Node" on page 43

❏ "HPOM Agent Software Management" on page 44

❏ "Subagent Management in HPOM" on page 48

❏ "Debugging Software Installation and Removal on Managed Nodes" on page 52

The installation procedures assume that you have already installed and configured the database and HPOM on the management server, as described in the *HPOM Installation Guide for the Management Server*.

Installation Requirements

This section describes the operating system, hardware, and software requirements for installing HPOM agents on the managed nodes.

Operating System Requirements

For a detailed list of the specific versions of the various agent operating systems that are supported by HPOM, refer to the *HPOM Installation Guide for the Management Server*.

Hardware and Software Requirements

For details about the hardware and software requirements for each supported managed node platform, refer to the *HPOM Software Release Notes*.

Setting Kernel Parameters

Before installing HPOM on Linux, make sure the kernel parameters are set correctly. Although system default values are normally sufficient, the logfile encapsulator sometimes requires that the number of open files be increased.

Table 1-1 gives values for kernel parameters on HP-UX managed nodes. Other UNIX-based agent platforms generally require similar values.

NOTE For information about recommended kernel parameters for Solaris managed nodes, refer to the *HPOM Software Release Notes*.

Table 1-1 Important Kernel Parameters for Managed Nodes

Parameter	Description	Minimum Value
nfile	Maximum number of open files.	20 [a]
semmns	Required semaphores.	20

Table 1-1 Important Kernel Parameters for Managed Nodes (Continued)

Parameter	Description	Minimum Value
shmmax	Maximum shared memory.	None required.
msgmni	Message queues.	None required.
nflocks	File locks.	10

a. This number depends on several factors. Normally a value of 20 per process is sufficient. However, the more log files that are configured for the logfile encapsulator, the more file descriptors are needed. Normally, one logfile requires about one file descriptor. Any actions that result in processes being started on the managed node need additional file descriptors.

Communication Software

To communicate between the management server and the client nodes, HPOM uses the HTTPS mechanism.

HTTPS 1.1 based communication is the latest communication technology used for HP BTO Software products and allows applications to exchange data between heterogeneous systems. HTTP/SSL is the default communication type for new HPOM nodes.

Installation Tips

This section describes tips for installing HPOM agents on managed nodes, on the management server, and on UNIX managed nodes.

Installation on Managed Nodes

When installing on the managed nodes, follow these guidelines:

❏ Installation target:

Whenever possible, install the latest HPOM agent software version on all managed nodes. Installing the latest version enables the latest HPOM features to be used on those nodes.

❏ Node-name restrictions:

You may not use the names `bin`, `conf`, `distrib`, `unknown`, and `mgmt_sv` for managed nodes. These names are used internally by HPOM, and therefore may not be used as names of other systems.

❏ Host aliases:

Avoid using host aliases. Identical host aliases cause system problems.

❏ IP address:

Identify managed nodes having more than one IP address. Specify the most appropriate address (for example, the IP address of a fast network connection) in the HPOM configuration. Verify that all other IP addresses of that managed node are also identified on the management server. Otherwise, messages from multiple IP address systems might not be forwarded by HPOM.

❏ Disk space:

During installation on managed nodes, twice the amount of disk space normally required by HPOM is needed. This extra disk space is needed because the tape image is transferred to the managed node before it is uncompressed and unpacked.

If you do not have enough disk space for HPOM in your UNIX file system, apply one or both of the following solutions:

- Use a symbolic link.

For example, for Solaris, enter the following:

```
# ln -s /mt1/OV /opt/OV
```

- Mount a dedicated volume

❏ Long host names:

Use long host names in your policies only when performing automatic actions or operator-initiated actions.

❏ Operating system versions:

Do not upgrade or downgrade the operating system version of the management server or managed node to a version not supported by HPOM. For a list of supported operating system versions on the management server and on the managed nodes, see the *HPOM Installation Guide for the Management Server*.

You can also get a list of supported operating systems by running the following script on the management server:

```
# /opt/OV/bin/OpC/agtinstall/opcversion
```

❏ System time:

Verify that the system times of the management server and the managed nodes are synchronized. By synchronizing system times, you ensure that the time at which the message is generated on the managed node is earlier than the time at which the message is received on the management server.

❏ Passwords:

Before you install the HPOM agent software, make sure you know the root passwords for all the managed nodes on which you want to install the software.

On UNIX managed nodes, passwords are not required if an `.rhosts` entry exists for the root or if the management server is included in `/etc/hosts.equiv` (HP-UX 11.x, Solaris).

❏ Network paths:

There must be an existing route (network path) in both directions between the HPOM management server and the managed nodes.

- ❑ Software removal:

  If you want to move the HPOM management server from one host to another, you must first remove the HPOM managed node software from all managed nodes. See also “Hostnames and IP Addresses” on page 437 for more information.

- ❑ Default operator functionality:

  If you do not need the functionality of the HPOM default operator on your managed nodes (except for the management server), you can purge the related information. The purged information is recreated when you re-install the HPOM agent software.

  On UNIX managed nodes:

  - Erase the home directory of the user `opc_op`.
  - Remove the `opc_op` entry from `/etc/passwd`.
  - Remove the `opcgrp` entry from `/etc/group`.

NOTE You should not remove the HPOM default operator from Windows managed nodes because the agents run under the operator’s account.

- ❑ Program management with `opcmsg` APIs:

  When you upgrade or re-install HPOM software on managed nodes, make sure that all programs and applications that use the `opcmsg(3)` or `opcmon(3)` API are stopped.

  These APIs as well as other APIs are stored in the HPOM shared library, which is overwritten during HPOM software upgrade or reinstallation. For more information, see the *HPOM Developer’s Reference*.

Installation on the Management Server

When installing on the management server, follow these guidelines:

❑ Distribution directory:

If you want to stop the configuration and script or program distribution (for example, if the configuration is invalid), clean the `distrib` directory:

```
# /var/opt/OV/share/tmp/OpC/distrib
```

Clean the `distrib` directory only in an emergency and only after the HP Operations management server processes have been stopped.

❑ Installation or removal:

Avoid interrupting the software installation or removal process on managed nodes. Interrupting either process causes a semaphore file to be left on the management server. As a result, you will not be able to re-invoke the installation.

If a semaphore file is created on the management server, remove the file manually by entering:

```
# /var/opt/OV/share/tmp/OpC/mgmt_sv/inst.lock
```

If you interrupt the software installation or removal on the managed nodes at the time you are asked for a password, your terminal settings will be corrupted, and any commands that you type will not be echoed in the terminal.

If your terminal settings are corrupted, you can reset the terminal by entering the following:

```
# stty echo
```

❑ Management-server software:

If any managed node is still configured and has the HPOM bits, do not remove any of the management server software bundles from the management server, for example: `OVOPC-ORA` or `OVOPC`.

❑ Tape image:

If another managed node of the type you are de-installing is still configured and has the HPOM agent software installed, do not remove the managed node tape images (for example `OVOPC-CLT-ENG`) from the management server. If you remove the tape image, you will be unable to remove the HPOM agent software from the managed node.

UNIX Installations

When installing on UNIX managed nodes, follow these general guidelines:

❏ Short system name:

Make sure that `uname(1M)` (HP-UX) or `uname(1)`(Solaris) returns the short system name.

❏ Fully qualified system name:

Configure the name service (`/etc/hosts` or DNS) so *all* name-service operations (for example, `nslookup`) are consistently resolved to the fully qualified system name. For example, `hostname` is not name-service related and may return the short hostname.

❏ Log directory:

Removal of HPOM deletes any non-default log directory on UNIX systems. The following rules apply to the *default* log directory:

- Managed nodes:

  Do not use the same logging directory for more than one managed node. Using the same log directory for multiple managed nodes can cause problems if the directory is NFS-mounted across several systems.

- Other applications:

  Do not use the same log directory for *both* HPOM *and* other applications.

- Subdirectories:

  Do not create subdirectories other than the HPOM log directory for use by other applications or managed nodes.

❏ Security file:

Make sure that the security file for `inetd` on the managed nodes allows `remshd` or `ftpd` for the management server. For example, for HP-UX 11.x, use the following:

`/var/adm/inetd.sec`

- ❏ Root user:

  If no `.rhosts` entry for `root` and no `/etc/hosts.equiv` entry for the management server are available, make sure the `root` is *not* registered in `/etc/ftpusers` on the managed node.

- ❏ User IDs and group IDs:

  For consistency, make sure that the user ID and group ID are identical on all your managed nodes.

- ❏ NIS clients:

  If the managed node is a Network Information Service (NIS or NIS+) client, you must add the HPOM default operator `opc_op` on the NIS server before installing the HPOM software on a managed node. By doing so, you ensure that the HPOM default operator `opc_op` is used by HPOM and is consistent on all systems. Make sure that you adapt the user registration of adapted system resources accordingly.

Automatic Installation or Update of HPOM Software

This section describes how to install or update HPOM software automatically by using the installation script.

Before You Begin

Before you install or update HPOM, you need to understand how to work with the installation script, root passwords, and managed nodes.

Installation Scripts

When you install, update, or remove HPOM software, you use the `inst.sh(1M)` script. If the connection between management server and managed node is lost during installation or upgrade of the HPOM agent software upgrade, the `inst.sh` script tries to reconnect automatically to the agent and returns an error if it fails.

By default, `inst.sh(1M)` uses ping to send 64-byte ICMP packets when installing the agent. If you are installing the agent through a firewall that does not allow 64-byte ICMP packets, reduce the packet size before installing the agent, for example:

```
# ovconfchg -ovrg server -ns opc -set OPC_PING_SIZE 56
```

To avoid the verbose output produced by the `ovconfchg` script, set a shell variable for user `root`, as follows:

Bourne/Korn	**`OPC_SILENT=1; export OPC_SILENT`**
C	**`setenv OPC_SILENT`**

Root Passwords

Before you can begin software maintenance, you need to know either the root passwords of the managed nodes, or you must make `.rhosts` entries available for user root (UNIX only). Failing that, make sure the local `/etc/hosts.equiv` (on the UNIX managed nodes) contains an entry for the management server.

Managed Nodes

Before installing or removing HPOM software on the managed nodes, read the section "Installation Tips" on page 29.

IMPORTANT Make sure you have either REXEC, RSH, or SSH services enabled on the remote agent before you start the HPOM agent installation. Otherwise the agent installation will fail.

Adding a Managed Node to the HPOM Database

NOTE Make sure that the SNMP agent is running before adding a managed node to the HPOM database.

Before you can install HPOM on a managed node, you must add the managed node by using the opcnode command line tool, for example:

```
# opcnode -add_node node_name=<node_name> \
net_type=<network_type> mach_type=<machine_type> \
group_name=<group_name> node_type=<node_type>
```

For detailed information, refer to the *opcnode(1m)* reference page.

Automatic Software Installation and Update

NOTE HPOM agent software installation does not include configuration distribution.

To install or update the HPOM software automatically, use the inst.sh script. The installation script inst.sh(1M) verifies that all specified systems are reachable and accessible by the super user. If the connection between management server and managed node is lost during the installation or upgrade of the HPOM agent software, the inst.sh script tries to reconnect automatically to the agent and returns an error if it fails.

Watch the script execution carefully. Your interaction might be required if any errors or warnings occur. For example, if a password is required, the script prompts you to supply one before continuing the installation process. When the script is finished, verify the overall result of the script run.

Check the local (managed node) installation logfile for any problems.

If you could not review the installation process in a terminal window), check the following logfile on the management server for errors or warnings:

`/var/opt/OV/log/OpC/mgmt_sv/install.log`

Secure Shell Installation

This section describes how to use Secure Shell (SSH) software for installing HPOM agent software on managed nodes.

The SSH installation method provides enhanced security for installations that are performed over insecure lines (for example, over the Internet).

NOTE

HPOM does *not* provide the SSH software. If you want to use SSH for the HPOM agent installation, you must first install and configure the SSH software on the management server and the managed node.

There are two SSH protocol versions available: **SSHv1** and **SSHv2**. The HPOM agent installation uses whichever version of the SSH protocol that is available on the management server and the managed node.

Hardware and Software Requirements

This section describes the hardware and software requirements for installing HPOM agents on the managed nodes using the SSH installation method.

See the *HPOM Installation Guide for the Management Server* for a list of managed node platforms and operating system versions on which the SSH installation method is supported.

Hardware Requirements

For details about the hardware requirements for each supported managed node platform, see the *HPOM Software Release Notes*.

Software Requirements

❑ Basic software requirements:

- Management server:

  Check the software requirements listed in the *HPOM Installation Guide for the Management Server*.

- Managed nodes:

  Check the software requirements for the HPOM managed node listed in the *HPOM Software Release Notes*.

❏ Communication:

Make sure that the SSH client and server (daemon) is installed and fully configured on both the HPOM management server and the managed nodes.

❏ User logins:

Login without a password for user `root` must be enabled on both the HPOM management server and the managed nodes. See “Installing HPOM Agent Software Using SSH” on page 39.

NOTE Login without a password is only required during the HPOM agent installation and upgrade. You can disable it afterwards.

Installing HPOM Agent Software Using SSH

To install HPOM agent software using the SSH installation method, follow these steps:

1. Configure login for user root.

   The recommended method to configure login without a password is RSA authentication, based on the user’s public/private key pair and the `ssh` agent utility.

   To configure a login using the provided utilities, follow these steps:

   a. If you are setting up an HP-UX managed node, make sure that the `sshd` configuration options in `/usr/local/etc/sshd_config` are set as follows:

   ```
   AllowTcpForwarding yes
   X11Forwarding yes
   X11DisplayOffset 10
   X11UseLocalhost no
   ```

   b. Generate the key pair using the `ssh-keygen` command, as follows:

```
# ssh-keygen

Initializing random number generator...
Generating p: ...........++ (distance 186)
Generating q: ......................................++
(distance 498)
Computing the keys...
Testing the keys...
Key generation complete.
Enter file in which to save the key
(/home/username/.ssh/identity): <press Enter>
```

NOTE Make sure *not* to provide a passphrase. This way, no private key is needed when establishing a connection.

```
Enter passphrase: <press Enter>
Enter the same passphrase again: <press Enter>
Identification has been saved in
/home/username/.ssh/identity.
Your public key is:
1024 35 718535638573954[...] username@local

Public key has been saved in
/home/username/.ssh/identity.pub
```

c. Use `ssh` to connect to the managed node, and from there connect back to the management server.

   This step creates the `$HOME/.ssh` directory on the managed node, as well as some files in that directory. After the directory is created, log out from the managed node.

d. Copy the local public key to the managed node using one of the following methods:

   - Use the secure-copy command, `scp`:

     ```
     # scp .ssh/identity.pub \
     user@managednode:.ssh/authorized_keys
     ```

   - Use the secure-shell command, `scp`:

     ```
     # ssh user@managednode 'cat >>
     ~/.ssh/authorized_keys' < ~/.ssh/identity.pub
     ```

NOTE

Since the file ~/.ssh/authorized_keys can contain many keys, it is important that it is not overwritten during the preparations for the installation on a new system. The second method for transferring public key mentioned above, will not overwrite the file.

e. During the HPOM agent installation, ssh and scp executables must reside in one of the following recommended locations:

- /usr/bin/
- /usr/sbin/

Create a soft link to the **ssh** executable. For example:

```
# ln -s /usr/local/bin/ssh /usr/bin/ssh
# ln -s /usr/local/bin/scp /usr/bin/scp
# ln -s /usr/local/sbin/sshd /usr/sbin/sshd
```

2. Set up managed nodes for HPOM agent installation using SSH.

   When the inst.sh script prompts you to enter the distribution method for the agent package, choose 4=Secure Shell installation (default=1).

Installing HPOM Agent Software Using SSH Agent Installation Method

This section describes how to use the Secure Shell (SSH) agent to install the HPOM agent software on managed nodes. The difference between the method described in this section and the method described in "Installing HPOM Agent Software Using SSH" on page 39 is that, for the software-installation method described in *this* section, you must provide a password before the installation starts. The software-installation method described in this section helps prevent password-less logins to managed nodes by the root user from the HPOM management server.

The procedure is as follows:

1. Generate and distribute a password protected key (identity):

a. Run `ssh-keygen` as described in step 1b of the “Installing HPOM Agent Software Using SSH” section.

IMPORTANT Make sure that you provide a password.

b. Distribute keys to the managed nodes as described in steps 1c and 1d of the “Installing HPOM Agent Software Using SSH” section.

2. Run the SSH agent and set environment variables that are required by the SSH agent:

```
# eval `ssh-agent`
```

You can do it also manually by first running the SSH agent, and then the commands, which the SSH agent lists:

```
# ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-fbdkZc4730/agent.<pid>;
export SSH_AUTH_SOCK;SSH_AGENT_PID=<pid>;
export SSH_AGENT_PID;
echo Agent pid <pid>;
```

3. Add the key to the SSH agent database, and enter the password from step 1 when required:

```
# ssh-add <identity_file_name>
```

For example:

```
# ssh-add /home/username/.ssh/identity
```

NOTE The SSH agent imports all keys under `/home/username/.ssh/` if it is run without the arguments.

4. Run the SSH agent installation. See step 2 of the “Installing HPOM Agent Software Using SSH” section.

5. Remove the key from the database, or stop the SSH agent by running the following command:

```
# ssh-add -d <identity_file_name>
```

HPOM Software Removal on the Managed Node

To remove the HPOM agent software from the managed node, follow these steps:

1. Stop all HPOM agents running on the managed node.
2. Enter commands to remove the software.

To find out which command to enter for the platform from which you are removing the software, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

NOTE After removing the HPOM software from a managed node, you must enter the following command on the management server:

```
# opcsw -de_installed <node>
```

HPOM Agent Software Management

Frequently, managed nodes, including those with the same architecture, do not run the same operating system versions. Different operating systems are used for different purposes, for example:

- ❏ Production systems:

  Run approved operating systems versions where all required applications are available.

- ❏ Development systems:

  Run the approved or latest operating systems versions.

- ❏ Test systems:

  Run approved or latest operating system versions.

Agent Software Version Control

Because different operating systems are used for different purposes, HPOM has to support a growing list of operating system versions. Because of technical limitations and new technologies, it is possible that not all future versions of HPOM may be able to support the entire spectrum of operating system versions. Nevertheless, HPOM does provide internal management of the HPOM agent software version.

If you install a new HPOM agent version (with the same fileset name) on a management server supporting the same set (or a superset) of operating system versions as the previously installed HPOM agent version, the previous HPOM agent version is erased. However, if you install a new HPOM agent version on a management server supporting only some of the previously supported operating system versions, then both HPOM agent versions are kept on the management server.

Displaying Versions of Available Agent Packages

To display a summary of all HPOM agent packages including the supported operating system versions that are currently available on the management server, run the following script on the management server:

`#` **`/opt/OV/bin/OpC/agtinstall/opcversion -a`**

The latest possible HPOM agent version supporting the operating system version of the managed node is probably installed on that node. See “Displaying Versions of Installed Agent Packages” on page 45 for information about how to query the version of the installed agent software.

The related HPOM software for each supported architecture is available in the following directory:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/\
<platform_selector>/<ovo_version>/<package_type>
```

You need to replace the following strings:

<platform_selector>	Specific platform, (for example, `hp/ipf32/hpux1122/`).
<ovo_version>	Version of HPOM that supports the specified agent platform (for example, `A.08.10`).
<package_type>	Type of RPC communication used by the specified agent platform (for example, `RPC_BBC`).

Displaying Versions of Installed Agent Packages

To display the version number of the HPOM agent software that is currently installed on a managed node, run the following command on the management server:

`#` **`/opt/OV/bin/OpC/opcragt -agent_version`** ***`<node>`*****`...`**

See the reference page *opcragt(1M)* for more information about possible restrictions of this command.

Managed Node Administration with Subagent ID Values

If the managed-node communication type is HTTPS in HPOM on Linux, the `opcragt` command with the `-id` parameter enables you to specify the subagent ID either as a number or a name. For more information about the `-id` option and the `opcragt` command, refer to the command's reference page.

If the `-id` is specified as a name, HPOM can communicate with the selected node directly. If the `subagent id` is specified as a number, the number must be mapped to a `subagent id name` in the `subagt_aliases` file, which is located in the following directory:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/`

The following mappings are defined by default in the `subagent_aliases` file:

0	AGENT
1	EA
12	CODA

If a mapping between number and name is required but is not defined, the `opcragt` command displays the following error message:

```
Subagent XXX:
Subagent not registered.
```

NOTE The `-id` option is provided for backward compatibility with older versions of HPOM on Linux.

For example, you can use the `-id` option to specify the subagent ID when querying the status of the subagent processes on the managed node or when stopping and starting the subagent processes.

Querying the HPOM Subagent Status

To display the current status of the HPOM subagent using the subagent ID, use the `opcragt` command with the `-start` and `-id` options, as follows:

```
# opcragt -id CODA <node_name>
```

```
Node <node_name>:
OVO Managed Node status :
-------------------------
Control Agent /opt/OV/bin/OpC/opcctla            (7052) is running
Message Agent/opt/OV/bin/OpC/opcmsga             (7059) is running
BBC Local Location Broker /opt/OV/bin/llbserver(7060    is running
Subagent 12:
Performance Agent /opt/OV/bin/coda -redirect     (7062) is running
Done.

Node <node_name>:
OVO Managed Node status :
-------------------------
OV Control                 ovcd                 (12338) is running
OV Communication Broker    ovbbccb              (12339) is running
OV Config and Deploy       ovconfd              (12342) is running
Subagent CODA:
OV Performance Core    coda                     (12345) is running
Done.
```

Stopping and Starting HPOM Subagents

To use the subagent ID to start or stop the HPOM Subagent on a managed node, use the opcragt command with the -start and -id options, as follows:

`#` **`opcragt -start -id CODA`** ***`<node_name>`***

```
Node <node_name>:
Starting OpC services...Done.
```

<node_name> Name of the managed node where you want to stop or start the HPOM subagent using the subagent ID

Subagent Management in HPOM

Subagents are components that are not a part of the default HPOM distribution but can be partially managed from HPOM. Some of the subagents are controlled by the OV Control daemon.

CAUTION The term “subagent” is used in several contexts to mean different things. In this section, subagent refers to third-party software which runs as a subagent and can be controlled by HPOM. However, “subagent” is also used to refer to parts of the DCE agent that can be individually started and stopped, for example, using the `opcragt` command, as described in “Managed Node Administration with Subagent ID Values” on page 46.

Prerequisites for Managing Subagents

Managing subagents in HPOM relies on some underlying concepts and prerequisites which are normally fulfilled by the subagent software provider. Nevertheless, their understanding is crucial for successful administration of subagents within HPOM. They are briefly presented in the *HPOM Concepts Guide*.

Subagent Administration in HPOM

When you install the subagent software packages on the HPOM management server, there are some tasks you should perform to ensure that subagents are properly installed and functioning on managed nodes. The tasks are outlined in the following topics:

❏ “Subagent Assignment to Managed Nodes” on page 49
❏ “Subagent Installation on Managed Nodes” on page 49

To avoid problems during the distribution of subagent to managed nodes, consider also the tasks presented in the following topics:

❏ “Activating the Subagent” on page 50
❏ “Resolving Migration Problems” on page 50

Subagent Assignment to Managed Nodes

Subagents are assigned to managed nodes in the way that their corresponding subagent registration policies are assigned to these nodes. In case these policies are placed in the appropriate policy group, both the subagent and its configuration are also simultaneously assigned when the policy group is assigned to a node.

NOTE If the appropriate node type is not present in the subagent registration file, the installation of a subagent fails.

Refer to the *HPOM Concepts Guide* for information about assigning policies and policy groups to managed nodes.

Subagent Installation on Managed Nodes

The `opcbbcdist` process uses already prepared distribution description files to install the subagent on the managed node. These files are placed upon the subagent software installation at the predefined location on an HPOM management server.

Installing the Subagent Software

To install the subagent software on the managed node, type the following:

```
# opcragt -subagent -install <subagent_name> <node_name>
```

Where the *<node_name>* is the name of the node on which you want to install the subagent.

Removing the Subagent Software

To uninstall the subagent software, use the `opcragt` command with the following options:

```
# opcragt -subagent -uninstall <subagent_name> <node_name>
```

Installing all Subagents

To install *all* assigned subagents on a managed node simultaneously, use the `opcragt` command with the following options:

```
# opcragt -distrib -subagts <node_name>
```

Redistributing the Subagent Software

To redistribute the subagent software, use the `opcragt` command with the following options:

`#` **`opcragt -subagent -reinstall`** ***`<subagent_name> <node_name>`***

NOTE Using the `opcragt` command with the `-force` option does not trigger the redistribution process. This is to prevent the unnecessary deployment of subagent packages on the agent. For more information about the `opcragt` command options, refer to the *opcragt (1M)* reference page.

To find out how to configure installed subagent packages, see the documentation supplied with the subagent packages.

Activating the Subagent

To activate the subagent on a particular node, use the `opcragt` command with the following options:

`#` **`opcragt -subagent -active`** ***`<subagent_name> <node_name>`***

Activating a subagent means setting the active flag for this subagent in the HPOM database.

Since active flag indicates that the subagent is already installed on the managed node, this subagent will not be installed again on this particular managed node during the subagent distribution process.

Activating a subagent is useful when an agent was either manually installed on the managed node, or it was installed from another HPOM management server. When the configuration is migrated from one HPOM server to another, it is especially advisable to activate subagents for managed nodes on the target HPOM server. In this case, the subagent packages may not be transferred as well, and if the subagents are not activated, error messages appear upon subsequent distribution.

Resolving Migration Problems

To avoid problems during the distribution of subagent software to the managed nodes, perform *one* of the following tasks:

- ❏ Install all subagent packages on the HPOM management server where you intend to upload the downloaded configuration.

- ❑ Remove subagent registration policies from the policy groups when they are uploaded (or deassigned from managed nodes, if they are previously directly assigned). Note that this makes it impossible to obtain a complete inventory report for particular subagents on managed nodes.

If you migrate the configuration from one HPOM server to another, subagent packages are not downloaded along with the policies. This results in failure of the subsequent subagent distribution to nodes, since subagent registration policies point to non-existing subagent packages. To avoid error messages during subsequent distributions, activate the subagents for managed nodes on the target HPOM server. For more information, see “Activating the Subagent” on page 50.

Debugging Software Installation and Removal on Managed Nodes

HPOM provides tools that help debug the installation and removal of the HPOM software on the managed nodes. These tools help developers when testing HPOM installation scripts for new platforms, and assist users in examining errors that occur during the installation of the HPOM agent software.

Debugging Tools for Software Installation and Removal

The following tools are available to help debug problems that occur when installing or removing HPOM software on the managed node:

- Command tracing:

  Prints shell commands and their arguments from installation programs into a file specified in the file `inst_debug.conf` as argument of the environment variable `OPC_DEBUG_FILE`.

- Event tracing:

  Can be used in addition to command tracing to record important events of the installation process into the existing installation logfile:

  `/var/opt/OV/log/OpC/mgmt_sv/install.log`

You can debug the installation or removal process locally (on the management server) and remotely (on the managed node). A debug definition file `inst_debug.conf` is provided to force debugging and to specify debug options.

Enabling Debugging

The file inst_debug.conf must be edited before starting the installation process. It can only be edited by user root.

To enable the debugging of software installation and removal, follow these steps:

1. Copy the file inst_debug.conf by entering:

   ```
   # cp /etc/opt/OV/share/tmp/OpC/mgmt_sv/inst_debug.conf \
   /var/opt/OV/share/tmp/OpC/mgmt_sv/inst_debug.conf
   ```

2. Edit your copy of the file inst_debug.conf by uncommenting the desired environment variables and by changing the values.

NOTE The syntax of the file inst_debug.conf is not checked. Be careful when editing this file. If there are any syntax errors in the file, the installation process will abort.

For a detailed description of the (de-)installation debug facilities, as well as examples of the file inst_debug.conf, see the reference page *inst_debug(5)*.

Disabling Debugging

To disable debugging, remove the following file:

```
/var/opt/OV/share/tmp/OpC/mgmt_sv/inst_debug.conf
```

2 HPOM Configuration

In this Chapter

This chapter describes the preconfigured elements for HP Operations Manager (HPOM). It also describes how to distribute the HPOM configuration to managed nodes, and how to integrate applications into HPOM. To better understand the elements and windows you can use to customize these preconfigured elements, refer to the *HPOM Concepts Guide*.

The information in this section covers the following topics:

❑ “Preconfigured Elements” on page 57
❑ “HPOM Policies” on page 79
❑ “Database Reports” on page 90
❑ “Flexible Management Configuration” on page 98
❑ “HPOM Variables” on page 135

Preconfigured Elements

This section describes defaults for managed nodes, message groups, and message ownership.

By default, the management server is configured as a managed node with the default policies for SNMP event interception, HPOM message interception, logfile encapsulation and monitoring.

Default Node Groups

HPOM provides default node groups for the management server. You can add, modify, delete, and hide these default node groups, as needed.

Managing Node Groups

You can add, modify, delete, and list node groups using the `opcnode` command line tool HPOM. For more information, refer to the *opcnode(1m)* reference page.

Default Message Groups

HPOM provides default message groups. You can add, review, and delete message groups. You can perform these tasks using the Administrator's GUI (CVPL). See the CVPL user documentation available for download in the HP Operations Manager for UNIX directory at:

http://support.openview.hp.com/selfsolve/manuals

Details about individual message groups provided with HPOM are shown in Table 2-1.

Table 2-1 HPOM Default Message Groups

Message Group	Description
Backup	Messages about backing up, restoring, and restoring HPOM (for example, `fbackup(1)`, HP Data Protector, HP OmniStorage, Turbo-Store).
Certificate	Messages related to certificate handling.

Table 2-1 HPOM Default Message Groups (Continued)

Message Group	Description
Database	Messages about database problems
HA	Messages about high-availability problems.
Hardware	Messages about hardware problems
Job	Messages about job streaming.
Misc	Messages that cannot be assigned to any other message group. If a message does not have a message group assigned, or if the message group is not configured, the message automatically belongs to the Misc message group. This message group cannot be deleted.
Network	Messages about network or connectivity problems.
OpC	Messages generated by HPOM itself. This message group should not be used by `opcmsg(1|3)`. Note that you cannot delete the OpC message group.
OS	Messages about malfunctions in the operating system, I/O, and so on.
Output	Messages about print spooling and hardcopy functionality (for example, `lp(1)`, `lpr(1)`.
Performance	Messages about hardware malfunctions (that is, CPU, disk, or process malfunctions) and software malfunctions (for example, HP Performance malfunctions).
Security	Messages about security violations or attempts to break into a system.
SNMP	Messages generated by SNMP traps.

Message Ownership

HPOM message ownership enables users to mark or own messages. The information in this section explains what marking and owning means and how you can configure HPOM to indicate who owns a message and how the ownership should be displayed.

By marking or owning a message, you can inform others that you have taken responsibility for resolving the message's underlying problem. Marking or owning a message restricts access to the message:

- ❏ Marking a message:

  Operator or administrator takes note of a message.

- ❏ Owning a message:

  Operator or administrator either chooses to take charge of a message or is forced to take charge of a message, depending on how your environment has been configured. The operator or administrator must take charge of the message to carry out actions associated with that message.

HPOM enables you to configure the way in which message ownership is displayed and enforced. To display message ownership, you set the message-ownership display mode; to enforce message ownership, you set the message-ownership mode.

The information in this section covers the following topics:

- ❏ "Ownership-Mode Types" on page 59
- ❏ "Configuring Message-Ownership Mode" on page 61
- ❏ "Ownership Display-Mode Types" on page 61
- ❏ "Changing Ownership Display Modes" on page 62

Ownership-Mode Types

You set the ownership policy by selecting one of the following default ownership modes:

Optional — User *may* take ownership of a message. Use the option `OPC_OWN_MODE OPTIONAL`, as described in "Optional Ownership Mode" on page 60.

Enforced	User *must* take ownership of messages. Use the option `OPC_OWN_MODE ENFORCED`, as described in "Enforced Ownership Mode" on page 60.
Informational	Concept of ownership is replaced with that of marking messages. A marked message indicates that an operator has taken note of a message. Use the option `OPC_OWN_MODE INFORM`, as described in "Informational Ownership Mode" on page 60.

Optional Ownership Mode In *optional* ownership mode, the owner of a message has exclusive read-write access to the message. All other users who can view the message in their browsers have only limited access to it.

In optional ownership mode, only the owner of a message may perform the following operations:

❏ Message actions:

Perform operator-initiated actions related to the message.

❏ Message acknowledgement:

Acknowledge the message (that is, move the message to the history database).

Enforced Ownership Mode In *enforced* ownership mode, a user either chooses explicitly to take ownership of a message, or is assigned the message automatically. A message can be assigned to an operator if the operator attempts to perform operations on a message that is not owned by any other operator.

In enforced mode, ownership of a message is assigned to any operator who performs any of the following operations on a message:

❏ Message actions:

Perform an operator-initiated action attached to the message.

❏ Message unacknowledgement:

Unacknowledge a message, that is: move the message from the history browser to the active-messages browser.

Informational Ownership Mode In *informational* mode, a marked message indicates that an operator has taken note of a message. Marking a message is for informational purposes only. Unlike optional and enforced modes of message ownership, informational mode does not restrict or alter operations on the message. Note that operators can unmark only those messages they themselves have marked.

Configuring Message-Ownership Mode

To specify the message-ownership mode, use the `ovconfig` command with the following options:

```
# ovconfchg -ovrg server -ns opc -set OPC_OWN_MODE\
<ownership_mode_value>
```

Where *<ownership_mode_value>* is one of the following:

- ❏ `ENFORCED`
- ❏ `OPTIONAL`
- ❏ `INFORM`

If the ownership mode is not specified, HPOM assumes the default value `OPC_OWN_MODE ENFORCED`. For more information about the different message-ownership modes, see “Ownership-Mode Types” on page 59.

Ownership Display-Mode Types

HPOM provides different ways to configure the way in which message ownership is displayed and enforced. HPOM provides the following ownership-display modes:

- ❏ No status propagation:

  Default setting: Uses the option `OPC_OWN_DISPLAY NO_STATUS_PROPAGATE`. For more information, see “No-Status-Propagation Display Mode” on page 61.

- ❏ Status propagation:

  Uses the option `OPC_OWN_DISPLAY STATUS_PROPAGATE`. For more information, see “Status-Propagation Display Mode” on page 62.

No-Status-Propagation Display Mode If the display mode is set to `NO_STATUS_PROPAGATE`, the severity color of a message changes when the message is owned or marked.

HPOM uses the following default colors to indicate ownership:

Pink	Message is owned by you.

Beige Message is owned by someone else.

In addition, the own-state color bar at the bottom of the Java GUI `Message Browser` reflects the new number of messages owned.

Status-Propagation Display Mode If the ownership-display mode is set to `STATUS_PROPAGATE`, the status of *all* messages (whether they are owned or not) is used for the propagation of severity status to the related symbols of other submap windows. In this display mode, the only indication that the a message is owned is a flag in the own-state column in the Java GUI `Message Browser`.

For information on how to configure the ownership and ownership-display modes, see "Configuring Message-Ownership Mode" on page 61.

Changing Ownership Display Modes

To change the ownership display mode, perform the following steps:

1. Change the ownership display mode using the `ovconfchg` command with the following parameters and options:

   ```
   # ovconfchg -ovrg server -ns opc -set OPC_OWN_DISPLAY\
   <ownership_display_mode_value>
   ```

   Note that *<ownership_display_mode_value>* is one of the following:

   - `STATUS_PROPAGATE`
   - `NO_STATUS_PROPAGATE`

   If the ownership display mode is not specified, HPOM assumes the default value `NO_STATUS_PROPAGATE`. For more information about message-ownership display modes, see "Ownership Display-Mode Types" on page 61.

2. Reload the configuration of any connected Java GUI. For more information about the configuration of the Java GUI, refer to the *HPOM Java GUI Operator's Guide*.

Policy Groups

You can use the `opcpolicy` command line tool to add, modify, or delete policies and policy groups. For more information about command options, refer to the *opcpolicy (1M)* reference page.

Default Policy Groups

HPOM provides a variety of policy groups that you can use for the monitoring and configuration of the HP Operations management server. You can use the `opcpolicy` command to list the installed policy groups and check the contents of individual policy groups. The `opcpolicy` command is located in the `/opt/OV/bin/OpC/utils` directory.

The following default policy groups are provided with the HPOM management server:

- ❏ Correlation Composer
- ❏ Examples:
  - — ECS
  - — Unix
  - — Windows
- ❏ Management Server
- ❏ SNMP
- ❏ SiteScope Integration/*<SiteScope Policy Group>*

Displaying a List of Policy Groups

To display a list of the policy groups deployed on an HPOM managed node or the HPOM management server, use the `opcpolicy` command with the `-list_groups` option, as follows:

```
# /opt/OV/bin/OpC/utils/opcpolicy -list_groups
```

The `opcpolicy` command with the `-list_groups` parameter displays the following information on the HPOM management server:

```
[root@omlinux1 ~]# opcpolicy -list_groups
---------------------------
policy group: /Correlation Composer
---------------------------
policy group: /Examples
---------------------------
policy group: /Examples/ECS
---------------------------
policy group: /Examples/Unix
---------------------------
policy group: /Examples/Windows
```

```
---------------------------
policy group: /Management Server
---------------------------
policy group: /SNMP
---------------------------
policy group: /SiteScope Integration
...
---------------------------
```

Displaying the Contents of a Policy Group

To display a list of the policies contained in an individual policy group, use the `opcpolicy` command with the `-list_group` option as follows:

`#` **`/opt/OV/bin/OpC/utils/opcpolicy -list_group \`**
`"group=<PolicyGroup_Name>"`

<PolicyGroup_Name>	Name of the HPOM policy groups whose contents you want to list, for example "Management Server", which produces the following result:

The following text is an excerpt from the output the command displays:

```
---------------------------
policy group: /Management Server
assigned policy    : opcmsg(1|3), version 0009.0000, LATEST
assigned policy    : distrib_mon, version 0009.0000, LATEST
assigned policy    : mondbfile, version 0009.0000, LATEST
assigned node      : omlinux1
---------------------------
```

Default Users

HPOM provides a number of user configurations. You can customize these default settings to match the specific requirements of your organization.

Default User Types

Standard HPOM user configurations include the following:

opc_adm	HPOM administrator

opc_op	HPOM operator

NOTE The home directory of `opc_op` is always `/home/opc_op` on HP-UX and `/export/home/opc_op` on Solaris.

netop	Network operator
itop	IT operator

Default HPOM User Names and Passwords

For a list of default user names and passwords for all preconfigured users, see Table 2-2 on page 65.

Table 2-2 **HPOM User Names and Passwords**

Default User	Default User Name	Default Password
HPOM administrator	opc_adm	OpC_adm
`itop` operator	itop	ItO_op
`netop` operator	netop	NeT_op
`opc_op` operator	opc_op	OpC_op

HPOM Administrators

HPOM supports only one HPOM administrator, whose responsibility it is to set up and maintain the HPOM software. You cannot modify the HPOM administrator's login name, `opc_adm`. For more detailed information about configuring HPOM users using the command-line interface, refer to the *opccfguser(1m)* reference page.

Default Operator Types

HPOM provides three default operators:

- ❏ `opc_op`
- ❏ `netop`
- ❏ `itop`

These default operators are preconfigured with distinct areas of responsibility. For more information on the scope of each default operator, see the *HPOM Concepts Guide*.

Default Node-Group Types

Table 2-3 shows which node groups are assigned by default to each HPOM operator.

Table 2-3 Default Node Groups for Operators

Node Group	opc_op	netop	itop
HP-UX	✓		✓
Net Devices		✓	✓
Solaris	✓		✓

Default Message-Group Types

Table 2-4 shows which message groups are assigned by default to each HPOM operator.

Table 2-4 Default Message Groups for Operators

Message Group	opc_op	netop	itop
Backup	✓		✓
Databases	✓		✓
HA	✓		✓
Hardware	✓		✓
Job	✓		✓
Misc	✓		✓
Network	✓	✓	✓
OpC	✓		✓
OS	✓		✓
Output	✓		✓

Table 2-4 Default Message Groups for Operators (Continued)

Message Group	opc_op	netop	itop
Performance	✓		✓
Security	✓		✓
SNMP	✓	✓	✓

The messages each operator receives and the nodes those messages come from are not necessarily the same. The responsibility matrix you chose for a given operator determines which node group sends which messages to which operator.

For example, by default, all HPOM operators have the `Network` message group in their Java GUI `Object Pane`. However, the node groups that send messages associated with the `Network` message group vary according to the operator. The origin of the messages depends on the selection you make in a given operator's responsibility matrix.

Default Application-Group Types

Table 2-5 shows which application groups are assigned by default to each HPOM operator.

Table 2-5 Default Application Groups for Operators

Application Groups	opc_op	netop	itop
Distr NNM Admin Tools			✓
NNM Admin Tools			✓
NNM Views		✓	✓
NNM-ET Views		✓	✓
Net Diag			✓
X-OVw		✓	✓

Default Application Types

The applications and application groups assigned by default to the HPOM users reflect the responsibilities you assign to them.

Table 2-6 on page 68 shows you which applications are assigned by default to each user. HPOM allows you to add, delete, and move applications using the `opcappl` command line tool. You can use the default settings as a base for configuring users and responsibilities that match the needs of individual environments. For more information about managing applications from the command-line interface, refer to the *opcappl(1m)* reference page.

Table 2-6 Default Applications for Operators

Applications	opc_op	netop	itop
Broadcast	✓		✓
Highlight Message Node		✓	✓
Highlight Selected Node		✓	✓
Start OVw		✓	✓
HPOM Status	✓		✓

Default Applications and Application Groups

Default applications and application groups are provided with the HPOM server installation.

NOTE HPOM applications are available for reference but no longer as default for the specified agent platforms.

Table 2-7 shows the default applications and application groups provided by HPOM.

Table 2-7 Default Applications and Application Groups

Name	Application	Application Group
Certificate Tools		✓
Distr NNM Admin Tools		✓
Jovw (old)		✓
NNM Admin Tools		✓
NNM Views		✓
NNM-ET Views		✓
NNMi		✓
NNMi Int-Admin		✓
NT Tools		✓
Net Diag		✓
OM License Tools		✓
OV Composer		✓
UN*X Tools		✓
X-OVw		✓
Broadcast	✓	
HPOM Status	✓	

Broadcast Application

The `Broadcast` application enables you to issue the same command on multiple systems in parallel:

- ❏ UNIX:

Default user:	`opc_op`
Default password:	None required because the application is started by the HPOM action agent.

- ❏ Windows:

Default user:	`system`
Default password:	None required because the application is started by the HPOM action agent.

NOTE For both UNIX and Windows operating systems, if the default user credentials have been changed by the operator, you must supply a password.

HPOM-Status Application

The `HPOM Status` application issues the `opcragt` command. This application enables you to remotely generate a current status report about all HPOM agents on all nodes.

The HPOM Control Agent must always run on the managed nodes. Otherwise, the agents cannot remotely be accessed from the HP Operations management server.

Default user:	**root** (user must be **root**)
Default password:	None is required because the application is started through the HPOM action agent.

NOTE If the default user has been changed by the operator, you must supply a password.

X-OVw Application Group

The `X-OVw` application group contains the following applications:

- `Highlight Message Node in OVw`:

  Maps the node related to a selected message to an NNM system, and highlights the node in an ovw session of that NNM system.

- `Highlight Selected Node in OVw`:

  Maps the selected node to an NNM system, and highlights the node in an ovw session of that NNM system.

- `Start OVw`:

  This application starts an ovw session on a remote NNM system.

These application provide the basis for the default integration of HPOM with the Network Node Manager.

IMPORTANT You must not install NNM on the same system as the HPOM management server.

Event Correlation

The runtime engine for HPOM event-correlation is available for the HP Operations management server and the HP Operations agent. See the *HPOM Installation Guide for the Management Server* for a list of platforms on which the runtime engine currently runs.

For more information about the concepts behind event correlation, as well as the way event correlation works in HPOM, see the *HPOM Concepts Guide*.

Configuring Event Correlation for HPOM

The HPOM message-source policy allows you to specify which conditions generate a message and whether or not the generated message is copied or diverted to the message stream interface (MSI) from where it may be passed to and processed by the event correlation template. Follow the procedure below to configure the event correlation:

1. Enable output from the HPOM internal message stream to the MSI as required at either (or both) management server or managed node level as follows:

   - On the HP Operations management server, run the following command:

     `#` **`opcsrvconfig -msi -enable`**

   - On the HP Operations agent, enable output to the MSI using the Administrator's GUI (CVPL). See the CVPL user documentation available for download in the HP Operations Manager for UNIX directory at:

     `http://support.openview.hp.com/selfsolve/manuals`

     Alternatively, you can use the `opcnode_modify()` API, though HPOM does not provide any command line tool to use with this API in the current version. For API related information, refer to the *HPOM Developer's Reference*.

2. Set up the HPOM message-source policy so that the message conditions that you are interested in output messages as intended. For each condition statement (policy block starting with CONDITION), make sure that:

- You specify a message-type attribute in the `CONDITION` or `SET` block of the policy body; attribute can be any of the allowed attributes specified in the policy grammar. For information on policy grammar, see the *HPOM Concepts Guide*.
- The specified message-type attribute matches the corresponding attribute referenced in the Input node that starts the flow in the event-correlation circuit which you want to process the message in question.

3. Enable the Copy/Divert to MSI option for each condition that you wish to output a message, using one of the following keywords in the `SET` section(s):

`MPI_SV_COPY_MSG`	Copy message to MSI and pass it on to HPOM server processes.
`MPI_SV_DIVERT_MSG`	Send message to MSI and remove it from HPOM processing chain on the management server.
`MPI_AGT_COPY_MSG`	On a managed node, copy message to MSI and pass it on to HPOM server processes.
`MPI_AGT_DIVERT_MSG`	On a managed node, send message to MSI and remove it from HPOM processing chain on the management server.

4. Enable, if required, the logging options for each template, by using one or more of the following keywords in the policy body, before specifying conditions:

`LOGMATCHEDMSGCOND`	Logs messages matching message conditions (section starting with `MSGCONDITIONS`).
`LOGMATCHEDSUPPRESS`	Logs messages matching suppress conditions (section starting with `SUPPRESSCONDITIONS`).
`LOGUNMATCHED`	Logs unmatched messages.

Logfile Encapsulation

For detailed information about encapsulating logfiles with the logfile encapsulator, see the *HPOM Concepts Guide*.

Logfile policies are configured to collect information from logfiles that are produced by standard installations. If you are monitoring a non-standard installation, you should modify the policies to suit your particular needs.

Listing Default Log-File Policies

To display details of the logfiles that are monitored by default, use the `opcpolicy` command with the following parameters:

```
# opcpolicy -list_pols pol_type=LOG
```

You can edit existing (and configure new) logfile policies by modifying the policy body. The corresponding logfile policies must be configured so that the HPOM operator knows which system the logfile originated from, or the event which triggered the message. For information on policy body grammar, refer to the *HPOM Concepts Guide*.

SNMP Trap Interception

This section contains information that is specific to NNM version 7. To display details of the SNMP traps and events that HPOM intercepts by default, use the `opcpolicy` command to list the polices matching the SNMP-trap policy type.

Listing SNMP-Trap Policies

To display a list of all policies matching the SNMP-Trap policy type, use the `opcpolicy` command with the following parameters:

```
# opcpolicy -list_pols pol_type="SNMP_Interceptor"
```

By default, HPOM intercepts SNMP traps from any application sending traps to the `opctrapi` daemon. HPOM also intercepts SNMP traps on all managed nodes where the trap daemon (`ovtrapd`) is running, or where port 162 can be accessed directly.

See the *HPOM Installation Guide for the Management Server* for a list of platforms on which the SNMP event interceptor is currently supported.

Intercepted Trap Types

The following types of traps can be intercepted:

- ❏ Well-defined traps

  Example: system coldstart, network interface up/down, and so on

- ❏ Internal HP traps

  Example: traps originating from netmon

Localhost IP Address Resolution

By default, intercepted traps whose source address is the local host address (127.0.0.1) are forwarded to the management server with that address.

Resolving Trap IP Addresses

To intercept traps whose source address is the local host address and forward them to the management server with the local host address replaced by the resolved IP address of the node processing the trap, perform the following on HTTPS-based managed nodes:

```
# ovconfchg -ns eaagt -set OPC_RESOLVE_TRAP_LOCALHOST TRUE
```

Distributed Event Interception

HPOM can intercept distributed events which enables you to intercept SNMP traps on systems other than the HP Operations management server. Intercepting these SNMP traps provides performance benefits by allowing the local processing of messages. Automatic actions, for example, can be triggered and executed directly on the node or in the subnet, instead of being first forwarded to the management server.

HPOM distributed event interception has two configurations:

- ❏ Basic configuration:

  Configure SNMP destinations or NNM collection stations. For more information about setting up the basic configuration for distributed event interception, see “Intercepting Distributed Events” on page 76.

- ❏ Configuration to avoid duplicate messages:

  Make certain that an HPOM agent (and consecutively an HPOM event interceptor) runs on all NNM collection stations. Use the Print Poll Station application in the Distr NNM Admin Tools application group to verify which managed nodes are set up as NNM collection stations.

Intercepting Distributed Events

To configure a basic configuration for distributed event interception, perform the following steps:

1. Configure SNMP destinations or NNM collection stations.

   Make sure that SNMP devices have only one SNMP destination, or that there is only one system serving as the NNM collection station for the management server (preferably, the collection station connected through the fastest network).

   Set the destination systems for SNMP devices on HP-UX and Solaris nodes in the `/etc/SnmpAgent.d/snmpd.conf` file with the following statement:

   `trap_dest:`*<nodename>*

2. If NNM is not running on the node where you want to intercept events, use the `ovconfchg` command with the following options on each managed node:

   ```
   # ovconfchg -ns eaagt -set SNMP_SESSION_MODE NO_TRAPD
   ```

3. Assign and distribute the trap policy to the node.

Event Interception with Event Correlation Services

By default, the trap interceptor `opctrapi` connects to the correlated event flow of `pmd`. You can change the default behavior by using the `ovconfchg` command with the following options on the managed node:

```
# ovconfchg -ns eaagt -set SNMP_EVENT_FLOW [CORR|RAW|ALL]
```

The following options enable you to qualify the SNMP_EVENT_FLOW parameter:

`CORR`	Correlated event flow (default). The correlated event flow (CORR) is further divided into streams.
`RAW`	Uncorrelated event flow. This flow does not contain events created by correlations.
`ALL`	`CORR` plus `RAW` minus any duplicates.

Connecting opctrapi to a Specific ECS Stream

To configure the trap interceptor `opctrapi` to connect to a specific ECS stream of `pmd`, use the `ovconfchg` command with the following options on the managed node:

```
# ovconfchg -ns eaagt -set SNMP_STREAM_NAME <stream_name>
```

For more information about ECS, see *HP ECS Configuring Circuits for NNM and HPOM*.

HPOM Message Interception

By default, any message submitted with the `opcmsg(1)` command or the `opcmsg(3)` API is intercepted. For more information about using the command-line interface to set message-attribute defaults, logging options, and so on, refer to the reference pages *opcmsg(1)* and *opcmsg(3)*.

HPOM internal error messages can also be intercepted by the HPOM message interceptor.

Object Monitoring

Table 2-8 shows how HPOM monitors object thresholds on the management server.

Table 2-8 Object Thresholds on the Management Server

Object	Description	Threshold	Polling Interval
`disk_util`	Monitors disk space utilization on the root disk.	90%	10m
`distrib_mon` [a]	Monitors the software distribution process. Generates a message for each pending distribution.	1	10m

Table 2-8 Object Thresholds on the Management Server (Continued)

Object	Description	Threshold	Polling Interval
`mondbfile` [a]	Monitors free space on disk, as well as the remaining space available for Oracle autoextend datafiles.	0%	10m
`proc_util`	Monitors process table utilization.	75%	5m
`swap_util`	Monitors SWAP utilization.	80%	5m

a. Deployed by default.

Monitoring MIB Objects from Other Communities

To monitor MIB objects from communities other than, Use the `ovconfchg` command-line tool as follows on HTTPS-based managed nodes:

```
# ovconfchg -ns eaagt -set SNMP_COMMUNITY <community>
```

In this instance, *<community>* is the community for which the SNMP daemon `snmpd` is configured. If `SNMP_COMMUNITY` is not set, the default community `public` is used. To find out how to determine the configuration of `snmpd`, see the documentation supplied with the SNMP daemon.

Policies for External Interfaces

By default, no notification is configured. You can configure HPOM Notification Services by using the `opcnotiservice` command line interface. No trouble-ticket system interface is configured. You can set up one by using the `opctt` command line interface.

For more information about using the command-line interface to set up external notification and trouble-ticket services, refer to the *opcnotiservice(1m)* and *opctt(1m)* reference pages.

HPOM Policies

A policy is a configuration element consisting of data and meta information. Policies are deployed to managed nodes. The data information part usually consists of a set of rules for generating the messages on the managed node to which the policy is deployed. While the data information part is completely defined by the user, the meta information part is used for administrative tasks and is managed by the HPOM product. Each policy has a policy type, which means that its bodies conform to a specific set of rules. To learn more about policies and policy types, refer to the *HPOM Concepts Guide*.

Policies can have multiple versions on the HPOM 9.0x management server, and are organized in a tree-like structure. See “Policy Versions” on page 87 and the *HPOM Concepts Guide* for more information.

Policies can also contain category assignments. **Categories** unify the related instrumentation files and make their distribution to the managed nodes easier. For more details, see “Category-Based Distribution of Instrumentation” on page 174.

Policy File-Naming Conventions

The names of policy files must adhere to the following rules:

- Policy header:

  `<uuid>_header.xml`

  For example,
  `33F23DD0-4092-11DE-8A39-0800200c9A66_header.xml`

- Policy body:

  `<uuid>_dataX`

  Where X is the body number. If a policy has only single body, this number can be omitted.

  For example, `33F23DD0-4092-11DE-8A39-0800200c9A66_data`

Adding Policies

Policies can be added to HPOM in one of the following ways:

- Direct upload of policies:

  Policies can be uploaded to the HPOM repository directly using `opcpolicy` command line tool or `opcpolicy_add()` API. Both mechanisms allow upload of single or multiple policies. If multiple policies are to be uploaded, they should be located in the same directory and follow the naming schema rules.

  An example of uploading a single policy using `opcpolicy` command line tool:

  ```
  # opcpolicy -upload \
  file=970FF268-24FA-4f03-9E48-339E2F9A3827_header.xml
  ```

  If multiple policies are located in directory `/tmp/policies`, they can be uploaded using the following command:

  ```
  # opcpolicy -upload dir=/tmp/policies
  ```

  Any files that do not conform to the policy files naming schema will be ignored.

- Upload of policy data downloaded from another HPOM server:

  Transfer of policies from one HPOM server to another can be accomplished using `opccfgdwn` (download) and `opccfgupld` (upload) tools.

Refer to the *opcpolicy (1M)* and *opccfgupld (1M)* reference pages for more information about command options. For more information about available policy-related APIs refer to the *HPOM Developer's Reference* guide.

Registering Policy Types

The policy type must be known on the HPOM server before policy of that type is registered. This is performed by using the `opcpoltype` command line tool, for example:

```
# opcpoltype -reg -xml /var/conf/poltypes.xml
```

Input for `opcpoltype` is an XML file, which describes the policy types registered on the HPOM server.

If you specify the `-dir` option, all files with the `.xml` extension in the specified directory are processed, and treated as policy type registration files.

Refer to the *opcpoltype (1M)* reference page for more information about the `opcpoltype` command options. For information about policy type registration using APIs, refer to the *HPOM Developer's Reference*.

NOTE A new policy type should be registered before any policy of that type is uploaded. If you attempt to upload a policy of an unknown type to the management server, an error is returned. Once the new policy type is registered, policies of that type can be uploaded and later deployed to the HPOM server.

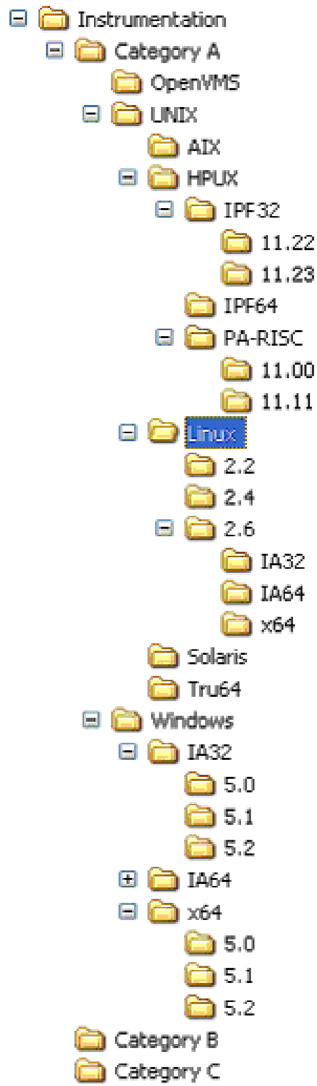
The following is an example of the XML registration file:

```
<policyTypeList>

      <policyType>

              <policyTypeName>Special-log</policyTypeName>

              <policyTypeAgentType>le</policyTypeAgentType>

             <policyTypeUUID>E8405458-2970-4DB7-825C- \
               816B3FBF11FE</policyTypeUUID>

              <policyTypeEditor>/usr/local/bin/specedit \
               -argument</policyTypeEditor>

              <policyTypeCallbacks>

                       <edit>/usr/local/bin/speccopy</edit>

                       <deploy>/usr/local/bin/specadapt</deploy>

              </policyTypeCallbacks>

             <policyTypeTemplate>/usr/local/templates/ \
               special-log.tmpl</policyTypeTemplate>

     </policyType>

</policyTypeList>
```

NOTE Any number of policy types can be registered in a single policy type registration file.

Figure 2-1 on page 82 illustrates the policy type registration schema corresponding to the XML file given in an example above.

Figure 2-1 **Policy type registration schema**



Assigning Policies

Policies can be assigned to policy groups using the `opcpolicy` command and to managed nodes using the `opcnode` command, as follows:

- ❑ Policy assignment to a policy group:

  ```
  # opcpolicy -add_to_group group=<policy_group> \
  pol_name=<policy_name> pol_type=<policy_type_name>
  version=<policy_version>
  ```

- ❑ Policy assignment to a node:

  ```
  # opcnode -assign_pol pol_name=<policy_name> \
  pol_type=<policy_type_name> version=<policy_version>
  node_name=<node_name> net_type=<node_network_type>
  ```

You can list policy types by using the `opcpoltype -list` command. To remove policy assignments, use the following options:

- `opcpolicy -del_from_group`
- `opcnode -deassign_pol`

To list the contents of a policy group, use the `opcpolicy` command as follows:

```
# opcpolicy -list_group pol_group=<policy_group_name>
```

To retrieve a list of policies assigned to a managed node, use the `opcnode` command as follows:

```
# opcnode -list_ass_pol node_name=<node_name> \
<net_type>=<node_network_type>
```

Example of assigning a policy to a policy group:

```
opcpolicy -add_to_group pol_name="Test policy" \
pol_type=Logfile_Entry version=1.0 pol_group="Test group"
```

Example of assigning a policy to a managed node:

```
opcnode -assign_pol pol_name="Measurement policy" \
pol_type=Measurement_Threshold version=1.2 \
node_name=remote.hp.com net_type=NETWORK_IP
```

For more information about the parameters and options available with the `opcpolicy` and `opcnode` commands, refer to the *opcpolicy (1M)* and *opcnode (1M)* reference pages.

Deploying Policies

You can start the policy distribution process as follows:

```
# /opt/OV/bin/OpC/opcragt -distrib -templates <node_name> \
[ <node_name> ... ]
```

By using the `-templates` option of the `opcragt` command you retrieve the assigned policies from the HPOM repository, prepare them for the distribution and start their deployment to the managed nodes.

For more information about the `opcragt` command options, refer to the *opcragt (1M)* reference page.

Deleting Policies

A single policy, as well as an entire container, can be removed from the database by using the `opcpolicy` command line tool. To delete a policy, it has to be uniquely identified by either its name/type/version combination or by its UUID. If just policy name and type are provided, the entire policy container is deleted.

NOTE Deleting the policy also results in deleting all its assignments.

Following is an example of deleting a policy container:

```
# opcpolicy -remove pol_name="Test policy"
pol_type=Logfile_Entry
```

Policy groups are deleted by using `-del_group` option of the `opcpolicy` command line utility. For example, to delete the policy group ”Test group”, use the following command:

```
# opcpolicy -del_group pol_group="Test group"
```

For more information about command options, refer to the *opcpolicy(1M)* reference page.

Downloading Policies

You can download policies using the `-download` option of the `opcpolicy` command line utility.

NOTE If a policy version is omitted from the command line arguments, the entire container is downloaded.

Example of policy download using the `opcpolicy` command line tool:

```
# opcpolicy -download pol_name="Oracle messages"
pol_type="Open_Message_Interface" version=1.0 dir=/tmp
```

For more information about the parameters available with the `opcpolicy` command, refer to the *opcpolicy (1M)* reference page.

Policy Configuration

This section describes how you can use the tools provided to edit and modify policies to suit the needs of your particular environment. The section includes information and tips covering the following areas:

Registering a Policy Editor

The default policy types delivered with HPOM 9.0 have a defined editor, You can define a different editor for custom policy types when registering the new policy-type.

To define and register an editor for a policy type, use the `opcpoltype` command with the following options:

```
# opcpoltype -reg -editor
```

For more information about registering new policy types, see "Registering Policy Types" on page 80.

Changing the Defined Policy Editor

To change the defined editor use the `opcpoltype` command line tool as shown in the following example:

```
# opcpoltype -editor -type "X policy type" \
/usr/local/bin/xeditor
```

For more information about command options, refer to the *opcpoltype(1M)* reference page.

You can edit policies using the Administrator's GUI (CVPL). See the CVPL user documentation available for download in the HP Operations Manager for UNIX directory at:

`http://support.openview.hp.com/selfsolve/manuals`

NOTE If the editor is running on a system other than the HPOM management server, make sure that the policy body is transferred back to the HPOM server, and that the upload is properly performed. To upload a new policy, after the editing is done, you can use either `opcpolicy -upload` or the provided APIs. For more information about the `opcpolicy` command options, refer to the *opcpolicy (1M)* reference page. For information about APIs, refer to the *HPOM Developer's Reference*.

Changing Policy Attributes

To change policy attributes such as description or policy body syntax, use the `opcpolicy` command line tool with `-update` option. `opcpolicy` can only be used to modify attributes that are part of the policy header and will not affect the contents of the policy bodies. For a list of the attributes that can be changed, refer to the *opcpolicy (1M)* reference page.

Changing the Policy Syntax Versions

Each policy type can have a different syntax version. If the syntax version is not specified in the command line arguments when registering a new policy, it is set to the default, 1.

You can change the syntax version of a policy by using the `opcpolicy -update` option with `syn=<syn>` argument set, for example:

```
# opcpolicy -update syn=<policy_syntax_version>
```

NOTE After editing a policy, its syntax version is not changed by default. It can be automatically changed with the `opcpolicy -syn` command within check callback. If you want to change the syntax version manually without using the check callback, you must do it before the next deployment. Otherwise, the policy will be deployed with an old syntax version.

Refer to the *opcpolicy (1M)* reference page for more information about the `opcpolicy` command options.

Policy Versions

With HPOM 9.0x, it is possible to have multiple versions of policies stored on the management server. Having multiple versions of policies on the HPOM 9.0x management server enhances the flexibility in operating with policies and policy groups, and allows simplified interoperability between HPOM on Linux and Windows platforms.

❏ “Changing the Policy Version” on page 87

❏ “Migrating HPOM 8.xx Templates to HPOM 9.0x Policies” on page 88

For more information about the concepts of policy versions and the organization of the policy-group hierarchy, see the *HPOM Concepts Guide*.

Changing the Policy Version

All policies have version numbers. To replace a particular policy version, use the `opcpolicy` command with the `-update` parameter as follows:

```
# opcpolicy -update version=<policy_version>
```

You can also upload and download specific versions of a policy and instruct HPOM what to do if a version already exists. For more information about the `opcpolicy` command and the `-update` parameter, refer to the *opcpolicy(1m)* reference page.

The policy version numbers can also be changed without the need to modify the policy content. This is especially useful when aligning the policy versions that are released together. Refer to the *opcpolicy (1M)* reference page for more information about command options. For more information about the available APIs, refer to the *HPOM Developer's Reference*.

NOTE The new version number creation results in the creation of a new policy, even if the content is unchanged. The new policy has a new version UUID, but the container ID is same as before. On the other hand, changing the policy name results in a new object in the database with a new version UUID and a new container ID.

Migrating HPOM 8.xx Templates to HPOM 9.0x Policies

To migrate templates from HPOM 8.xx to HPOM 9.0x, use the `opccfgupld` utility with the `-replace` parameter as follows:

`#` **`opccfgupld -replace [-subentity]`**

When migrating policies, note the changes in the directory structure used for the upload and the download operations. For example:

- HPOM 8.xx:

  <upload_path>/TEMPLATES/*

  (also includes <upload_path>/TEMPLATES/TEMPLGROUPS)

- HPOM 9.0x:

  <upload_path>/POLICIES

  and

  <upload_path>/POLICYGROUPS

For more information about the `opcdfgupld` command and permitted parameters, refer to the *opccfgupld (1M)* reference page.

NOTE If the HPOM policy checksum comparison finds version 1.0 policies are identical, the upload is skipped. In the event that policies with the same version number have different contents, you can use the `-add | -replace [-subentity]` parameter to add a new policy version or replace the existing version.

Policy Assignment Tasks in HPOM

Table 2-9 lists policy-related tasks and operations provided with HPOM for Windows 8.xx, HPOM for Unix 8.xx and 9.0x, and HPOM on Linux 9.01. The comparison can help you to get a clear overview of the scope of assignment tasks, and to enhance the interoperability among these products. Refer to the *HPOM Administrator's Reference* for more information about HPOM interoperability.

Table 2-9 Policy Management in HPOM

		HPOM 8.xx for Windows Policies		HPOM 8.xx for Unix Templates		HPOM 9.0x on Unix/Linux Policies	
		New	Existing	New	Existing	New	Existing
Create		✔		✔		✔	
Deploy		✔	✔	✔	✔	✔	✔
Assign				✔		✔	
Update assignments							✔
Modify	Create new version		✔				✔
	Overwrite				✔		✔

Updating Policy Assignments

Policies can be assigned to nodes, node groups, and policy groups. A basic difference between HPOM 8.xx and HPOM 9.0x is that the modification of the policy leads to a new policy version in HPOM 9.0x, while in HPOM 8.xx the existing template is overwritten. This also means that the existing assignments point to the older policy version, and not to the modified one. Therefore, the assignments must be updated. The update of the assignments can be done automatically. HPOM 9.0x introduces three assignment modes, namely `FIX`, `LATEST`, and `MINOR_TO_LATEST`.

You can specify the assignment mode by using the `opcpolicy` and `opcnode` command line utilities. Refer to the *opcpolicy (1M)* and *opcnode(1m)* reference pages for usage details.

Database Reports

HPOM provides preconfigured reports for the administrator and the operators. In addition, you can create customized reports using the report writer supplied with the installed database or any other report-writing tool.

You can do the following with database reports:

- ❏ Display in a window
- ❏ Save to a file
- ❏ Print

Defining a Printer for Reports

You can define a printer for reports using the X resource, `Opc.printCommand`, in the general application defaults file:

`/opt/OV/lib/X11/app-defaults/<language>/Opc`

Or you can use `Opc.printCommand` in your private file:

`$HOME/.Xdefaults`

Configuring Time-Outs for Report Generation

If you expect that generating a report may take longer than five minutes, set the keyword `OPC_REPORT_TIMEOUT` using the command-line tool `ovconfchg` on the HP Operations management server. By default, this keyword assumes a value of 300 seconds. To increase the time-out, set the keyword using the `ovconfchg`, specify the desired value in seconds, and restart your GUI session.

Generating Reports for the Internet

You can retrieve specific information directly from the database and publish and view the resulting reports in graphically rich formats on the Internet. To generate these Internet-ready reports, use enhanced reporting features of HPOM in conjunction with HP Service Reporter. For more information, see the documentation supplied with the HP Service Reporter and the *HPOM Concepts Guide*.

Integrating a New Report

You can create SQL*Plus reports (called from the shell script `call_sqlplus.sh`) or program reports. To modify a report you can either change the program, or customize the report's configuration file.

You configure a new report by creating a new script, writing a new program, or by creating a new SQL*Plus file. Then you edit existing plain text files to integrate the new reports. These configuration files define which reports are intended for the administrator and which are for the operator.

1. Change to the directory containing the report files.

   Enter:

   `#` **`/etc/opt/OV/share/conf/OpC/mgmt_sv/reports/<`*`lang`*`>`**

2. Either modify an existing report, or create a new SQL*Plus report.

   The name of the new report must have the ending `.sql` and must reside in the `reports` directory you accessed in the previous step.

3. Test the new or modified report.

   Use the `call_sqlplus` command with the following parameters, where <*name*> is the name of the report file *without* the `.sql` suffix, and <*parameter*> is an optional parameter passed to the report:

   `#` **`/opt/OV/bin/OpC/call_sqlplus.sh <`*`name`*`> <`*`parameter`*`>`**

   For more information about report syntax, permitted parameters, and file-naming conventions, see "Report Syntax" on page 92 and "Report Parameters" on page 92.

4. Choose the intended audience for the report.

   Edit the appropriate configuration file to define the target audience for the report. The configuration file `oper.rpts` lists HPOM operator reports; `admin.rpts` lists reports for the HPOM administrator. The `.rpts` file contains a definition for each report. For more information about report syntax, permitted parameters, and file-naming conventions, see "Report Syntax" on page 92 and "Report Parameters" on page 92.

5. Save the appended `.rpts` file.

   Save the new or modified report definition in the `reports` directory: `/etc/opt/OV/share/conf/OpC/mgmt_sv/reports/<`*`lang`*`>`.

Report Syntax

The syntax of the report definition is as follows:

```
DESCRIPTION   %<descriptive text>
PARM          %<OpC parameter>
REPORTFILE    %<full directory path to file or program>
REPORTNAME    %<name>
REPORTTYPE    %<PGM>
```

Report Parameters

HPOM reports support the use of the following parameters:

`$node`	selected node name
`$nodegrp`	selected node group id
`$msggrp`	selected message group name
`$application`	selected application id
`$operator`	selected operator id
`$message_history`	selected message id
`$message_active`	selected message id
`$template`	selected template

Preconfigured Administrator Report Types

Table 2-10 describes various reports configured for the HPOM administrator. You can access these reports by using the `call_sqlplus.sh` script.

Table 2-10 Preconfigured Reports for the HPOM Administrator

Report Name	Description
All Active Messages	Report on the number of active messages per message group.
Cert. State Overview	Report about Cert. States for all configured nodes.
Licence Overview	HPOM licence status and report.

Table 2-10 Preconfigured Reports for the HPOM Administrator (Continued)

Report Name	Description
Node Config Report	Report on all resulting policy to node assignments.
Node Group Report	Detailed report on a selected Node Group. Same as "Nodes Overview" except it adds user and message-group assignments for the given node group.
Node Groups Overview	Report on all configured Node Groups indicating which nodes and external nodes belong to which node groups.
Node Reference Report	Report on referenced nodes that are not in the Node Bank.
Node Report	Detailed report on a selected managed node.
Nodes Overview	Report on all configured nodes. Shows the node name, machine type, node type (for example, message-allowed, controlled), license, and heartbeat polling settings.
Oper. Active Details	Report on all active messages for an operator (detailed description).
Oper. Active Message	Report on all active messages for an operator (short description).
Operator History Messages	Short history of the (acknowledged) messages for a given operator.
Operator Overview	Short description of all configured operators, including real and logon names, role, rights, and responsibilities.
Operator Pending Messages	Short description of pending messages for a given operator.
Operator Report	Detailed report on a selected operator. Includes a responsibility matrix (node and message groups), available applications, and assigned user profiles.

Table 2-10 Preconfigured Reports for the HPOM Administrator (Continued)

Report Name	Description
HPOM Error Report	Review of the HPOM error logfile on the management server: `/var/opt/OV/log/System.txt` (Plain text) or `/var/opt/OV/log/System.bin` (Binary)[a]
Policy Detail	Detailed report on one selected policy.
Policies Overview	Lists all policies. Shows which policy groups the various policies belong to.
Policies Summary	Report about *all* aspects of *all* policies. Might take a long time to generate.
Unmonitored	Report on configured but currently unmonitored objects. Indicates, for example, the unassigned node group or message group combinations.
User Logon/Logoff Report	Same as “Logon/Logoff Report” except it is for only one selected user.
User Profile Overview	Report on all configured user profiles.
User Profile Report	Detailed report on one selected user profile.
Working HPOM Users	Report on all HPOM users who are currently logged on. Shows, for example, the IP addresses of their machines.

a. For more information about the logfiles containing the errors, see “Reporting Errors” on page 408.

Defining Customized Administrator Reports

You can define customized administrator reports by modifying the following file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/reports/<lang>/\
admin.rpts
```

If no absolute path is specified, the output of all HPOM administrator reports is saved by default in the directory of the UNIX user that started the HPOM administrator session. This directory is defined by $HOME or `/tmp` in that order. All files that you create and save as HPOM administrator are owned by the UNIX user who started the administrator's session; the user can (but does not have to) be the `root` user.

Preconfigured Operator Report Types

Table 2-11 shows the types of reports that are preconfigured for HPOM operators. You can access operator reports by using the `call_sqlplus.sh` script.

Table 2-11 Preconfigured Reports for HPOM Operators

Report Name	Description
All Active Details	Detailed report on *all* active messages seen by the user who runs the report.
All Active Messages	Short report on *all* active messages seen by the user who runs the report.
All History Messages	Brief report on *all* history messages seen by the user who runs the report.
All History Details	Detailed report on *all* history messages seen by the user who runs the report.
All Pending Details	Detailed report on *all* pending messages seen by the user who runs the report.
All Pending Messages	Brief report on *all* pending messages see by the user who runs the report.
Sel. Active Details	Detailed report on selected active messages.
Sel. Active Message	Report on selected active messages.
Sel. History Details	Detailed history of selected (acknowledged) messages.
Sel. History Message	History of selected (acknowledged) messages.
Sel. Pending Details	Detailed report on selected pending messages.

Table 2-11 Preconfigured Reports for HPOM Operators (Continued)

Report Name	Description
Sel. Pending Messages	Brief report on selected pending messages.
HPOM Error Report	Review of the HPOM error logfile on the management server: `/var/opt/OV/log/System.txt` (Plain text) or `/var/opt/OV/log/System.bin` (Binary)[a]

a. For more information about the logfiles, see “Reporting Errors” on page 408.

Defining Customized Operator Reports

You can define customized operator reports by modifying the following file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/reports/<lang>/\
oper.rpts
```

Whenever an operator saves report output to a file without specifying an absolute path (starting with “/”), the file is stored in the operator’s UNIX working directory, which is defined by $HOME or `/tmp`, in that order. In addition, the file is owned by the operator’s UNIX user, not by opc_op, unless the operator logged in as UNIX user opc_op. The permissions of the file are determined by the umask.

Generating Statistical and Trend-analysis Reports

HPOM enables you to generate statistical and trend-analysis reports over a defined period of time. These reports can be configured to cover periods from as little as a few days to as much as weeks or even months.

NOTE The tool `/opt/OV/bin/OpC/opcdbmsgmv` moves all messages that are marked as acknowledged to the history-message tables in the database, where they are retained with little or no negative effect on operational tasks. Although automatically started every two hours by the HPOM control manager, `opcdbmsgmv` may also be called manually for troubleshooting purposes.

Report Security

To enhance report security, HPOM restricts database access, Net8 access, and web reporting capabilities. You can customize these security measures to match the particular needs of your organization.

Restricting Database Access

For report-writing tools, HPOM restricts database access to a single database user, **opc_report**. This user has read-only access. The opc_report user makes use of the Oracle report role **opc_report_role**. This report role is a kind of database user profile. You can use the role to enable additional users to access to the database so they can create reports using information in the HPOM database tables.

Restricting Net8 Access

To accept net connections, Net8 requires a listener process running on the database node. The listener process accepts connection requests from any legal database user. If you want to tighten security still further, there are products available (for example, from Oracle) that help improve general communication security in this area. For more information, see the Oracle product documentation.

Restricting Web Reporting

To restrict web reporting, HPOM requires you to place the web-reporting server on the same side of your firewall as the HPOM database server. Any other configuration is not supported.

Flexible Management Configuration

This section describes the conventions you use to set up flexible management with the example policies provided by HPOM. For more information about the HPOM flexible management environment, see the *HPOM Concepts Guide*.

Locations of Flexible Management Policies

HPOM provides a set of plain text policies you use to define the HPOM to configure and implement flexible management in a widely-distributed environment.

The plain text policies are located in the following directory:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs`

Types of Flexible Management Policies

Table 2-12 provides a brief description of each policy.

Table 2-12 Example Policies for HPOM Flexible Management

Policy Name	Description
`backup-server`	Defines the responsible managers for an HPOM backup server. If the HPOM primary server fails, management responsibility can be switched to a backup server. The policy defines two management servers: `M1` and `M2`. Management server `M2` can act as a backup server for management server `M1`.
`example.m2`	Combines follow-the-sun and service-oriented message distribution functions.
`example.m3`	Additional example policy for follow-the-sun functions.

Table 2-12 Example Policies for HPOM Flexible Management (Continued)

Policy Name	Description
`followthesun`	Defines the time policies and responsible managers for **HPOM follow-the-sun** responsibility switching. The policy defines three management servers: `M1`, (`M2`, and `M3`. These management servers can switch responsibility at different times of the day and week.
`hier.specmgr`	Provides an example of hierarchical management responsibility. SNMP traps are sent to the local management server. All other messages are sent to the primary management server.
`hier.time.all`	Provides an example of hierarchical management responsibility. Responsibility is switched between two servers according to a follow-the-sun time policy.
`hier.time.spec`	Provides an example of hierarchical management responsibility. SNMP traps are sent to the local management server. All other messages are sent to the primary management server according to a follow-the-sun time policy.
`hierarchy.agt`	Defines the responsible managers for hierarchical management responsibility switching for *all nodes*. The policy defines two management servers: `M1` and `MC`. `M1` is configured as the *primary manager* for all nodes. `MC` is configured as an *action-allowed manager* for all nodes.
`hierarchy.sv`	Defines the responsible managers for hierarchical management responsibility switching for *regional management servers*.
`msgforw`	Defines the responsible managers for manager-to-manager message forwarding. The policy defines the message-forwarding target rules.

Table 2-12 Example Policies for HPOM Flexible Management (Continued)

Policy Name	Description
`outage`	Defines the period of time in which a service is to be provided, or in which a system (for example, a database server) or service is scheduled to be unavailable.
`service`	Defines the responsible managers for **service-related message distribution** (for example, competence centers). The policy defines a local management server: `M1`. The policy also defines two examples of service centers: a database service center (`DBSVC`) and an application service center (`ASVC`).

Keywords for Flexible Management Policies

To define the various elements required in a flexible management configuration, HPOM uses the following keywords and definitions:

- ❏ `ACTIONALLOWMANAGERS`

  HPOM managers that are allowed to execute actions on the managed node. The action response (for example, command broadcast) is sent to this manager. Only the primary HPOM manager can configure action-allowed managers for an agent.

`ACTIONALLOWMANAGER`	Name of the manager allowed to execute actions on the managed node.
`NODE`	Node name of the action-allowed manager. You can use the variable `$OPC_PRIMARY_MGR` to specify that this node name is always the node name of the primary manager.
`DESCRIPTION`	Short description of the action-allowed manager.

- ❏ `CONDSTATUSVARS`

Conditions status variables, which enable (TRUE) or disable (FALSE) scheduled-outage conditions. For details, see “Status Variables for Conditions” on page 112.

- ❑ DESCRIPTION

  Short description of the manager.

- ❑ MSGTARGETRULES

  Message-target rules. The rules that define where messages are sent and who can work on the message.

  MSGTARGETRULE Rule to configure the message target conditions and the message target manager.

  DESCRIPTION Description of the message target rule.

- ❑ MSGTARGETMANAGERS

  Message-target manager. The name of the HP Operations manager to which the agents send HPOM messages, as well as the action responses to those HPOM messages. The result of an HPOM message is sent to only one HPOM manager.

  MSGTARGETMANAGER Message target manager. Management server to which you forward a message. Always specify the IP address of the target management server as **0.0.0.0**. The real IP address is then resolved by the domain name server (DNS).

  TIMETEMPLATE Time policy. Name of the time policy corresponding to the target manager. If the time condition is always true, you can use the variable $OPC_ALWAYS. If you use this keyword, message transfers to the target manager will *not* depend on the time.

  OPCMGR Node name of the target manager. You can use the keyword $OPC_PRIMARY_MGR to indicate that this will always be the primary manager.

  MSGCONTROLLINGMGR Message-controlling manager. Enables message target manager to switch control of a message.

  NOTIFYMGR Notify manager. Enables the message target manager to notify itself. This attribute is set by default if no attribute is defined for the message target manager.

`ACKNONLOCALMGR` Enables a message rule to force a direct acknowledgment of a notification message on a source management server.

- ❏ `MSGTARGETRULECONDS`

  Conditions for message-target rules.

  `MSGTARGETRULECOND` Condition that tells the agent to which management server to send specific messages. Messages are sent based on message attributes or time. The message agent evaluates the message target conditions by reading the file `mgrconf`. If the `mgrconf` file does not exist, the messages are sent to the management server name stored in the `primmgr` file. If the `primmgr` file does *not* exist, messages are sent according to instructions set using the `ovconfchg` command-line tool.

  `DESCRIPTION` Description of the message-target rule condition

  `SEVERITY` Severity level of the message, for example: Unknown, Normal, Warning, Minor, Major, or Critical.

  `NODE` <*node*> One or more node names or node groups, separated by spaces:

  - IP <*ipaddress*> or IP <*ipaddress*> <*string*>

    For example, `NODE IP 0.0.0.0 hpbbn`.

    If the node is defined using the format IP <*ipaddress*> or IP <*ipaddress*> <*string*>, you should use the IP address "0.0.0.0". The real IP address is then resolved by the domain name server (DNS).

  - NODEGROUP <*string*>

    For example, `NODEGROUP "maintenance"` specifies all nodes in the node group `maintenance`.

  For example, to specify multiple nodes and node groups:

`NODE IP 192.168.12.5 NODEGROUP "maintenance" IP 192.168.25.4 NODEGROUP "office"`

`NODEPATTERN` — Pattern matching can be used to match nodes. Note that pattern-matching is case insensitive. Two match types are possible:

- `IPPATTERN`:

  Pattern matching using IP address of a node. Example: `NODEPATTERN IPPATTERN "10.1.<*>"`.

- `NAMEPATTERN`:

  Pattern matching using the node name. Example: `NODEPATTERN NAMEPATTERN "testnode.<*>"`.

`APPLICATION` — Application name.

`MSGGRP` — Message group name.

`OBJECT` — Object name.

`MSGTYPE` — Description of the message type.

`MSGCONDTYPE` — Message condition type:

- Match:

  Condition is true if the specified attributes are matched.

- Suppress:

  Condition is true if the specified attributes are *not* matched.

`TEXT` — A string containing all or part of the message text. Pattern-matching may be used. Example: `TEXT "^Path: /[dir1|dir2]<_>[dir3|dir4]" SEPARATORS "/"`

`SERVICE_NAME` — A string containing the unique identifier of the service. Pattern-matching may be used. Example: `SERVICE_NAME "Service<*> [A|B]" ICASE`

`MSGOPERATION` — Message operation:

- Suppress
- Log-only
- Inservice

For details, see Table 2-13.

- ❑ `RESPMGRCONFIG`

  Responsible manager configuration

- ❑ `SECONDARYMANAGERS`

  Secondary HPOM managers of an agent. Each of these management servers have permission to take over responsibility and become the primary HPOM manager for an agent.

`SECONDARYMANAGER`	Name of the secondary manager
`NODE` *<node>*	Node name of the secondary manager
`DESCRIPTION`	Description of the secondary manager

Syntax for Flexible Management Policies

You can use the syntax described in the following sections as a basis for configuring flexible management features (for example, the switching of responsibility between managers) in the policy files provided.

For more information about the policy syntax for flexible management policies, refer to the reference pages *opcmom(4)* and *opcmomchk(1m)*, as well as the `README` file in the policy directory:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs`

Special Characters

The syntax examples below use the following special characters that you can use in flexible-management policies:

`e`	Empty string. If you want to include an empty string in a policy, enter `e`. Example: `e`

#	Comment. If you want to include a comment in a policy, include a pound sign (#) at the start of every line of the comment. Every character in the line is treated as part of the comment by HPOM. Example: # This is a comment
\	Escape character. If you want to use quotation marks in a syntax string, escape the quotation marks with a backslash (\). Example: `\"quotation\"`

Syntax for Responsible Manager Configuration Policies

Use the following syntax for responsible manager configuration policies:

```
respmgrconfigs ::= <respmgrconfigs> RESPMGRCONFIG DESCRIPTION
                   <string> <respmgrconds> | e
respmgrconds   ::= SECONDARYMANAGERS <secondmgrs>
                   ACTIONALLOWMANAGERS <actallowmgrs>
                   [MSGTARGETRULES <msgtargetrules>]
secondmgrs     ::= <secondmgrs> SECONDARYMANAGER NODE <node>
                   [DESCRIPTION <string>] | e
actallowmgrs   ::= <actallowmgrs> ACTIONALLOWMANGER
                   NODE <node>
                   [DESCRIPTION <string>] | e
msgtargetrules ::= <msgtargetrules> MSGTARGETRULE DESCRIPTION
                   <string> <msgtargetrule> | e
msgtargetrule  ::= MSGTARGETRULECONDS <mtrconditions>
                   MSGTARGETMANAGERS <msgtargetmgrs>
                   | MSGTARGETRULECONDS <mtrconditions>
                   MSGTARGETMANAGERS <msgtargetmgrs>
                   ACKNONLOCALMGR
mtrconditions  ::= <mtrconditions> MSGTARGETRULECOND
                   DESCRIPTION
                   <string> <mtrcond> | e
mtrcond        ::= <mtrcond> SEVERITY <severity> |
                   <mtrcond> NODE <nodelist> |
                   <mtrcond> APPLICATION  <string> |
                   <mtrcond> MSGGRP <string> |
                   <mtrcond> OBJECT <string> |
                   <mtrcond> MSGTYPE <string> |
                   <mtrcond> TEXT <pattern> |
                   <mtrcond> SERVICE_NAME  <pattern> |
                   <mtrcond> CMA NAME <string> |
```

```
                              VALUE <pattern> |
                   <mtrcond> MSGCONDTYPE  <msgcondtype> | e
                   <mtrcond> NODEPATTERN <nodepatternlist> |

severity        ::= Unknown | Normal | Warning | Critical |
                    Minor | Major
msgcondtype     ::= Match | Suppress
nodelist        ::= <node> | <nodelist> <node>
node            ::= IP <ipaddress> | IP <ipaddress> <string> |
                    NODEGROUP <string>
string          ::= "any alphanumeric string"
ipaddress       ::= <digits>.<digits>.<digits>.<digits>
```

Syntax for Time Policies

Use the following syntax for time policies:

```
timetmpls      ::= <timetmpls> TIMETEMPLATE <string>
                   DESCRIPTION
                   <string> <conditions> | e
conditions     ::= TIMETMPLCONDS <timetmplconds> | e
timetmplconds  ::= <timetmplconds> TIMETMPLCOND <timetmplcond>
timetmplcond   ::= [TIMECONDTYPE <timecondtype>] [TIME FROM
                   <time> TO <time>] [WEEKDAY <weekday>]
                   [DATE <exact_date>] | e
timecondtype   ::= Match | Suppress
time           ::= <hh>:<mm>
weekday        ::= ON <day> | FROM <day> TO <day>
exact_date     ::= ON <date> | FROM <date> TO <date>
day            ::= Monday | Tuesday | Wednesday | Thursday
                  | Friday | Saturday | Sunday
date           ::= <mm>/<dd>/<yyyy> |<mm>/<dd>/*|*/<dd>/*
```

NOTE The time policy is compared with the creation time of the message on the managed node. Message creation time is always defined in GMT.

Syntax for Switching Management Responsibility

Use the following syntax for policies that switch management server responsibility:

```
configfile := [TIMETEMPLATES <timetmpls>] RESPMGRCONFIGS
              <respmgrconfigs>
```

Syntax for Message-Target-Rules

Use the following syntax for policies that define message target rules:

```
msgtargetmgrs ::= <msgtargetmgrs> MSGTARGETMANAGER
                  TIMETEMPLATE <string> OPCMGR <node> |
                  <msgtargetmgrs> MSGTARGETMANAGER
                  TIMETEMPLATE <string> OPCMGR <node>
                  MSGCONTROLLINGMGR | <msgtargetmgrs>
                  MSGTARGETMANAGER TIMETEMPLATE <string>
                  OPCMGR <node> NOTIFYMGR | e
```

NOTE You can replace the <*string*> variable with `$OPC_ALWAYS` to specify that the time condition is always true. To specify that the current primary manager is always used as the message target server, replace the <*node*> variable with `$OPC_PRIMARY_MGR`.

Syntax for Message Operations

Use the following syntax for message operations policies:

```
msgoperations   ::=  <msgoperations> MSGOPERATION TIMETEMPLATE
                     <string> <msgoperation> |
                     <msgoperations> MSGOPERATION
                     <msgoperation> | e

msgoperation    ::=  INSERVICE|SUPPRESS|LOGONLY
```

Syntax for Service Hours and Scheduled Outages

Use the following syntax for policies that define service hours and scheduled outages:

```
configfile := [TIMETEMPLATES <timetmpls>]
              [CONDSTATUSVARS <statusvarsdef>]
              RESPMGRCONFIGS <respmgrconfigs>
```

Syntax for the declaration of condition-status variables:

```
statusvarsdef ::= <statusvarsdef> CONDSTATUSVAR
                  <string> <bool> | e
```

Syntax for the Time Policy:

```
timetmpls       ::= <timetmpls> TIMETEMPLATE <string>
                    DESCRIPTION <string> <timetmpldefs>
                    <conditions> | e
timetmpldefs    ::= TIMEZONETYPE <timezonetype>
                    TIMEZONEVALUE <string> | e
timezonetype    ::= Fix | Local
conditions      ::= TIMETMPLCONDS <timetmplconds> | e
timetmplconds1  ::= <timetmplconds> TIMETMPLCOND <timetmplcond>
timetmplcond    ::= [TIMECONDTYPE <timecondtype>] [TIME FROM
                    <time> TO <time>] [WEEKDAY <weekday>]
                    [DATE <exact_date>] | e
timecondtype    ::= Match | Unmatch
time            ::= <hh>:<mm>
weekday         ::= ON <day> | FROM <day> TO <day>
exact_date      ::= ON <date> | FROM <date> TO <date>
day             ::= Monday | Tuesday | Wednesday | Thursday
                   | Friday | Saturday | Sunday
date            ::= <mm>/<dd>/<yyyy> |<mm>/<dd>/*|*/<dd>/*
```

Syntax for service hours and scheduled outages:

```
respmgrconfigs  ::=  <respmgrconfigs> RESPMGRCONFIG2
                     DESCRIPTION
                     <string>  <respmgrconds>  |  e
respmgrconds    ::=  MSGTARGETRULES  <msgtargetrules>
msgtargetrules  ::=  <msgtargetrules> MSGTARGETRULE
                      DESCRIPTION  <string>
                      <msgtargetrule>  |  e
msgtargetrule   ::=  MSGTARGETRULECONDS  <mtrconditions>
                     MSGOPERATIONS  <msgoperations>
mtrconditions   ::=  <mtrconditions>  MSGTARGETRULECOND
                     DESCRIPTION   <string>  <mtrcond>  |  e
mtrcond         ::= <mtrcond>  CONDSTATUSVAR  <string>  |
                      <mtrcond> SEVERITY  <severity>  |
                      <mtrcond> NODE  <nodelist>  |
                      <mtrcond> APPLICATION  <string>  |
                      <mtrcond> MSGGRP  <string>  |
                      <mtrcond> OBJECT  <string>  |
                      <mtrcond> MSGTYPE  <string> |
                      <mtrcond> TEXT <pattern>   |
                      <mtrcond> SERVICE_NAME <pattern>   |
```

1. Outages only.
2. Only one RESPMGRCONFIG (responsible-manager configuration) is supported in scheduled outage configuration files.

```
                      <mtrcond> CMA NAME <string> |
                                VALUE <pattern> |
                      <mtrcond> MSGCONDTYPE <msgcondtype>  | e
                      <mtrcond> NODEPATTERN <nodepatternlist>
bool             ::=  True  | False
severity         ::=  Unknown  |  Normal  |  Warning
                      |  Critical | Minor   |  Major
msgcondtype      ::=  Match  |  Unmatch
nodelist         ::=  <node>  |  <nodelist>  <node>
node             ::=  IP  <ipaddress>  |  IP  <ipaddress>
                      <string> | NODEGROUP <string>
string           ::=  "any  alphanumeric  string"
ipaddress        ::=   <digits>.<digits>.<digits>.<digits>
```

NOTE You can replace the <*string*> variable with `$OPC_ALWAYS` to specify that the time condition is always true.

Policy Schedules

The policy for service hours and scheduled outages allows you to **suppress**, or buffer (**inservice**) messages that match certain conditions for defined time periods. You configure service hours and scheduled outages on the management server with a policy similar to the one used to configure flexible management.

A log-only message, also known as a server message, is processed on the HP Operations management server as follows:

- HPOM does *not* forward a copy of a log-only message to the Trouble-ticket interface.
- HPOM does *not* start any automatic actions associated with a log-only message.
- HPOM *does* use a log-only messages for message-correlation purposes. A log-only message can have message key relationships which are able to acknowledge messages from the browser of the active messages.

Syntax for Service Hours and Scheduled Outages Policies

The syntax used to configure service hours and scheduled outages is the same as that used to configure flexible management. The syntax for both may be checked with the `opcmomchk` tool. For more information about policy syntax, see "Syntax for Time Policies" on page 106 and "Syntax for Service Hours and Scheduled Outages" on page 107.

Location of Service Hours and Scheduled Outages Policies

When you are configuring service hours and scheduled outage policies, remember that HPOM expects to find files and templates in the following locations:

❏ Default files:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs/outage`

Central store for all the default templates and files associated with scheduled outages and service hours.

❏ Work files:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs`

Working area. Do not work on default templates and files. Before making any changes, copy the file to the working directory and modify the copy.

❏ Enabled files:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs`

When the modified configuration file is ready for use, move it to the `respmgrs` directory, where HPOM stores files that specify the currently enabled configuration. Start a new HPOM session if you want to force the management server to read and implement the new configuration.

NOTE You must not change the default names assigned to outage policies. HPOM looks for specific policy file names and performs actions depending on whether it finds them. For more information about how to set up configuration files for service hours and scheduled outages, see the "Syntax for Service Hours and Scheduled Outages" on page 107

Parameters for Service Hours and Scheduled Outages Policies

Table 2-13 on page 111 describes the parameters in the policy used to define service hours and scheduled outages.

Table 2-13 Parameters for Service Hours and Scheduled Policies

Parameter	Description
`INSERVICE`	Sends messages to the Pending Messages browser if the message condition matches but the time policy condition does *not* match. The messages remain in the Pending Messages browser remain until the **unbuffer** time condition is matched or until the message is unbuffered manually.
`LOGONLY`	Sends a matching messages to the History browser.
`SUPPRESS`	Deletes messages. Message-related actions triggered by the HPOM management server are *not* started if the SUPPRESS option is defined.

NOTE Scheduled outages and service hours may be configured by an external application. However, the designated external application must create the policy for outages and service hours and use the `opccfgout(1M)` command to control outages.

Parameters for Buffering Messages

Messages buffered in the Java GUI `Pending Messages Browser` are automatically moved to the `Message Browser` as soon as the specified buffer time expires. You can change this behavior by setting the value of the `OPC_AUTO_DEBUFFER` parameter using the `ovconfchg` command-line tool on the HP Operations management server to `FALSE`. In this case, messages remain in the `Pending Messages Browser`.

Forwarding Messages to a Trouble Ticket or Notification Interface

You can change the value of message attributes to do the following:

❑ Forward to a trouble-ticket service

❏ Forward to an external notification interface

In conjunction with the time policy, you can forward messages to a trouble ticket or notification interface according to time of day.

For example, set the following values in the service hours policy to forward messages to the Trouble Ticket interface:

```
MSGOPERATION TIMETEMPLATE "SLA_cust1" TROUBLETICKET True
MSGOPERATION TIMETEMPLATE "SLA_cust2" NOTIFICATION False
```

For more information on these and other variables, see "Syntax for Service Hours and Scheduled Outages" on page 107.

Status Variables for Conditions

Status variables for conditions allow you to enable and disable conditions dynamically. The conditions are used in conditions for message target rules, and must be declared at be *beginning* of the policy, *after* the TIMETEMPLATES values.

HPOM enables you to declare several variables for one condition, as well as declare one variable in several conditions. For example, an external interface can set the state of many conditions with one call.

The following abbreviated (. . .) example of a policy defining service hours sets the condition status variable for SAP to true:

```
TIMETEMPLATES
...
CONDSTATUSVARS
        CONDSTATUSVAR "sap" True
...
RESPMGRCONFIG
...
     MESSAGETARGETRULECONDS
        MESSAGETARGETRULECOND
           DESCRIPTION "Filter SAP messages"
           CONDSTATUSVAR "sap"
APPLICATION "Sap"
     MSGOPERATIONS
        MSGOPERATION
           INSERVICE
```

NOTE Status variables are persistent. They are not affected by the message manager stopping and restarting.

Time-Zone Strings

The creation time of an HPOM message is always defined in UTC, regardless of where in the world the managed node is located. As a result, HPOM messages contain an indication of the difference between UTC and the local time on the managed node. By tracking time in this way, the HP Operations management server is able to calculate the local time of the managed node that sent the message. The management server can then decide whether or not it is appropriate to act.

Service hours are usually defined in terms of the local time on the managed node. For example, a service provider uses the service hours policy to tell the HP Operations management server that managed nodes in various time zones must be supported between 08:00 and 16:00 local time. Policies for scheduled outages define time in terms of the local time on the server that provides the service that is scheduled to be unavailable. For example, the administrator of an HP Operations management server in the United Kingdom (UK) knows that a SAP server situated in eastern United States (U.S.) will be unavailable for maintenance reasons between 22:00 and 02:00 U.S. Easter Standard Time (EST).

The policies for scheduled outages and service hours on the HP Operations management server can contain a string that defines a fixed local time zone (for example, EST). The HP Operations management server uses the value of the time zone string and the time (in UTC) to calculate the fixed local time on the given management server for which an outage has been scheduled.

Time-Zone Syntax

The following example illustrates the syntax that is required for the time zone string:

```
TIMEZONETYPE Fix TIMEZONEVALUE "EST"
```

By default, HPOM evaluates time conditions for both service hours *and* scheduled outages by comparing the time frame defined for each condition to the time the message is received on the HP Operations management server.

Setting the Time-Zone Parameter

You can force the HP Operations management server to use the message creation time on the local managed node, rather than the message arrival time on the management server.

To specify the time-zone parameter for service hours or scheduled outages, set one of the following strings using the `ovconfchg` command-line tool:

❏ Service hours:

```
OPC_SERVHRS_USE_AGENT_TZ TRUE
```

❏ Scheduled outages:

```
OPC_OUTAGE_USE_CREATE_TIME TRUE
```

These strings force the HP Operations management server to apply the time frame for service hours and scheduled outages defined on the HP Operations management server (for example, 08:00 -- 16:00) as a sliding time frame for managed nodes in their respective local time zone.

NOTE Make sure the local time is correctly set on the managed node.

Command-Line Interface

The message manager does not automatically read the configuration policy for outages and service hours each time the policy file is modified (for example, by the system administrator or an external application).

You can use the command-line tool `opccfgout(1M)` to start the reconfigure request, as follows:

```
# opccfgout -update
```

Additional options allow you to set status variables for the conditions:

```
# opccfgout -set_cond <cond_stat_var> \
[-true|-false|-default]
```

To list the current status of the status variables, enter:

`# opccfgout -list_cond <cond_stat_var>|-all`

Message-Forwarding Policies

HPOM enables you to generate notification messages to be sent to remote management servers. You can also assign control of the messages to the source management server with same policy. You can check the validity of the syntax in the policy using the tool `opcmomchk`. For more information about the parameters and options available with the `opcmomchk` tool, refer to the `opcmomchk(1)` command.

HPOM stores the message-forwarding policy in the following location:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw`

NOTE For all flexible-management considerations, such as hosting several certificate servers, certificate handling for a second HP Operations management server, and so on, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

Configuring the Message-Forwarding Policy

Configuring the message forwarding policy includes the following:

❏ Message targets:

You can forward a message to one or more target server.

❏ Message control:

You can assign the attribute `MSGCONTROLLINGMGR` to target management servers to which you forward a message. This attribute enables the target servers to switch control of a message.

❏ Message notification:

You can assign the attribute `NOTIFYMGR` to target management servers to which you forward a message. This attribute enables the target server to send notifications to themselves.

❏ Message acknowledgement:

You can assign the attribute ACKNONLOCALMGR to messages. This attribute forces the source management server to acknowledge message notifications explicitly.

Message-Forwarding Policy Attributes

The message forwarding policy accepts any of the following message attributes in a message condition:

- OBJECT
- APPLICATION
- MSGGRP
- SEVERITY
- NODE
- MSGCONDTYPE

For more information about message attributes and how to configure them by means of the command-line interface, refer to the reference page *opcmom(4)*.

Message-Forwarding Policy Parameters

You can set several parameters to configure message forwarding on various target or source management servers. These parameters are required for the management of system and network resources. You can add the parameters with the ovconfchg command on each target management server. The value of the parameters must be set for each target manager.

NOTE The OPC_SOURCE_FORW_NOTIF_TO_TT parameter should be specified on the source management server, see Table 2-14.

Table 2-14 provides more information about these parameters, their default values, and a short description of the function of each parameter.

Table 2-14 **Message Forwarding Parameters**

Parameter Name	Default Value	Description
OPC_ACCEPT_CTRL_SWTCH_ACKN	TRUE	Accepts acknowledgment for control-switched messages from other management servers.
OPC_ACCEPT_CTRL_SWTCH_MSGS	TRUE	Accepts control-switched messages from other management servers.
OPC_ACCEPT_NOTIF_MSSGS	TRUE	Accepts notification messages from other management servers.
OPC_FORW_CTRL_SWTCH_TO_TT	TRUE	Forwards control-switch messages to a trouble ticket or a notification service.
OPC_SOURCE_FORW_NOTIF_TO_TT	TRUE	Forwards notification-planned messages to a trouble ticket or a notification service on a source server. Must be set on the source server
OPC_FORW_NOTIF_TO_TT	FALSE	Forwards notification messages to a trouble ticket or a notification service.

Table 2-14 Message Forwarding Parameters (Continued)

Parameter Name	Default Value	Description
OPC_ONE_LINE_MSG_FORWARD	FALSE	Controls forwarding in larger manager hierarchies.
OPC_SEND_ACKN_TO_CTRL_SWTCH	TRUE	Sends acknowledgements to control-switched messages.
OPC_SEND_ANNO_TO_CTRL_SWTCH	TRUE	Sends annotations to control-switched messages.
OPC_SEND_ANNO_TO_NOTIF	TRUE	Sends annotation to notification messages.
OPC_SEND_ANT_TO_CTRL_SWTCH	TRUE	Sends action-related data to control-switched messages.
OPC_SEND_ANT_TO_NOTIF	TRUE	Sends action-related data to notification messages.

Message Target Rules

Message-target rules define the management server to which specific messages are sent based on the time of day, date, and message attribute conditions. HPOM provides a set of plain text policies, which you can copy and edit to define Flexible Management features. You can find the example files and policies in the following directory:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs`

Defining Message-Target Rules

To define message-target rules, perform the following steps:

1. Open the appropriate responsible-management policy file.
2. Find the section header `MSGTARGETRULES`.

3. Define the message conditions in the subsection, `MSGCONDTYPE`. You can define the following conditions: Match and Suppress
4. Define the message attributes in the subsection, `MSGTARGETRULES`. You can define the following attributes: application, custom message attribute, message group, message type, message text, node, node pattern, object, service name, severity.
5. Define the message-target manager, according to the time policy used, in the subsection, `MSGTARGETMANAGER`.
6. Save and close the modified policy file.
7. Run the HPOM policy validation tool `opcmomchk(1)` on the finished configuration file to make sure that any additions or changes changes are valid:

   ```
   # /opt/OV/bin/OpC/opcmomchk <file_name>
   ```

   For more information about required syntax and permitted parameters, refer to the reference page *opcmomchk(1)*.
8. As user root, copy the validated file to the configuration directory `respmgrs` as follows:

   ```
   # cp <file_name> \
   /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs
   ```

9. To activate the configuration, use the `ovconfchg` utility without any options:

   ```
   # /opt/OV/bin/ovconfchg
   ```

HTTPS-Based Event Forwarding

HPOM uses HTTPS-based communication to forward events in a flexible management environment. HTTPS-based event forwarding establishes a higher level of security for the communication between management servers in an HPOM environment.

Enabling HTTPS-based Forwarding

To enable HTTPS-based event forwarding, you must establish a trust relationship between the HP Operations management servers that will be communicating directly.

For more detailed information about how to set up a trust relationship between HP Operations management servers, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

To disable HTTPS-based event forwarding, set the parameter to false.

For faster HTTPS-based event forwarding set the configuration setting OPC_DONT_FORW_MSGKEY_ACK to TRUE:

```
# ovconfchg -ovrg server -ns opc -set\
OPC_DONT_FORW_MSGKEY_ACK TRUE
```

In this case, the acknowledge and annotation add change events caused by message key relations are not forwarded. If the target server has the same messages, it already handles the same message key relation. If this flag is not set to TRUE (by default), the correlation is performed twice, which may lead to lock time-outs and duplicate annotations.

Configuring HTTPS-Based Forwarding

Although the default values will be adequate for most needs, you can reconfigure HTTPS-based message forwarding to suit your needs.

The parameters listed in Table 2-15 on page 120 let you configure different aspects of event forwarding. See "Message-Forwarding Configuration Parameters" on page 121 for more information about each parameter.

Table 2-15 Event Forwarding Configuration Parameters

Parameter Name	Default value	Description
MAX_DELIVERY_THREADS	10	Maximum number of delivery threads
MAX_INPUT_BUFFER_SIZE	100000	Maximum size of the internal input buffer (bytes)
MAX_FILE_BUFFER_SIZE	0 (unlimited)	Maximum size of the buffer file on disk (bytes)
BUFFER_PATH	/var/opt/OV/share/\ tmp/OpC/mgmt_sv/snf	Directory for buffering files
REQUEST_TIMEOUT	3600	Time after which a request time-outs and will not be delivered to remote servers (seconds)

Message-Forwarding Configuration Parameters

`MAX_DELIVERY_THREADS`

Determines the maximum number of delivery threads that the forward manager will create when using HTTPS-based message forwarding. It is recommended to leave this variable at its default value, unless your environment contains a large number of servers to which messages are forwarded and you experience performance problems with forwarding.

`MAX_INPUT_BUFFER_SIZE`

Determines the size of the memory buffer used by the forward manager (in bytes). There is no need to change this value, unless issues with the delivery of very large messages occur.

`MAX_FILE_BUFFER_SIZE`

Determines the maximum size of the buffer file on a disk, used by the forward manager to store messages that are to be delivered to remote HP Operations management servers that are currently inaccessible. Increase this value if you expect frequent communication failures between HP Operations management servers and usually transfer large amounts of messages.

`BUFFER_PATH`

Determines the location of the directory in which the forward manager stores buffer files. Change this location only if you experience loss of messages and need to place the buffer files on a file system with more disk space.

`REQUEST_TIMEOUT`

Time limit after which undeliverable messages and message operations are discarded. Increase this value if you expect frequent communication failures that last longer than one hour.

Changing Parameter Values

The parameters listed in Table 2-15 on page 120 are located in the `opc.opcforwm` namespace. To change their values, use the `ovconfchg` command line tool.

For example, if you want to limit the size of the buffer file on the disk to 200000 bytes, use the following command:

```
# ovconfchg -ovrg server -ns opc.opcforwm -set \
MAX_FILE_BUFFER_SIZE 200000
```

After changing the value of the parameters, restart the HPOM server.

To check the current values of the HTTPS-based forwarding parameters, use the following command:

```
# ovconfget -ovrg server opc.opcforwm
```

Note that only the non-default values are displayed.

Troubleshooting Message Forwarding Problems

If you need to remove all buffered messages, perform the following steps:

1. Stop the HP Operations management server processes:

   ```
   # ovc -stop OPC
   ```

2. Remove the directory in which the forwarding manager stores buffered files:

   ```
   # rm -rf /var/opt/OV/share/tmp/OpC/mgmt_sv/snf
   ```

3. Start the HP Operations management server processes:

   ```
   # ovc -start OPC
   ```

Time Policies

A time policy consists of the following:

- Policy name
- Time conditions

Each time condition defines a specific time period. This time period contains definitions of the time, day, date, or any combination of the three. The local time zone is always used to evaluate the policy.

NOTE When specifying a time, use the 24-hour clock notation. For example, for "1:00 p.m." enter `13:00`. HPOM time inputs are interpreted as hh:mm:00. For example, if you want to specify a 24 hour time period ending at midnight, enter:

00:00–24:00

Specifying a notification time period of 00:00–23:59 for every day would mean that any message being received after 23:59:00 and before 00:00:00 would not create notification. When setting time values for the Scheduled Action Policy, you leave time unspecified. The scheduled action is executed repeatedly at one minute intervals. Wildcard characters are not recognized.

Example Time Policies

The following examples show various ways to specify time formats in the time policies:

- ❏ Time:

  If you do not specify a particular time, day of the week, or year, HPOM assumes that you want the condition to be true for 24 hours, from 00:00 to 24:00, every day of the year.

  HPOM requires you set up a time policy for the message target rules even if the scheduled action does not depend on time. You can use the variable `OPC_ALWAYS` to configure time policies when the condition is always true.

- ❏ Day or date:

  If you specify a condition, HPOM assumes the conditions exist continually for the day or date specified:

  - Day:

    If you specify only Tuesday, HPOM will evaluate the condition as true every Tuesday, from 00:01 to 23:59, throughout the year, every year. Use the syntax:

    ```
    WEEKDAY ON Tuesday
    ```

  - Date:

Specifying January 1 and nothing else will match a condition every January 1st of every year. Use the syntax:

```
DATE ON 01/01/*
```

- ❏ Time periods:

  You can set time periods:

  - Time:

    To set a time period from 7:00 to 17:00, use the syntax:

    ```
    TIME FROM 7:00 TO 17:00
    ```

  - Day:

    To set a time period from Monday to Friday, use the syntax:

    ```
    WEEKDAY FROM Monday TO Friday
    ```

  - Date:

    To set a time period from the year 2005 to 2010, use the syntax:

    ```
    DATE FROM 01/01/2005 TO 12/31/2010
    ```

  - Date and time:

    To set a time on December 31 2008, from 23:00 to 23:59, use the syntax:

    ```
    TIME FROM 23:00 TO 23:59 DATE ON 12/31/2008
    ```

  If you include the day of the week (for example, Monday April 1, 2008), HPOM cross-checks the day and date you have entered to make sure that they match the calendar. If they do not match, however, the action will not be correctly completed. HPOM does not issue an error message.

- ❏ Wildcards (*)

  You can set dates or periods using a wildcard character (`*`):

  - Specific date:

    To set a condition for December 1st every year, use the syntax:

    ```
    DATE ON 12/01/*
    ```

  - Time period:

To set a condition from August 6th to September 10th every year, use the syntax:

```
DATE FROM 08/06/* TO 09/10/*
```

NOTE

Although syntactically correct, HPOM cannot handle mixed conditions such as: `DATE FROM 05/07/08 TO 10/10/*`.

For further examples of time policies, see the following:

- ❑ Manuals:

  See "Syntax for Time Policies" on page 106.

- ❑ Reference pages:

  Refer to the *opcmom(4)* reference page.

- ❑ The default flexible-management templates directory:

  `/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs`

  See the default template files in the `tmpl_respmgrs` directory. If you want to use any of the template files, make a copy of the default file in the working directory (`work_respmgrs`) and modify the new copy.

NOTE

HP-UX Only: To correct time differences between the different time resources used by the HPOM C-routines, the `TIMEZONE` variable must be set on the appropriate managed nodes. If not, messages can be sent to the wrong management server as they are processed using the incorrect time.

Keywords in Time Templates

To define the various elements required in a flexible-management configuration, HPOM uses the following keywords and definitions:

`DESCRIPTION`	Describes the scope of time template.
`TIMETEMPLATE`	Defines the name of the time template; the name itself is specified in, for example, <*string*>.
`TIMETMPLCONDS`	Defines a time period, which can include one or more time intervals specified in time conditions (`TIMETMPLCOND`).
`TIMETMPLCOND`	Defines a single time interval. Several time conditions together comprise a time period. A time condition allows you to use combinations of day, date, and time to define a time period.
`TIMECONDTYPE`	Defines the type of time condition, which determines what to do with messages that arrive inside or outside the defined time period. Use one of the following for the definition: • *Match*: If the current time is within the defined time period, forward *matching* messages to the Message Browser. • *Suppress*: If the current time is outside the defined time period ignore or delete *suppressed* messages.
`TIME`	Specifies a time period. Set the variable <*time*> using the format: `FROM <time> TO <time>`, where <time> is specified in the format: <*hh*:*mm*> The variable `FROM <time>` must appear before the time variable `TO <time>`, for example: `FROM 18:00 TO 24:00`, or `FROM 22:00 TO 06:00`).
`WEEKDAY`	Specifies a day of the week, for example: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday. The required syntax is: • `ON <day>` Specifies the day of the week (`ON Sunday`).

- `FROM <day> TO <day>`

  Specifies the time period (`FROM Monday TO Wednesday`).

`DATE` Specifies the date. The date must have one of the following formats:

`<MM>/<DD>/<YYYY>`

`<MM>/<DD>/<YY>`

`<MM>/<DD>/*`

HPOM does not verify that the time period is valid. For example, `10/35/*` is not recognized as an invalid date.

You specify the date as follows:

`ON <date>`

`FROM <date>`

`TO <date>`

Example Flexible-Management Policies

This section provides a number of example policies that illustrate a simple implementation of selected flexible-management features. In this section you can find examples of the following flexible-management configurations:

- ❏ “Management Responsibility Switch” on page 127
- ❏ “Follow-the-Sun Responsibility Switch” on page 129
- ❏ “Multiple Subnet Management” on page 131
- ❏ “Message Forwarding between Management Servers” on page 132
- ❏ “Service-Hour Schedules” on page 133
- ❏ “Scheduled Outage Configuration” on page 133

Management Responsibility Switch

The following example policy switches management responsibility from one HPOM management server to another.

```
#
# Configuration file
# /etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/f887818
# and managed node hptest with
# the IP address 15.136.120.24 (= f887818 in hex notation)
#
TIMETEMPLATES
    TIMETEMPLATE "shift1"
        DESCRIPTION "Time Template 1"
        TIMETMPLCONDS
            TIMETMPLCOND
                TIMECONDTYPE Match
                TIME FROM 10:00 TO 14:00
                WEEKDAY FROM Monday TO Friday
            TIMETMPLCOND
                TIMECONDTYPE Match
                TIME FROM 17:00 TO 24:00
                WEEKDAY FROM Monday TO Friday
    TIMETEMPLATE "shift2"
        DESCRIPTION "Time Template 2"
        TIMETMPLCONDS
            TIMETMPLCOND
                TIMECONDTYPE Match
                TIME FROM 6:00 TO 18:00
                WEEKDAY FROM Monday TO Friday
                DATE 1/1/95
RESPMGRCONFIGS
    RESPMGRCONFIG
        DESCRIPTION "responsible mgrs for agents in Europe"
        SECONDARYMANAGERS
            SECONDARYMANAGER
                NODE IP 0.0.0.0"hptest.bbn.hp.com"
                DESCRIPTION "Boeblingen"
            SECONDARYMANAGER
                NODE IP 0.0.0.0 "hpsystem.bbn.hp.com"
                DESCRIPTION "Boeblingen gateway"
        ACTIONALLOWMANAGERS
            ACTIONALLOWMANGER
                NODE IP 0.0.0.0 "hptest.bbn.hp.com"
                DESCRIPTION "Boeblingen"
            ACTIONALLOWMANGER
                NODE IP 0.0.0.0 "hpsystem.bbn.hp.com"
                DESCRIPTION "Boeblingen gateway"
            ACTIONALLOWMANGER
                NODE IP 0.0.0.0 "$OPC_PRIMARY_MGR"
                DESCRIPTION "HPOM primary manager"
```

```
    MSGTARGETRULES
        MSGTARGETRULE
            DESCRIPTION "other messages"
            MSGTARGETRULECONDS
            MSGTARGETMANAGERS
                MSGTARGETMANAGER
                    TIMETEMPLATE "shift2"
                    OPCMGR NODE IP 0.0.0.0 "system.aaa.bb.com"
```

Follow-the-Sun Responsibility Switch

The following example policy defines follow-the-sun responsibility switching.

```
#
# Time-template configurations for follow-the-sun functions
#
# Three responsible managers are used in this example
TIMETEMPLATES
        # time template 1
        TIMETEMPLATE "shift1"
        DESCRIPTION "Time Template 1 "
        # Time template for shift1
        # this include the time from 17:00 to 24:00  and from
        # 0:00 to 6:00
        # on the weekday Monday to Friday
           TIMETMPLCONDS
               TIMETMPLCOND
                  TIME FROM 0:00 TO 6:00
                  WEEKDAY FROM Monday TO Friday
               TIMETMPLCOND
                  TIME FROM 17:00 TO 24:00
                  WEEKDAY FROM Monday TO Friday
        TIMETEMPLATE "shift2"
        DESCRIPTION "Time Template 2 "
        # Time template for shift2
        # this includes the time from 6:00 to 17:00
        # on the weekday Monday to Friday
           TIMETMPLCONDS
               TIMETMPLCOND
                  TIME FROM 6:00 TO 17:00
                  WEEKDAY FROM Monday TO Friday
        # time template 3
        TIMETEMPLATE "shift3"
        DESCRIPTION "Time Template 3 "
        # Time template for shift3
```

```
        # include the time from 0:00 to 24:00 (all day)
        # on the weekday Saturday and Sunday
           TIMETMPLCONDS
               TIMETMPLCOND
                  TIME FROM 0:00 TO 24:00
                  WEEKDAY FROM Saturday TO Sunday
#
# Responsible Manager Configurations for follow the sun
# functionality
#
RESPMGRCONFIGS
   RESPMGRCONFIG
   DESCRIPTION "responsible managers M1 "
      SECONDARYMANAGERS
         SECONDARYMANAGER
            NODE IP 0.0.0.0 "M1"
            DESCRIPTION "secondary manager M1"
         SECONDARYMANAGER
            NODE IP 0.0.0.0 "M2"
            DESCRIPTION "secondary manager M2"
         SECONDARYMANAGER
            NODE IP 0.0.0.0 "M3"
            DESCRIPTION "secondary manager M3"
      ACTIONALLOWMANAGERS
         ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 "M1"
            DESCRIPTION "action allowed manager M1"
         ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 "M2"
            DESCRIPTION "action allowed manager M2"
         ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 "M3"
            DESCRIPTION "action allowed manager M3"
      MSGTARGETRULES
         MSGTARGETRULE
         DESCRIPTION "target rule description "
            MSGTARGETRULECONDS
            # for all messages
            MSGTARGETMANAGERS
               MSGTARGETMANAGER
               # target manager from 17:00 to 24:00
               # and 00:00 to 6:00
               # from Monday to Friday
                  TIMETEMPLATE "shift1"
                  OPCMGR IP 0.0.0.0 "M1"
               # target manager from 6:00 to 17:00
```

```
# from Monday to Friday
MSGTARGETMANAGER
   TIMETEMPLATE "shift2"
   OPCMGR IP 0.0.0.0 "M2"
# target manager on the whole weekend
MSGTARGETMANAGER
   TIMETEMPLATE "shift3"
   OPCMGR IP 0.0.0.0 "M3"
```

Multiple Subnet Management

If you are using an HP Operations management server that manages multiple subnets through multiple ethernet interfaces, you should distribute the appropriate `mgrconf` file to the managed nodes in subnets to support this setup environment. The following example can be used as a template:

```
RESPMGRCONFIGS
        RESPMGRCONFIG
        DESCRIPTION "responsible mgrs for <server_name>"
                SECONDARYMANAGERS
                        SECONDARYMANAGER
                        NODE <IP_address_1> "<server_name_1>"
                        DESCRIPTION         "first_IP_address"
                        SECONDARYMANAGER
                        NODE IP <IP_address_2> "<server_name_2>"
                        DESCRIPTION         "second_IP_address"
                ACTIONALLOWMANAGERS
                        ACTIONALLOWMANAGER
                        NODE IP <IP_address_1> "<server_name_1>"
                        DESCRIPTION         "first_IP_address"
                        ACTIONALLOWMANAGER
                        NODE IP <IP_address_2> "<server_name_2>"
                        DESCRIPTION         "second_IP_address"
```

Where the meaning of the above stated selectors is as follows:

- *<server_name_1>* is the name the management server uses for the first subnet.

- *<server_name_2>* is the name the management server uses for the second subnet.
- *<IP_address_1>* is the IP address the management server uses for the first subnet.
- *<IP_address_2>* is the IP address the management server uses for the second subnet.

IMPORTANT Your DNS server must properly resolve all hostnames and IP addresses that belong to the management server.

Message Forwarding between Management Servers

The following example policy defines message forwarding between management servers.

If you install the policy on a server named *Source*, that server Source performs the following actions:

1. Forwards messages to expert center

   Forward messages assigned to the message group `DATABASE` to a database expert center (dbexpert) and pass control of the message to the expert center. The Source server also informs a second server (dbnotify). Finally, the Source server causes the message to be acknowledged directly on the local HPOM server.

2. Informs treasury server

   Inform a treasury server (Treasury) about messages that concern financial and CAD applications.

3. Informs master server

   Inform a master server (Master) about critical messages coming from nodes x1 and x2.

```
RESPMGRCONFIGS
       RESPMGRCONFIG
        DESCRIPTION "msg-forwarding target specification"
                MSGTARGETRULES
                     MSGTARGETRULE
                     DESCRIPTION "application appl"
                          MSGTARGETRULECONDS
                             MSGTARGETRULECOND
```

```
    DESCRIPTION "no condition"
MSGTARGETMANAGERS
   MSGTARGETMANAGER
      TIMETEMPLATE "$OPC_ALWAYS"
    OPCMGR IP 0.0.0.0 "ligety.bbn.hp.com"
     MSGCONTROLLINGMGR
  MSGTARGETMANAGER
     TIMETEMPLATE "$OPC_ALWAYS"
    OPCMGR IP 0.0.0.0 "moses.bbn.hp.com"
      MSGCONTROLLINGMGR
```

Service-Hour Schedules

The following example policy defines service hours for a SAP server with the node name saparv01. This node must be in service on weekdays from 08:00 hours to 16:00 hours.

```
TIMETEMPLATES
   # time template
   TIMETEMPLATE "service hours"
   DESCRIPTION "template match for service hours"
      TIMETMPLCONDS
          TIMETMPLCOND
             TIME FROM 08:00 TO 16:00
             WEEKDAY FROM Monday TO Friday

RESPMGRCONFIGS
   RESPMGRCONFIG
   DESCRIPTION "Define service hours for a SAP server"
      MSGTARGETRULES
          MSGTARGETRULE
          DESCRIPTION "Buffer msg outside service hrs for SAP"
             MSGTARGETRULECONDS
                MSGTARGETRULECOND
                DESCRIPTION "Node with SAP server"
                NODE IP 0.0.0.0 "sapsrv01"
             MSGOPERATIONS
                MSGOPERATION
                TIMETEMPLATE "service hours"
                INSERVICE
```

Scheduled Outage Configuration

The following example policy defines a scheduled outage that suppresses all messages relating to the application oracle from node sapsrv01.

```
CONDSTATUSVARS
   CONDSTATUSVAR "ora_on_sapsrv01" False
RESPMGRCONFIGS
   RESPMGRCONFIG
   DESCRIPTION "define outage for oracle on node orasv01"
      MSGTARGETRULES
         MSGTARGETRULE
         DESCRIPTION "outage for oracle on node orasv01"
            MSGTARGETRULECONDS
               MSGTARGETRULECOND
               DESCRIPTION "Node with oracle server"
               CONDSTATUSVAR "ora_on_sapsrv01"
               NODE IP 0.0.0.0 "sapsrv01"
               APPLICATION "oracle"
            MSGOPERATIONS
               MSGOPERATION
               SUPPRESS
```

HPOM Variables

This section lists and defines the variables that can be used with HPOM, and gives an output example, where appropriate. Each variable is shown with the required syntax.

Types of Variables Supported by HPOM

HPOM supports the following types of variables:

❏ Environment variables:

  Variables for the shell environment. These variables can be set before starting HPOM.

❏ Configuration variables:

  Variables for configuring the HP Operations management server and HTTPS agents.

❏ Variables in all message-source policies:

  Variables must be enclosed with angle brackets. If the HPOM agents cannot resolve a variable, the variable itself is displayed in the GUI.

❏ Variables in instruction-text interface calls:

  Variables can be used when calling the instruction text interface in the Java-based operator GUI

❏ Variables in application calls and the user interface:

  Variables can be used when calling applications or issuing a broadcast command, or can be passed to external programs. Do not use angle brackets with these variables.

NOTE It is also often useful to enclose the variable in quotes (““), especially if the variable might return a value that contains spaces.

HPOM and User-Defined Variables

HPOM and user-defined variables can be used to compose messages, or can be passed as parameters to action calls. They can also be passed to external applications, by using the instruction text interface. Note that HPOM variables are reserved words that cannot be used for any other purpose, for example, creating user-defined variables.

A variable is defined simply by assigning a matched string to it. Variables must be delimited by the use of angle brackets (<>).

The following example shows a user-defined variable, error_text followed by an HPOM variable `$MSG_APPL`, used for obtaining the name of the application associated with the message:

`/tmp/example_command <`*`error_text`*`> <$MSG_APPL>`

Personal Environment Variables

You can set personal environment variables in the `.dtprofile` file, which resides in the home directory of the UNIX user whose variables you want to change or set.

Setting Personal Environment Variables

To define and set personal environment variables, use the `.dtprofile` file located in the home directory of the logged-in UNIX user, as follows:

1. Edit the user-session configuration file:
   `<`*`HomeDirectory`*`>/.dtprofile`
2. Add lines to the file to set the environment variable

The desktop accepts either `sh` or `ksh` syntax for the commands in this file. The commands should only be those that set environment variables; do not enter commands that perform terminal input and output (I/O), for example: **`tset`** or **`stty`**.

NOTE By default, the desktop session manager does *not* read the files `<`*`HomeDirectory`*`>/.profile` and `<`*`HomeDirectory`*`>/.login` as they could contain terminal I/O based commands that are inappropriate for a graphical interface. To ensure that all the lines in the .profile and .login files *are* read, remove the comment from the last line of the .dtprofile so that it reads DTSOURCEPROFILE=true.

The desktop automatically sets the following environment variables for each user:

DISPLAY	Set to the value of the first field in the Xservers file.
EDITOR	Set to the desktop default editor.
HOME	Set to the user's home directory, as specified in the file: /etc/passwd.
KBD_LANG	Set to the value of $LANG for some languages .
LANG	Set to the display's current NLS language (if any).
LC_ALL LC_MESSAGES	Set to the value of $LANG.
LOGNAME	Set to the user name.
MAIL	Set to /var/mail/$USER.
PATH	Set to the value of the Dtlogin “userPath” resource.
USER	Set to the user name.
SHELL	Set to the user's default shell, as specified in the file: /etc/passwd.
TERM	Set to dtterm.
TZ	Set to the system's zone or to the value of the Dtlogin “timeZone” resource.

Environment Variables

You can use the following environmental variables before starting HPOM.

$OPC_BRC_HISTSIZE

Returns the value of the environment variable for the length of the user’s broadcast command history. The default number of commands saved is 128 per user. Example: `export OPC_BRC_HISTSIZE=512`

Configuration Variables

For a complete list of the HPOM server configuration variables, see the *HPOM Server Configuration Variables*.

HPOM provides an automatic synchronization of the most configuration variables after a change of the HPOM configuration. Most configuration variables used in server processes (`opcdispm`, `opcmsgm`, `ovoareqsdr`, `opcforwm`, `opcactm`, `opcttnsm`) are updated automatically each time the `ovconfchg` command is used.

Some configuration varialbes used in the server processes are exceptions and are not always synchronized. The configuration variables that represent file and path names, queues and pipes names, port ranges, and pid files are rather set at process startup and are not usually synchronized automatically. However, the variables for the file names of the following configuration files are synchronized automatically:

- Outage policy:

  `OPC_OUTAGE_TEMPLATE` (default: `outage`)
- Message forward policy:

  `OPC_MSG_FORW_TEMPLATE` (default: `opcforw`)
- MSI conf. file:

  `OPC_MSI_CONF` (default: `msiconf`)
- Remote action filter conf. file:

  `OPC_ACTSEC_FILTER` (default: `remactconf.xml`)

The following configuration variables are set only at startup and are never updated online:

- `OPCMSGM_USE_GUI_THREAD`
- `OPC_OPCCTLM_START_OPCSVCAM`
- `_M_ARENA_OPTS`
- `_M_SBA_OPTS`

The following configuration variables have a specific behavior:

`OPC_RQS_NUM_AGT_WORKERS`	Updated online, only if the value is increased.

`OPC_BBCDIST_RETRY_INTERVAL`	Might not update till the end of the previous interval.

Variables in Message-Source Policies

You can use the following variables in most text entry fields (exceptions are noted) for logfiles, the HPOM interface, the threshold monitor, and the SNMP trap policy. You can use the variables within HPOM, or pass them to external programs. To ensure correct processing, you must enter the variables with the angle brackets. For details on policy body grammar, see the *HPOM Concepts Guide*.

`<$MSG_APPL>`

Returns the name of the application associated with the message. This variable cannot be used in logfile policies.

Sample output:

`/usr/bin/su(1) Switch User`

`<$MSG_GEN_NODE>`

Returns the IP address of the node from which the message originates.

Sample output:

`14.136.122.123`

`<$MSG_GEN_NODE_NAME>`

Returns the name of the node on which from which the message originates.

Sample output:

`richie.c.com`

`<$MSG_GRP>`

Returns the default message group of the message.

Sample output:

`Security`

`<$MSG_ID>`

Returns the unique identity number of the message, as generated by the message agent. Suppressed messages do not have message IDs.

Sample output:

`6e998f80-a06b-71d0-012e-0f887a7c0000`

`<$MSG_NODE>`

Returns the IP address of the node on which the event took place.

Sample output:

`14.136.122.123`

`<$MSG_NODE_ID>`

Returns the name of the node on which the event took place.

Sample output:

`richie.c.com`

This variable is only available in the `Service Name` field.

`<$MSG_NODE_NAME>`

Returns the name of the node on which the event took place. This is the name returned by the node's name service.

Sample output:

`richie.c.com`

`<$MSG_OBJECT>`

Returns the name of the object associated with the event. This is set for the `SNMP` policy. This variable cannot be used in logfile policies. The variable returns the default object, not the object set in the conditions window.

<$MSG_SERVICE>

Returns the service name associated with the message. This variable can also be used for automatic and operator-initiated actions.

Sample output:

`Application_Server`

<$MSG_SEV>

Returns the default value for the severity of the message. This is set for the `Logfile` and OPCMSG policies.

Sample output:

`Normal`

<$MSG_TEXT>

Returns the original text of the message. This is the source text that is matched against the message text pattern in each condition. This variable returns an empty string when used in threshold monitor policies.

Sample output:

`SU 03/19 16:13 + ttyp7 bill-root`

<$MSG_TIME_CREATED>

Returns the time the message was created in seconds since January 1, 1970.

Sample output:

`950008585`

<$MSG_TYPE>

Returns the default name set for Message Type. This name is set with the keyword `MSGTYPE` in the policy body.

<$OPTION(N)>

Returns the value of an optional variable that is set by opcmsg or opcmon (for example, `<$OPTION(A)>` `<$OPTION(B)>`, and so on). To find out how to set this variable, refer to the *opcmsg(1)* or *opcmon(1)* reference pages.

NOTE The `$OPTION` variable cannot contain double quotes. Use single quotes instead.

Variable Resolution in HPOM

The variables used in HPOM can take one of several values, depending on the incoming message, default policy configuration or the configuration of the condition that the variables are matching. HPOM resolves the variable according to a specific order of priority.

Understanding Variable Resolution

HPOM calculates and sets the value of a variable according to the following order:

1. Use the value set by the external source (API/executable, event, and so on). For example, the `opcmsg` command with the following options to assign the value APP to the variable `<$MSG_APPL>`:

   ```
   # opcmsg app=APP object=O msg_text="Message text"
   ```

2. If the variable cannot be set by external sources, use a value generated by HPOM, for example, message ID.
3. If none of the above is valid for a variable, HPOM uses the value set in the policy body for which the variable is evaluated. If there is no default value set, set the value of the variable to 0 (zero) or leave it empty, depending on its type.

Note that HPOM adheres strictly to the specified order when resolving variable values. For example, if a value for `<$MSG_OBJECT>` is set by an external source (step 1), a default value set in step 3 is ignored.

Variables for Actions Only

The following variables can only be used in the `Node` field of *operator-initated actions*, except for the variable `<$OPC_MGMTSV>` which can be used in all fields.

The variables `<$OPC_MGMTSV>`, `<$OPC_GUI_CLIENT>` and `<$OPC_GUI_CLIENT_WEB>` must be entered with angle brackets.

The variables must not be part of a string or be nested.

`$OPC_ENV(env variable)`

Returns the value of the environment variable for the user who has started HPOM. This variable is only available for operator-initiated actions. It is resolved in the action call.

Sample output:

`PATH, NLS_LANG, EDITOR, SHELL, HOME, TERM`.

For example, if `SHELL` is set to `/usr/bin/ksh` and you have set up the operator-initiated action `echo $OPC_ENV(SHELL)`, the following command will be executed as operator initiated action: `echo /usr/bin/ksh`.

`<$OPC_GUI_CLIENT>`

Executes the application or action on the client where the Java-based GUI is currently running.

This variable is resolved differently, depending on whether the GUI client is running on a UNIX-based system with DNS or on a PC using Microsoft Windows Internet Name Service (WINS). If you are using WINS, `<$OPC_GUI_CLIENT>` returns the WINS hostname.

`<$OPC_MGMTSV>`

Returns the name of the current HP Operations management server. This variable can be used in all fields related to actions.

Sample output:

`richie.c.com`

<$OPC_GUI_CLIENT_WEB>

Starts a web browser on the client where the Java-based GUI is currently running.

This variable is resolved differently, depending on whether the GUI client is running on a UNIX-based system with DNS or on a PC using MS WINS (Windows Internet Name Service). If you are using WINS, `<$OPC_GUI_CLIENT_WEB>` returns the WINS hostname.

$OPC_USER

Returns the name of the HPOM user who is currently logged in on the management server. This variable is only available for operator-initiated actions. It is resolved in the action call.

Sample output:

`opc_adm`

Variables for Logfile Encapsulator Policies Only

You can use the following variables for most text entry fields in logfile policies. You can use the variables within HPOM, or pass them to external programs.

<$1>

Policies of Windows Event Log type. Returns one or more of the possible parameters that are part of a Windows event (for example, `<$1>` returns the first parameter, `<$2>` returns the second parameter, and so on.)

<$EVENT_ID>

Policies of Windows Event Log type. Returns the event ID of the Windows event. `<$EVENT_ID>` simplifies the processing of multi-line EventLog messages. You need the `Source` field and `<$EVENT_ID>` of the event to identify the event uniquely.

Sample output:

`0x0000600F`

`<$LOGFILE>`

Returns the name of the monitored logfile.

Sample output:

`sulog`

`<$LOGPATH>`

Returns the full path to the monitored logfile including the file name.

Sample output:

`/var/adm/sulog`

Variables for Threshold Monitor Policies Only

You can use the following variables in most text entry fields (exceptions are noted) of threshold monitor policies. You can use the variables within HPOM, or pass them to external programs.

`<$NAME>`

Returns the name of a threshold monitor. This name is set in the `Monitor Name` field of the `Add/Modify Monitor` window. This variable cannot be used in the `Monitor Program or MIB ID` field.

Sample output:

`cpu_util`

`<$THRESHOLD>`

Returns the value set for a monitor threshold. This value is set in the `Threshold:` field in the `Condition No.` window.

Sample output:

`95.00`

`<$VALAVG>`

Returns the average value of all messages reported by the threshold monitor.

Sample output:

`100.00`

`<$VALCNT>`

Returns the number of times that the threshold monitor has delivered a message to the browser.

Sample output:

`1`

`<$VALUE>`

Returns the value measured by a threshold monitor.

Sample output:

`100.00`

Variables for SNMP Trap Policies Only

You can use the following variables in most entry fields (exceptions are noted) for SNMP trap text. You can use the variables within HPOM, or pass them to external programs.

`<$#>` Returns the number of variables in an enterprise-specific SNMP trap (generic trap 6 Enterprise specific ID).

Sample output:

`2`

`<$*>` Returns all variables assigned to the trap.

Sample output:

`[1] .1.1 (OctetString): arg1 [2] .1.2 (OctetString): kernighan.c.com`

`<$@>` Returns the time the event was received as the number of seconds since the Epoch (January 1, 1970) using the *time_t* representation.

Sample output:

`859479898`

`<$1>` Returns one or more of the possible trap parameters that are part of an SNMP trap (for example, `<$1>` returns the first variable, `<$2>` returns the second variable, and so on).

<$\>1>

Returns all attributes greater than *n* as *value* strings, which are useful for printing a variable number of arguments. <$\>0> is equivalent to $* without sequence numbers, names, or types.

Sample output:

richie.c.com

<$\>+1>

Returns all attributes greater than *n* as *name:value* string.

Sample output:

.1.2: richie.c.com

<$+2>

Returns the *n*th variable binding as *name:value*. This variable is not valid in the command field.

Sample output:

.1.2: richie.c.com

<$\>-n>

Returns all attributes greater than *n* as *[seq] name (type): value* strings.

Sample output:

[2] .1.2 (OctetString): kernighan.c.com

<$-2>

Returns the *n*th variable binding as *[seq] name-type:value*. This variable is not valid in command field.

Sample output:

[2] .1.2 (OctetString): richie.c.com

<$A>

Returns the node which produced the trap.

Sample output:

richie.c.com

<$C>

Returns the community of the trap.

Sample output:

public

<$E>

Returns the enterprise ID of the trap.

Sample output:

`private.enterprises.hp.nm.openView.hpOpenView`

`<$e>` Returns the enterprise object ID.

Sample output:

`.1.3.6.1.4.1.11.2.17.1`

`<$F>` Returns the textual name of the remote machine where the pmd is running, if the event was forwarded.

Sample output:

`kernighan.c.com`

`<$G>` Returns the generic trap ID.

Sample output:

`6`

`<$N>` Returns the event name (textual alias) of the event format specification used to format the event, as defined in the Event Configurator.

Sample output:

`OV_Node_Down`

`<$O>` Returns the name (object identifier) of the event.

Sample output:

`private.enterprises.hp.nm.openView.hpOpenView.0.58916872`

`<$o>` Returns the numeric object identifier of the event.

Sample output:

`.1.3.6.1.4.1.11.2.17.1`

`<$R>` Returns the true source of the event. This value is inferred through the transport mechanism that delivered the event.

Sample output:

`kernighan.c.com`

`<$r>` Returns the implied source of the event. This may not be the true source of the event if the true source is proxying for another source, such as when a monitoring application running locally is reporting information about a remote node.

Sample output:

`richie.c.com`

`<$S>` Returns the specific trap ID.

Sample output:

`5891686`

`<$s>` Returns the event's severity.

Sample output:

`Normal`

`<$T>` Returns the trap time stamp.

Sample output:

`0`

`<$V>` Returns the event type, based on the transport from which the event was received. Currently supported types are SNMPv1, SNMPv2, SNMPv2C, CMIP, GENERIC, and SNMPv2INFORM.

Sample output:

`SNMPv1`

`<$X>` Returns the time the event was received using the local time representation.

Sample output:

`17:24:58`

`<$x>` Returns the date the event was received using the local date representation.

Sample output:

`03/27/97`

Variables in Scheduled-Action Messages

You can use the following variables in the `Scheduled Action - Start/Success/Failure Message` windows of scheduled action policies. You can use the variables within HPOM, or pass them to external programs.

`<$PROG>` Returns the name of the program executed by the scheduled action policy.

Sample output:

`opcsv`

`<$USER>` Returns the name of the user under which the scheduled action was executed.

Sample output:

`root`

Variables for Instruction-Text Interface Calls

The following variables can only be used in instruction text interface calls executed on the Java-based operator GUI.

`<LOCAL_ON_JAVA_CLIENT>`

Starts a program or script on the client where the Java-based GUI is currently running as a result of the instruction text interface call.

For example, to start Microsoft Internet Explorer on the Java GUI client, use the following with the `INSTR_INTERF_CALL` argument in the file used as input to the `opcinstr` command line tool:

```
<LOCAL_ON_JAVA_CLIENT> "C:\Program Files\
Internet Explorer\IEXPLORE.EXE"
```

`<LOCAL_ON_JAVA_CLIENT_WEB>`

Starts a web browser on the client where the Java-based GUI is currently running as a result of the instruction text interface call.

For example, to start a web browser on the Java GUI client at the URL `http://www.hp.com`, use the following with the `INSTR_INTERF_CALL` argument in the file used as input to the `opcinstr` command line tool:

```
<LOCAL_ON_JAVA_CLIENT_WEB>
http://www.hp.com
```

Depending on the configuration of the Java GUI workspace, either the embedded or an external web browser is started.

For information about the command-line interface to the instruction-text interface, refer to the *opcinstrif(1m)* reference page.

Variables in Application Calls and the User Interface

You can use the following variables listed in most application text entry fields (exceptions are noted) of the GUI. You can use the variables within HPOM, or pass them to external programs.

`$OPC_ENV(env variable)`

Returns the value of the environment variable for the user who has started HPOM.

Sample output:

`PATH, NLS_LANG, EDITOR, SHELL, HOME, TERM.`

`$OPC_EXT_NODES`

Returns the node pattern of all external nodes that are selected at the time the application is executed. The names are separated by spaces.

`$OPC_MSG_NODES`

Returns the names of all nodes on which the events that generated currently selected messages took place. The names are separated by spaces. The nodes do not need to be in the node bank. If the same message is selected in more than one of these browsers, the duplicate selections is ignored. In the HPOM Java-based GUI, only nodes of the messages currently selected in the topmost browser are returned.

Sample output:

`kernighan.c.com richie.c.com`

`$OPC_MSG_GEN_NODES`

Returns the names of all nodes from which currently selected messages were sent by HPOM agents. The names are separated by spaces. The nodes do not need to be in the node bank. If the same message is selected in more than one of these browsers, the duplicate selections are ignored. In the HPOM Java-based GUI, only nodes of the messages currently selected in the topmost browser are returned.

Sample output:

`kernighan.c.com richie.c.com`

`$OPC_MSG_IDS`

Returns the Message IDs (UUIDs) of the messages currently selected in one ore more open Message Browsers. If the same message is selected in more than one browser, the duplicate selections are ignored. In the HPOM Java-based GUI, only Message IDs of the messages currently selected in the topmost browser are returned.

Sample output:

```
85432efa-ab4a-71d0-14d4-0f887a7c0000
a9c730b8-ab4b-71d0-1148-0f887a7c0000
```

`$OPC_MSGIDS_ACT`

Returns the Message IDs (UUIDs) of the messages currently selected in the Active/All and any HP Software Message Browsers. If the same message is selected in more than one of these browsers, the duplicate selections are ignored. In the HPOM Java-based GUI, only Message IDs of the messages currently selected in the topmost browser are returned.

Sample output:

```
85432efa-ab4a-71d0-14d4-0f887a7c0000
a9c730b8-ab4b-71d0-1148-0f887a7c0000
```

`$OPC_MSGIDS_HIST`

Returns the Message IDs (UUID) of the messages currently selected in the History Message Browser. In the HPOM Java-based GUI, only Message IDs of the messages currently selected in the topmost browser are returned.

Sample output:

```
edd93828-a6aa-71d0-0360-0f887a7c0000
ee72729a-a6aa-71d0-0360-0f887a7c0000
```

`$OPC_MSGIDS_PEND`

Returns the Message IDs (UUID) of the messages currently selected in the Pending Messages Browser. In the HPOM Java-based GUI, only Message IDs of the messages currently selected in the topmost browser are returned.

Sample output:

```
edd95828-ac2a-71d0-0360-0f887a7c0000
ee96729a-ada9-71d0-0360-0f887a7c0000
```

`$OPC_NODES`

Returns the names of all regular nodes that are selected at the time the application is executed. The names are separated by spaces. The nodes do not need tot be in the node bank. Nodes can be selected directly in a submap of the IP Map.

Sample output:

```
kernighan.c.com richie.c.com
```

`$OPC_USER`

Returns the name of the HPOM user who is currently logged in on the management server.

Sample output:

```
opc_adm
```

Variables for Applications Started from the Java-based GUI

The following variables can only be used in applications started from the Java-based operator GUI.

`$OPC_CUSTOM[`*name*`]`

Returns the value of the custom message attribute name. For example, the variable `$OPC_CUSTOM[device]` could return the value `Lan`.

`$OPC_EXACT_SELECTED_NODE_LABELS`

Returns the labels of all nodes and node groups that are selected at the time the application is executed. The names are separated by spaces.

`$OPC_GUI_CLIENT`

Executes the application or action on the client where the Java-based GUI is currently running. This variable is resolved differently, depending on whether the GUI client is running on a UNIX-based system with DNS or on a PC using MS WINS (Windows Internet Name Service). If you are using WINS, `$OPC_GUI_CLIENT` returns the WINS hostname.

`$OPC_GUI_CLIENT_WEB`

Starts a web browser on the client where the Java-based GUI is currently running. This variable is resolved differently depending on whether the GUI client is running on a UNIX-based system with DNS or on a PC using MS WINS (Windows Internet Name Service). If you are using WINS, `$OPC_GUI_CLIENT_WEB` returns the WINS hostname.

`$OPC_NODE_LABELS`

Returns the labels of all nodes in the node tree that are selected at the time the application is executed. The names are separated by spaces.

Message-Related Variables in the Java-Based Operator GUI

This section describes message-related variables:

❑ "Parameters for Message-related Variables" on page 155

❑ "Examples of Message-Related Variables" on page 164

Parameters for Message-related Variables

There are a few variables that return `TRUE` or `FALSE`, depending on the existence of a specific message attribute. For example, if an automatic action is defined, `TRUE` is returned. Otherwise, `FALSE` is returned.

If an attribute is empty, an empty string is returned. If you use an attribute that does not exist, it is treated like part of a normal string, which means no evaluation happens and the string remains unchanged.

The data returned from variables is exactly the same type as that shown in the `Message Properties` dialog box.

The indexing for word extraction from strings and for access to specific annotations starts with 1, not with 0.

`$OPC_MSG.ACTIONS.AUTOMATIC`

Indicates whether or not an automatic action is defined.

Sample output:

`TRUE`

`$OPC_MSG.ACTIONS.AUTOMATIC.ACKNOWLEDGE`

If an automatic action has been configured to provide an acknowledgement for the selected message, and the actions have been successfully completed, this variable returns `yes`. Otherwise, `no` is returned.

Sample output:

`yes`

`$OPC_MSG.ACTIONS.AUTOMATIC.ANNOTATION`

If this variable returns `yes`, an automatic action provides annotations for the selected message. If the action fails, an annotation will always be written.

Sample output:

`yes`

`$OPC_MSG.ACTIONS.AUTOMATIC.COMMAND`

Returns the script or program, including its parameters, performed as an automatic action for the selected message.

Sample output:

`dist_del.sh 30 warning`

`$OPC_MSG.ACTIONS.AUTOMATIC.NODE`

Returns the node on which an automatic action has been performed for the selected message.

Sample output:

`kernighan.c.com`

`$OPC_MSG.ACTIONS.AUTOMATIC.STATUS`

Returns the current status of the message's automatic action. The variable can return `running`, `failed`, or `successful`.

Sample output:

`successful`

`$OPC_MSG.ACTIONS.OPERATOR`

Indicates whether an operator-initiated action is defined.

Sample output:

`TRUE`

`$OPC_MSG.ACTIONS.OPERATOR.ACKNOWLEDGE`

If an operator-initiated action has been configured to provide an acknowledgement for the selected message, and the actions have been successfully completed, this variable returns `yes`. Otherwise, `no` is returned.

Sample output:

`yes`

`$OPC_MSG.ACTIONS.OPERATOR.ANNOTATION`

If this variable returns `yes`, an operator-initiated action provides annotations for the selected message. Note, if the action fails, an annotation will always be written.

Sample output:

`yes`

`$OPC_MSG.ACTIONS.OPERATOR.COMMAND`

Returns the script or program, including its parameters, performed as an operator-initiated action for the selected message.

Sample output:

`ps -ef`

`$OPC_MSG.ACTIONS.OPERATOR.COMMAND[n]`

Returns the *n*th parameter of the script or program, performed as an operator-initiated action for the selected message.

Sample output:

`-ef`

`$OPC_MSG.ACTIONS.OPERATOR.NODE`

Returns the node on which an operator-initiated action has been performed for the selected message.

Sample output:

`kernighan.c.com`

`$OPC_MSG.ACTIONS.OPERATOR.STATUS`

Returns the current status of the message's operator-initiated action. The variable can return `running`, `failed`, or `successful`.

Sample output:

`successful`

`$OPC_MSG.ACTIONS.TROUBLE_TICKET.ACKNOWLEDGE`

This variable can return the following values:

`yes`—The message was automatically acknowledged after having been forwarded to a trouble-ticket system.

`no`—The message was not acknowledged after having been forwarded to a trouble-ticket system.

Sample output:

`yes`

`$OPC_MSG.ACTIONS.TROUBLE_TICKET.STATUS`

This variable can return the following values:

`yes`—The message was forwarded to a trouble-ticket system.

`no`—The message was not forwarded to a trouble-ticket system.

Sample output:

`yes`

`$OPC_MSG.ANNOTATIONS`

Indicates whether or not annotations exist for a message. Returns `TRUE` if at least one annotation exists for a message. Otherwise, `FALSE` is returned.

Sample output:

`TRUE`

`$OPC_MSG.ANNOTATIONS[n]`

Returns the *n*th annotation.

Sample output:

```
Performed Message Correlation;
Message Key Relation:
Message 59d06840-ac4f-71d5-1f67-0f887e320000
with condition id
fe00fa34-9e34-71d5-143e-0f887e320000 ackn'ed
0 messages.
```

`$OPC_MSG.APPLICATION`

Returns the name of the application related to the selected message.

Sample output:

```
/usr/bin/su(1) Switch User
```

`$OPC_MSG.ATTRIBUTES`

This variable can return the following values:

`unmatched`—The message did not match any message conditions.

—The message was not originally displayed in the message browser.

Sample output:

```
unmatched
```

`$OPC_MSG.CREATED`

Returns the date and time the message was created on the managed node.

Sample output:

```
09/18/08 18:08:08
```

`$OPC_MSG.DUPLICATES`

Returns the number of duplicate messages that have been suppressed.

Sample output:

`17`

`$OPC_MSG.GROUP`

Returns the message group to which the selected message belongs.

Sample output:

`Security`

`$OPC_MSG.INSTRUCTIONS`

Returns the text of the instruction.

Sample output:

```
Available space on the device holding the /
(root) filesystem is less than the configured
threshold. This may lead to ...
```

`$OPC_MSG.LAST_RECEIVED`

Returns the date and time when the last duplicate message was received on the management server.

Sample output:

`09/16/08 03:17:23`

`$OPC_MSG.MSG_KEY`

Returns the message key that is associated with a message.

Sample output:

`my_appl_down:kernighan.c.com`

`$OPC_MSG.MSG_ID`

Returns the unique identification number for the selected message.

Sample output:

`217362f4-ac4f-71d5-13f3-0f887e320000`

`$OPC_MSG.NO_OF_ANNOTATIONS`

Returns the number of annotations of a message.

Sample output:

`3`

`$OPC_MSG.NODE`

Returns the managed node from which the selected message was issued.

Sample output:

`kernighan.c.com`

`$OPC_MSG.NODES_INCL_DUPS`

Returns the managed node from which the selected message was issued, including duplicate node names for multiple messages from the same node.

Sample output:

`kernighan.c.com richie.c.com richie.c.com`

`$OPC_MSG.OBJECT`

Returns the object which was affected by, detected, or caused the event.

Sample output:

`CPU`

`$OPC_MSG.ORIG_TEXT`

Returns the original text of the selected message.

Sample output:

`SU 09/18 18:07 + 6 root-spooladm`

`$OPC_MSG.ORIG_TEXT[`*n*`]`

Returns the *n*th word in the original text of the message.

Sample output:

`the`

`$OPC_MSG.OWNER`

Returns the owner of the selected message.

Sample output:

`opc_op`

`$OPC_MSG.RECEIVED`

Returns the date and time the message was received on the management server.

Sample output:

`09/18/08 18:08:10`

`$OPC_MSG.SERVICE`

Returns the service name that is associated with the message.

Sample output:

```
VP_SM:Agent:ServicesProcesses@@kernighan.c.co
m
```

`$OPC_MSG.SERVICE.MAPPED_SVC_COUNT`

Returns the number of service names in messages that are mapped to this message.

Sample output:

`3`

`$OPC_MSG.SERVICE.MAPPED_SVC[`*n*`]`

Returns the name of the *n*th service name in this message.

Sample output:

`SAP:applsv01`

`$OPC_MSG.SERVICE.MAPPED_SVCS`

Returns all service names in messages mapped by this message. The names are separated by spaces.

Sample output:

`SAP:applsv01 SAP:applsv02`

`$OPC_MSG.SEVERITY`

Returns the severity of the message. This can be `Unknown`, `Normal`, `Warning`, `Minor`, `Major`, or `Critical`.

Sample output:

`Normal`

`$OPC_MSG.SOURCE`

Returns the name of the application or component that generated the message.

Sample output:

`Message:opcmsg(1|3)`

`$OPC_MSG.TEXT`

Returns the complete text of the selected message.

Sample output:

```
The following configuration information was
successfully distributed:

Templates          (OpC30-814)
```

`$OPC_MSG.TEXT[`*n*`]`

Returns the *n*th word in the text of the message text.

Sample output:

`following`

`$OPC_MSG.TIME_OWNED`

Returns the date and time when the message was acknowledged.

Sample output:

`09/18/08 18:11:10`

`$OPC_MSG.TYPE`

Returns the message type of the message.

Sample output:

`ECS`

Examples of Message-Related Variables

This section contains examples of messages-related variables and parameters you can use to perform daily tasks.

- ❏ Message attributes:

  You can access all message attributes with the following variable:

  $OPC_MSG.ATTRIBUTES

  All you would need to do is add an attribute name.

  For example, to get text of a message, you would use the following:

  $OPC_MSG.TEXT

  Also when working with attributes that represent strings, you can access a specific word.

  For example, to get the fourth word in the text of a message, you would use the following:

  $OPC_MSG.TEXT[4]

  Annotations are an exception to this rule. In annotations, an index specifies the annotation that are returned.

  For example, you would access the seventh annotation of the current selected messages with the following:

  $OPC_MSG.ANNOTATIONS[7]

- ❏ Duplicate messages:

  If you need to find information about the number of message duplicates for an application, use the following:

  $OPC_MSG.DUPLICATES

- ❏ Creation time and severity:

  If want to do some use time and severity to do som statistical calculations, you would specify the message creation time and the severity, as follows:

  $OPC_MSG.CREATED

  $OPC_MSG.SEVERITY

- Message text:

  If you have defined a policy condition that creates a message text with some status as the third word, and you would like to extract this status easily and forward it to an application called `evaluate_status`, you would use the following:

  `evaluate_status $OPC_MSG.TEXT[3]`.

- Action attributes:

  If you want to use and evaluate action attributes, you could write shell scripts that check for automatic and operator-initiated actions, and get more information about their status and if they are annotated:

  `script_name` **`$OPC_MSG.ACTIONS.AUTOMATIC`**

  `script_name` **`$OPC_MSG.ACTIONS.AUTOMATIC.STATUS`**

  `script_name` **`$OPC_MSG.ACTIONS.AUTOMATIC.ANNOTATION`**

  The first parameter would be `TRUE` if an automatic action was defined for the message. This script would be useful only if there are more attributes used afterwards, but not to check for every attribute if it is an empty string.

- Annotations:

  To access the second annotation of a selected message in an application, you would use the following:

  `$OPC_MSG.ANNOTATIONS[2]`

3 HPOM Managed Node Configuration

In this Chapter

This chapter describes how to install and update the HP Operations Manager (HPOM) configuration on the managed nodes. The information in this chapter covers the following topics:

HPOM Agent-Configuration Distribution

After customizing the configuration and assigning policies to managed nodes, distribute the agent configuration to the managed nodes again using the `opcragt` command. If no configuration change has been made since the last configuration distribution, no new distribution is triggered unless you use the `-force` option. For more information about command options and parameters, refer to the *opcragt (1M)* reference page.

Instrumentation Distribution

This section contains the general recommendations before distributing commonly used instrumentation data to the managed nodes. You can call this data as automatic actions, operator-initiated actions, or scheduled actions. It can also be used by the monitoring agent and log file encapsulator.

Before You Distribute Instrumentation Data

Before you distribute instrumentation data to the managed nodes, review the following distribution requirements and tips.

Distribution Requirements

HPOM distributes instrumentation data only if one of the following is true:

❏ Deployment status:

Instrumentation files are available on the management server but are not yet deployed on the managed node.

❏ Available versions:

Instrumentation files available on the management server are newer than those already deployed to the managed node.

Distribution Tips for All Systems

To reduce network traffic and speed up distribution, follow these guidelines:

❏ Commonly used binaries:

Put only commonly used binaries to the instrumentation data location on the HPOM management server. Choose the appropriate location considering the criteria provided with your chosen distribution method. For more information, see “Distribution Methods” on page 172.

- ❏ Customized binaries:

  If you need a certain binary to be present only on specific systems, place this binary at an appropriate location under the category you have created for this purpose (see “Before You Distribute Instrumentation Data” on page 178 for more information). For description of categories and the distribution method based on them, see “Category-Based Distribution of Instrumentation” on page 174.

- ❏ Distribution process:

  If too many distribution requests are to be proceeded by the distribution process `opcbbcdist`, the other HPOM services (for example, the message manager) can be slowed down. By default, `opcbbcdist` handles 10 requests in parallel and the number of threads can be controlled using the OPC_MAX_DIST_REQS configuration setting.

  To avoid performance problems, do the following:

  - Do not configure all managed nodes at one time:

    Minimize the number of managed nodes getting new configuration data at the same time:

    — Distribute configuration to only a few nodes at a time by using the `opcragt` command.

    — Set a low number for maximum distribution requests by using the `ovconfchg` command as illustrated in the following example:

    ```
    /opt/OV/bin/ovconfchg -ovrg server -ns opc -set\
    OPC_MAX_DIST_REQS 3
    ```

  - Reduce the process priority of `opcbbcdist`:

    Use the `renice(1)` command to reduce the process priority of `opcbbcdist` on the management server.

  - Use category-based distribution method or selective distribution feature of `opcbbcdist`:

    Prevent distribution of the particular configuration files which are not needed on a specific node by choosing the category-based distribution method or the Selective Distribution feature of `opcbbcdist`.
    See “Category-Based Distribution of Instrumentation” on

page 174 for more information about categories. For details on Selective Distribution Feature, see “Selective Distribution to Managed Nodes” on page 185.

Distribution Methods

HPOM provides several different ways of distributing data to the managed nodes. The most appropriate distribution method depends on not only on the scope of the data you want to distribute but also on the selection of managed nodes to which you want to distribute the data. For example, you can distribute the complete instrumentation to a number of managed nodes or selected parts of the instrumentation to one, particular managed node.

Distributing All Instrumentation

To distribute all instrumentation data to all specified managed nodes, choose one of the following methods. Note that it is recommended to distribute instrumentation by category:

❏ Distribution based on instrumentation category:

For more information about distributing instrumentation based on categories, see the following sections:

1. “Category-Based Distribution of Instrumentation” on page 174.
2. “Before You Distribute Instrumentation Data” on page 178.

❏ Distribute from instrumentation directories:

For more information about distributing instrumentation directly from the directories in which the instrumentation is located, see the following section:

1. “Distribution of Instrumentation to Managed Nodes” on page 182.

Distributing Selected Instrumentation

To distribute only specific files to a particular managed node, choose one of the following methods. Note that it is recommended to distribute instrumentation by category:

❏ Distribute instrumentation to managed nodes based on *categories*. For more information, see the following sections:

1. “Category-Based Distribution of Instrumentation” on page 174.

2. “Before You Distribute Instrumentation Data” on page 178.

- Distribute selected instrumentation files to selected managed nodes. For more information, see the following section:

1. “Selective Distribution to Managed Nodes” on page 185.

Category-Based Distribution of Instrumentation

This section describes the distribution of instrumentation to managed nodes based on **categories**. An instrumentation category is a concept used to group related instrumentation files in logical units.

The possibility to group the instrumentation files into categories simplifies their distribution to the particular managed nodes. Customized scripts and programs can be grouped in a category, for example, `Custom`, which is then assigned to the specific managed nodes. Upon distribution, these scripts and programs are deployed only to the managed nodes to which the category is assigned to.

It is possible to deploy only the specified files to managed nodes because of the multi-level directory structure inside the categories. Each category can contain the specific instrumentation files in its directory substructure, as described in the "Instrumentation-Data Directory Structure" section.

Category information is stored in the HPOM database, and can be managed simultaneously in the file system and on the database level by means of the `opcinstrumcfg` command-line utility. Refer to the *opcinstrumcfg(1M)* reference page for more information about command options and parameters.

For the information about the category-related database tables, refer to *HPOM Reporting and Database Schema*. For Category Configuration API details, refer to *HPOM Developer's Reference*.

Instrumentation-Data Directory Structure

The instrumentation data is organized differently according to whether it is deployed on the HPOM management server or the managed node. For more information about the locations where HPOM deploys instrumentation data, see the following sections:

- "Instrumentation on the HPOM Management Server" on page 175
- "Instrumentation Data on the HPOM Managed Nodes" on page 177

Instrumentation on the HPOM Management Server

The directory for executable files on the HP Operations management server is located in:

`/var/opt/OV/share/databases/OpC/mgd_node/`

When you create the categories for the instrumentation files, inside the `instrumentation` directory is automatically created its multilevel subdirectory structure where the instrumentation files, organized within categories, are configured for the distribution.

NOTE All instrumentation data placed within `/var/opt/OV/share/databases/OpC/mgd_node/` are deployed, including the contents of the `monitor`, `actions`, and `cmds` directories. However, if there are files in `monitor`, `actions`, and `cmds` with the same names as files within the created categories, the files organized in categories are distributed in preference to the files in the `monitor`, `actions`, and `cmds` directories.

The subdirectory structure under the `instrumentation` directory can be either of the following:

- ❑ `$InstrumDir/`*<category>*`/`*<OS_family>*`/`*<OS_type>*`/\`
  <cpu_type>`/`*<OS_version>*
- ❑ `$InstrumDir/`*<category>*`/`*<OS_family>*`/`*<OS_type>*`/\`
  <OS_version>`/`*<cpu_type>*

The following list explains the selectors used in the instrumentation directories structure:

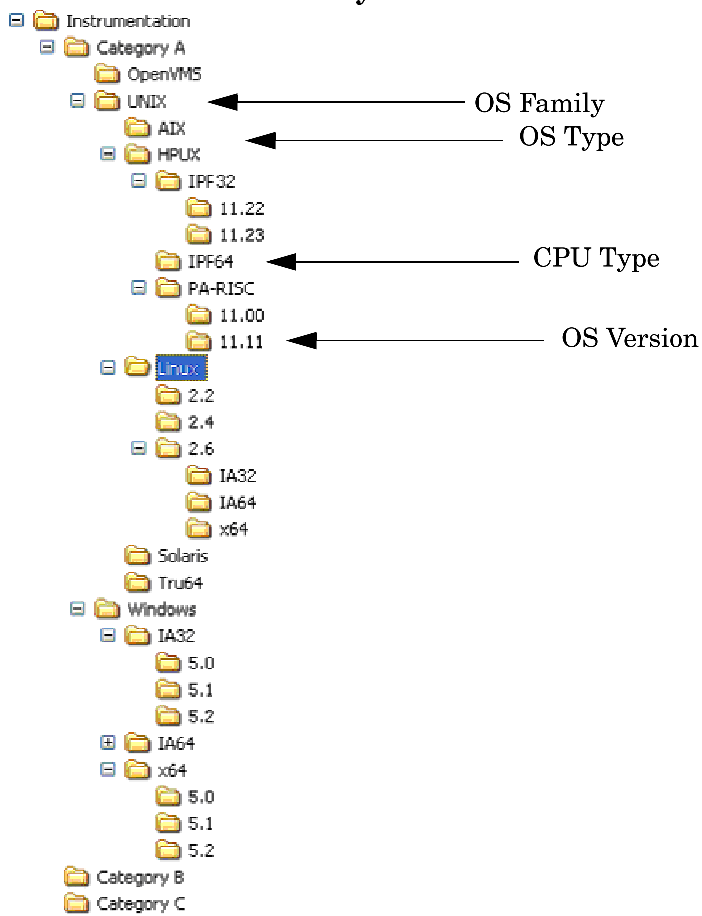
`$InstrumDir`	`/var/opt/OV/share/databases/OpC/mgd_node/\` `instrumentation`
<OS_family>	Unix, Windows
<OS_type>	Windows, Linux, HP-UX, Solaris, AIX, and OpenVMS Both Windows and OpenVMS combine the OS Family and OS type into a single directory level. For example, `$InstrumDir/`*<category>*`/Windows/X86/...` and *not* `$InstrumDir/`*<category>*`/Windows/Windows/...`

<cpu_type>	IPF32, IPF64, x64, x86, PA-RISC, SPARC, PowerPC, and Alpha
<OS_version>	All agent OS versions supported by HPOM 9.0x. Refer to *HPOM Software Release Notes* for more information. The following mapping is used for the OS versions in the Microsoft Windows family: • Windows 2000 = 5.0 • Windows XP = 5.1 • Windows 2003 = 5.2 • Windows Vista = 6.0 • Windows 2008 = 6.0 • Windows 2008r2 = 6.1 • Windows 7 = 6.1

NOTE The OS version directory can reside under the *<OS_type>* or *<cpu_type>* directory. However, if there is no *specific* instrumentation data for a certain agent OS version, the corresponding subdirectory is not created in the file system.

Figure 3-1 on page 177 shows the instrumentation directory structure on the HPOM management server.

Figure 3-1 **Instrumentation Directory Structure on the HPOM Server**



Instrumentation Data on the HPOM Managed Nodes

On HPOM managed nodes, all deployed instrumentation data (category-based instrumentation, as well as the files for monitors, actions, and commands) are located in the following directory:

```
/var/opt/OV/bin/instrumentation
```

Before You Distribute Instrumentation Data

Before you start the distribution of instrumentation, consider the following important points:

- If you want to deploy all the files from the `instrumentation` directory on the server to all specified managed nodes, create the `default` subdirectory inside the `instrumentation`, and move all the files into this directory, then start the distribution process.
- If you want to deploy instrumentation files to the particular managed nodes, create and assign categories in matter only to these target nodes, then start the distribution process.
- If you want to deploy only user-specified files to the managed nodes, make sure you have placed these files in the appropriate location under the category you have created for this purpose. For example, if you want to deploy only the instrumentation related to IPF32 11.23 under a category `Custom`, perform the following procedure:

  ```
  $InstrumDir/Custom/UNIX/HP-UX/IPF32/11.23/
  ```

  Make sure the category Custom is assigned to the appropriate managed nodes, and then start the distribution process.

Distributing Instrumentation using Categories

To distribute instrumentation data to managed nodes using *custom* categories, perform the following steps in the indicated order. For more information on how to perform each individual step, see the sections that follow:

1. Create the `Custom` category. For more information, see "Creating Instrumentation Categories" on page 179.
2. Place the instrumentation files in the appropriate location. For more information, see "Locating Instrumentation Data" on page 180.
3. Assign the category `Custom` to the appropriate managed nodes and to the appropriate policies. For more information, see "Assigning Instrumentation Categories" on page 180.
4. Start the distribution process using the `opcragt` command-line utility with the `-instrum` option. For more information about the distribution process, see "Deploying Instrumentation Data" on page 181.

Creating Instrumentation Categories

To create categories for the custom instrumentation you want to distribute, you can choose any of the following methods:

- `opcinstrumcfg` utility:

  To use the `opcinstrumcfg` utility to create a new instrumentation category, enter the following command:

  \# **opcinstrumcfg -add *<categoryA>,<categoryB>***

  Note that the items in a list of categories must be separated by a comma since the category names can contain blank characters.

  The `opcinstrumcfg` utility enables you to manage categories both on a file system and on a database level. Refer to the *opcinstrumcfg (1M)* reference page for more information about command options and parameters.

- `opcpolicy` utility:

  To use the `opcpolicy` utility to create a new instrumentation category, enter the following command:

  \# **opcpolicy -add_cat cat_list=*<categoryA>,<categoryB>* create=<yes/no>**

NOTE If you specify `create=no` (the default is `yes`), no subdirectory structure is created under these new categories in the file system.

  `opcpolicy` is a symbolic link to the `opctempl` command line utility, and is used for managing policies. Refer to the *opcpolicy (1M)* reference page for more information about command options and parameters. For additional information about policies, refer to the *HPOM Concepts Guide*.

- `opccfgupld` and `opccfgdwn` utilities.

  During the upload or download of the configuration data, the category assignments to policies are also added to the database, since they are regular policy header attributes. For more information about uploading and downloading the configuration data, refer to the *HPOM Administrator's Reference*, and the *opccfgupld (1M)* and *opccfgdwn (1M)* reference pages.

Locating Instrumentation Data

To make sure the deployment process completes successfully, you must place the instrumentation data in the correct location within the instrumentation subdirectory structure. HPOM expects to find instrumentation data in the following location:

```
$InstrumDir/Custom/<OS_family>/<OS_type>/<cpu_type>/\
<OS_version>
```

For example, you place custom instrumentation data for the HP-UX 11.31 operating system version in the following location:

```
$InstrumDir/Custom/Unix/HP-UX/IPF32/11.31/
```

For more information about where HPOM expects to find instrumentation data, see the following sections:

- "Before You Distribute Instrumentation Data" on page 178
- "Instrumentation-Data Directory Structure" on page 174

Assigning Instrumentation Categories

To assign instrumentation categories to managed nodes or policies (or both), choose any of the following methods:

- Assign a categories to a managed node(s) using the `opcnode` command, as follows:

  ```
  # opcnode -assign_cat node_list=<node_list>\
  cat_list=<category_list>
  ```

  Refer to the *opcnode (1M)* reference page for more information about command options and parameters.

- Assign categories to a policy using the `opcpolicy` command, for example:

  ```
  # opcpolicy -update policy=<policy_name>
  type=<policy_type> [version=<policy_version>]
  add_cats=<categoryA>,<categoryB>
  ```

NOTE Use the *`version`* option to assign a category to a specific policy version. Otherwise, the category is assigned to *all* versions of this policy.

When assigning a category with the `opcpolicy` command, note the following prerequisites:

— Categories must be assigned to a particular policy, for example, `policyX`.

— The policy (`policyX`) must be assigned to the managed nodes to which you want to distribute the instrumentation data.

For more information about policy management, see "HPOM Policies" on page 79. For more detailed information, see the *HPOM Concepts Guide*.

Deploying Instrumentation Data

To start the deployment of instrumentation data to managed nodes using the category-based distribution method, run one of the following commands on the HPOM management server:

1. Deploy all instrumentation data, including the contents of the `monitor`, `actions`, and `cmds` directories using the following command and parameters:

   `# /opt/OV/bin/OpC/opcragt -distrib -instrum <node_name>`

   <node_name> Name of the node to which you want to deploy the instrumentation data.

   If any files in the `monitor`, `actions`, and `cmds` directories have identical names to files in the `instrumentation` directory, HPOM deploys the files from the `instrumentation` directory.

2. Deploy all instrumentation data using the following command *only* if the policies are updated with the required category assignments:

   `# /opt/OV/bin/OpC/opcragt -distrib -templates`

   The `opcragt` command with the `-templates` option deploys policies and subsequently all categories assigned to these policies are added to the database. Refer to the *opcragt (1M)* reference page for more information about command options and parameters.

Distribution of Instrumentation to Managed Nodes

This section explains how to distribute commonly used instrumentation data from monitor, commands, and actions directories to the managed nodes.

Before You Distribute Instrumentation Data

Before you distribute instrumentation data from monitor, actions, and commands to the managed nodes, beside the general recommendations review also the following distribution requirements and tips:

❏ Customized scripts:

Specify the full path name of the customized script in the HPOM configuration. Or make sure the file is available through the *$PATH* settings of the executing user on the managed node.

For example, a customized script to determine running processes might look like one the following:

1. `/name/opc_op/scripts/my_ps`
2. `my_ps`

You can call this script as an application from the Java GUI or as a broadcast command.

❏ Customized binaries:

HPOM compresses the monitors, actions, and command binaries. If a file with a `.Z` extension already exists, do not put files into the following directory:

```
/var/opt/OV/share/databases/OpC/mgd_node/customer/\
<arch>/{monitor|actions|cmds}
```

<arch>	Architecture of the monitors, actions, and commands, for example: `hp/alpha/tru64` or `sun/sparc/solaris7`.

When distributing scripts to managed nodes on UNIX systems, follow these guidelines:

- Mixed clusters:

  You must install the scripts and programs for monitors, actions, and commands only once for each architecture type. For each architectural type, select one cluster node.

- File names:

  The file names of the monitors, actions, and commands binaries must not be longer than 14 characters (including the `.Z` extension if the binary is compressed). This limitation is set to ensure smooth processing on nodes running with short file names.

Instrumentation Data Distribution

You can distribute instrumentation data by using the `opcragt` command line interface. Instrumentation files are distributed only if they are not already installed on the managed node, or when a newer version is available on the management server.

NOTE To update only the changes in the configuration, do not use the `-force` option. The `-force` option (re-)distributes all files, which can cause an increase in network load.

For information about the directories on the management server and the managed node, see “Instrumentation Data Locations” on page 183.

The binaries are located in the temporary directories only during the distribution phase. When distribution is completed, the local HPOM action and monitor agents are stopped, the binaries are moved or copied to their final destination, and the HPOM action and monitor agents are restarted.

The HPOM action agent and monitor agent append directories to the *`$PATH`* setting of the executing user.

Instrumentation Data Locations

HPOM organizes instrumentation data differently according to whether it resides on the management server or the managed node. For example, on the management server, instrumentation data is split into vendor-related and customer-related areas. For more detailed information about the location of instrumentation data see the following sections:

- "Instrumentation on the HPOM Management Server" on page 184
- "Instrumentation on the HPOM Managed Node" on page 184

Instrumentation on the HPOM Management Server

Instrumentation files are located in the following two directories on the HP Operations management server:

- `/var/opt/OV/share/databases/OpC/mgd_node/vendor/\`
  `<arch>[/<comm>]/actions|cmds|monitor`
- `/var/opt/OV/share/databases/OpC/mgd_node/customer/ \`
  `<arch>[/<comm>]/actions|cmds|monitor`

The replaceable elements *<arch>* (hardware architecture) and *<comm>* (communication type) combine to define the directory specific to the operating system and, if desired, the communication type of the node to which you want to deploy the instrumentation data files.

The vendor-specific files contained within directory structure `/var/opt/OV/share/databases/OpC/mgd_node/vendor` are used for the default configuration of HPOM and are always distributed. The files contained in the customer tree are required only if policies are assigned and distributed.

NOTE If identical files for `actions`, `cmds`, and `monitor` exist in both the `customer` and `vendor` directories, use the `customer` files.

Instrumentation on the HPOM Managed Node

On HPOM managed nodes, all instrumentation data (category-based instrumentation, and the `actions`, `cmds`, and `monitor` files) is located in the following directory:

`/var/opt/OV/bin/instrumentation`

Selective Distribution to Managed Nodes

This section describes the selective distribution feature, which you start with the `opcbbcdist` command and configure with the `seldist` configuration file.

`opcbbcdist` usually distributes all the files to managed nodes from two sets of directories corresponding to the selected managed node type, for example HP-UX or Windows. For their location, see "Instrumentation Data Locations" on page 183.

During the default distribution process, HPOM deploys all instrumentation data including some files that might not be needed on a specific node. The problem of deploying unnecessary files is especially noticeable with the HP Operations Smart Plug-ins (SPIs). The SPI binaries can be very large and when distributed to all target nodes, may occupy a significant amount of network bandwidth during distribution and large amounts of disk space on the managed nodes.

The Selective Distribution functionality gives you greater flexibility in distributing files from the HP Operations management server. You can prevent distribution of a user-selected set of files and binaries, for example, files belonging to a SPI, from `actions`, `cmds`, and `monitor` directories to specific nodes that do not belong to the node group associated with the SPI.

The file `seldist` enables you to configure a list of files and target node groups that you have selected for deployment. For more information about the `seldist` configuration file, see "seldist Configuration File" on page 186.

The advantages of the selective-distribution feature include the following:

❏ Reduced disk-space utilization on managed nodes

❏ Reduced network traffic during configuration-file distribution

If selective distribution is *not* enabled, HPOM performs a standard distribution from monitors, actions and commands. If you want to avoid distributing *all* instrumentation data, use the the category-based distribution method since it also allows you to distribute specified user-selected files to a particular managed node. See "Category-Based

Distribution of Instrumentation” on page 174 for more information. See also “Distribution Methods” on page 172 to learn about the available distribution methods.

Selective Distribution Startup

On starting configuration file distribution from the command line, `opcbbcdist` checks the selective distribution configuration. When the distribution process of `actions`, `commands` or `monitors` is started, Selective Distribution in accordance with the requirements of the `seldist` file is started.

On distribution, each file from the customer actions, commands, and monitors directories is compared against each file name prefix in the `seldist` file. If it does not match any prefix, it is distributed to all agents of the respective platform.

If it matches one or more entries, it is only distributed to the agents of the corresponding node group(s). For example, an empty `seldist` file would result in all files being distributed to all nodes.

In a flexible-management environment, you must *manually* ensure synchronization of the `seldist` files on all of your HP Operations management servers.

Most of the files installed by the Database SPI have the `dbspi` prefix. SAP SPI files have an `r3` prefix. For example, a SAP SPI binary would be named `r3perfmon`.

In addition to the preconfigured SPI-related files, you can also add your own files and file prefixes together with a node-group name. This is most useful if you have your own policies and accompanying scripts that only need to be distributed to a subset of the nodes. For more information, see the section “Configuring Custom Selective Distribution” on page 192.

seldist Configuration File

A `seldist` configuration file is provided in which node group names together with file name prefixes and files are listed. This file is either read by `opcbbcdist` on startup, or triggered by the `opcseldist` utility. For more information on the `opcseldist` utility, usage and command line options, see “opcseldist Utility” on page 190 or the *opcseldist(1m)* reference page.

Selective Distribution is automatically enabled if the `seldist` file exists in the following directory: `/etc/opt/OV/share/conf/OpC/mgmt_sv/`

When the distribution of actions, commands, or monitors starts, the selective-distribution process uses the contents of the `seldist` file to distribute the instrumentation data.

The list of files in `seldist` refers only to files within the tree:

```
/var/opt/OV/share/databases/OpC/mgd_node/customer/\
<arch>[/<comm>]
```

The `seldist` configuration file lists, for each SPI, the target node group and a list of files and file prefixes that belong to this SPI. To include a managed node in the selective-distribution process, you must add the managed node to the node group specified in the `seldist` file.

All files that are not listed in the `seldist` file are also distributed to all nodes. Hence, this distribution is backwards compatible with the standard distribution of `actions`, `cmds`, and `monitor` as only certain "known" files are blocked from distribution to nodes that do not belong to a specific group of nodes.

The configuration file, `seldist.tmpl`, contains all currently known SPIs with suggested node-group names. To use this selective-distribution configuration file, make a copy of the default template in the same directory and name the new copy "`seldist`". For more information, see the section "Enabling Selective Distribution" on page 190. Example 3-1 on page 187 shows an extract from a sample `seldist.tmpl` file.

Example 3-1 Selective-Distribution Configuration File

```
# This is the specification file for Selective Distribution.
# It is delivered as:
#/etc/opt/OV/share/conf/OpC/mgmt_sv/seldist.tmpl.
# Before it can be used, the file has to be copied to:
# /etc/opt/OV/share/conf/OpC/mgmt_sv/seldist and edited there.

# Database SPI
#
DBSPI dbspi              # general prefix for most files
DBSPI ntwdblib.dll       # used for MS SQL on Windows
DBSPI sqlakw32.dll       # used for MS SQL on Windows
DBSPI libopc_r.sl          # used for Oracle 7.3.4 on HP-UX
11.00
# end of section Database SPI
```

```
# SPI for mySAP.com
#
sap r3                    # general prefix for most files
sap sap_mode.sh
sap netperf.cmd           # used for the NETPERF subagent
sap OvCor.dll             # used for SAP on Windows
sap OvItoAgtAPI.dll       # used for SAP on Windows
sap OvMFC.dll             # used for SAP on Windows
sap OvR3Wrapper.dll       # used for SAP on Windows
sap OvReadConfig.dll      # used for SAP on Windows
sap OvSpiASER3.dll        # used for SAP on Windows
sap librfc32.dll          # used for SAP on Windows
# end of section SPI for mySAP.com

# PeopleSoft SPI
# This is partitioned into 4 node groups.
# The PS DB Server nodes need the files from the Oracle SPI as
well.
#

PSAppServer psspi
PSBatchServer psspi
PSDBServer psspi
PSDBServer dbspi        # used for the PS DB Server nodes
PSDBServer libopc_r.sl  # used for Oracle 7.3.4 on HP-UX 11.00
PSWebServer psspi
# end of section PeopleSoft SPI
```

The syntax of the `seldist` file uses the following mandatory conventions:

- Comments:

  All text after a number sign (#) is treated as a comment and is *not* evaluated by the selective-distribution process.

- Active text:

  The selective-distribution process only evaluates the first two words are evaluated in any *enabled* (uncommented) lines, for example:

  ```
  DBSPI dbspi
  DBSPI ntwdblib.dll

  sap r3
  sap sap-mode.sh
  ```

In these examples, the first word represents the name of the node-group targeted for the selective-distribution process, for example: `DBSPI` and `sap`. The second word represents either a file name prefix or an individual file. For example, `dbspi` and `r3` are file name prefixes, and `ntwdblib.dll` and `sap-mode.sh` are individual files.

NOTE All file names are treated as prefixes. For example, the file name `ntwdblib.dll` would also match the file `ntwdblib.dll.old`, which would be included in the selective distribution.

- Node-group name:

  The same node group can be specified several times. As a result, it is possible to specify multiple prefixes, file names, or both for the same node group.

  To specify a node group whose name includes a space, wrap the node name in double quotes, for example, `"node group 1" prefix1`. If a node-group name does not contain any spaces, you do not need to wrap the name in quotes.

  Node group names may be localized.

- File-name prefix:

  You can associate the same prefix with more than one node group to ensure the deployment of a common subset of files. For example, the PeopleSoft SPI ships certain DBSPI files that are required on a PeopleSoft database server:

  ```
  DBSPI dbspi
  PS_DB_Server dbspi
  ```

  A file matching the `dbspi` prefix, for example, `dbspicao`, is distributed to a node only if that node belongs to either of the node groups `DBSPI` or “`PS DB Server`”. Similarly, it is possible to specify prefixes that are subsets of each other.

NOTE Any file names not included in the `seldist` file or that do not match any of the listed prefixes are distributed to *all* nodes, in the same way as they would be distributed to all nodes if the `seldist` functionality were not enabled.

opcseldist Utility

The `opcseldist` utility is a tool you can use to check the validity of `seldist` configuration files and send a re-configuration request to `opcbbcdist`. The `opcseldist` utility has the following command line options:

`-check` *<filename>*	Checks the syntax of the file *<filename>*
`-reconfig`	Notifies `opcbbcdist` of changes to the `seldist` file and instructs it to use the modified content.

If the syntax of the configuration file is invalid, `opcseldist` displays a list of errors. If an invalid configuration file is used to start a selective distribution, the distribution manager evaluates the `seldist` file only until it encounters the first error; any configuration data after the error is ignored.

Enabling Selective Distribution

To enable selective distribution using the configuration file supplied by a Smart Plug-in, perform the following steps:

1. Create node groups for the nodes to which you want to distribute your instrumentation data, for example: actions, commands, and monitors.

   Most SPIs already come with default node groups for their specific configurations. However, you can use a different node-group name as long as you remember to modify the `seldist` file accordingly.

2. Make sure that all required nodes are included in the node groups that are targeted for selective distribution of the SPI-related files.

3. Change directory to the location of the selective-distribution configuration file, as follows:

   `# cd /etc/opt/OV/share/conf/OpC/mgmt_sv`

4. Make a copy of the `seldist.tmpl` file and rename the copied file to `seldist`, enter:

   `# cp seldist.tmpl seldist`

5. In the `seldist` file, locate the configuration section for the SPI that you want to configure and make the desired changes.

TIP To avoid problems during the selective-distribution process, check the configuration sections for all SPIs that you do *not* have installed and make sure that these sections are disabled.

6. Save the configuration file and check the syntax, as follows:

   `# /opt/OV/bin/OpC/utils/opcseldist -check seldist`

   Correct any possible syntax errors in the file.

7. Run the `opcseldist` utility to re-configure `opcbbcdist`, as follows:

   `# /opt/OV/bin/OpC/utils/opcseldist -reconfig`

   The `opcbbcdist` process re-reads the `seldist` configuration file and checks the database for node groups specified in the configuration file. Because of possibly unwanted side effects, `opcbbcdist` will report to both the message browser and the `System.txt` file node groups that display in the `seldist` file, but are not in the database.

NOTE The `opcbbcdist` process reads the `seldist` configuration file during each startup. However, if you edit the `seldist` file and want to make the changes effective instantly, run the `opcseldist` utility with the `-reconfig` option. For more information on the `opcseldist` utility, usage, and command-line options, see “opcseldist Utility” on page 190.

8. Distribute the `actions`, `cmds`, and `monitor` binaries using the `opcragt` command.

9. If you have already distributed SPI actions, commands, and monitor binaries to the managed nodes and you now want to *remove* unnecessary binaries from these nodes, run a selective-distribution with the `-purge` option.

NOTE If you have distributed instrumentation from several, different HPOM servers, the `-purge` option from one management server removes instrumentation distributed from another HP Operations server, too.

Disabling Selective Distribution

To disable selective distribution, performing the following steps:

1. Locate the active selective-distribution configuration file.

   Change to the following directory:

   `# ` **`cd /etc/opt/OV/share/conf/OpC/mgmt_sv`**

2. Disable selective-distribution.

   Rename the active configuration file, `seldist`. For example, enter:

   `# ` **`mv seldist seldist.old`**

3. Notify HPOM about the new selective-distribution configuration.

   Run the `opcseldist` command with the `-reconfig` parameter. Enter:

   `# ` **`/opt/OV/bin/OpC/utils/opcseldist -reconfig`**

Configuring Custom Selective Distribution

The default `seldist` file currently contains configuration details for a selection of known SPIs. The configuration includes suggested names for node groups for the distribution of SPI-related files and binaries. You can configure a selective distribution of your own files and binaries placed in the `actions`, `cmds`, and `monitor` directories that you want to distribute to specified nodes or node groups, by creating a new configuration section in the `seldist` file.

To configure custom selective distribution, perform the following steps:

1. Update the `seldist` file.

   Modify the `seldist` configuration file by creating a new section for the instrumentation you want to distribute selectively. The new section should include the following information:

   - Node-group name:

     Name of the node group containing the managed nodes to which you want to selectively distribute instrumentation files.

   - File names and prefixes:

     Name (or prefix) of the file you want to include in the custom selective distribution.

   For more information about the syntax rules that are mandatory in the file you use to configure selective distribution, see “seldist Configuration File” on page 186.

2. Validate the changes you make to the `seldist` file.

   Run the `opcseldist` command with the `-check` parameter to make sure that the changes you made to the `seldist` file meet the syntax requirements and do not contain any errors. Enter:

   ```
   # /opt/OV/bin/OpC/utils/opcseldist -check seldist
   ```

3. Assign nodes to node groups, if necessary.

   Use the HPOM administrator’s user interface to make sure that the managed nodes to which you want to distribute selected files are included in the node group specified in the new section of the `seldist` configuration file.

4. Notify HPOM of the changes made in the selective-distribution configuration file.

   Run the `opcseldist` utility to force `opcbbcdist` to use the new configuration details. Enter:

   ```
   # /opt/OV/bin/OpC/utils/opcseldist -reconfig
   ```

4 HPOM Interoperability

In this Chapter

This chapter describes interoperability between HPOM on Linux and HP Operations Manager for Windows (HPOM for Windows). In this chapter, you can find information covering the following topics:

- "Interoperability in Flexible Management Environments" on page 197
- "Interoperability Between HPOM on Linux and HPOM for Windows" on page 198
- "Attribute-Based Message Forwarding" on page 200
- "Server-to-Server Message Forwarding" on page 201
- "Management-Server Synchronization" on page 209

Interoperability in Flexible Management Environments

In a flexible management environment, you can spread responsibility for managed nodes over multiple management servers, thereby enabling the managed nodes to send messages to the various management servers according to the time of day, location, or subject of the messages.

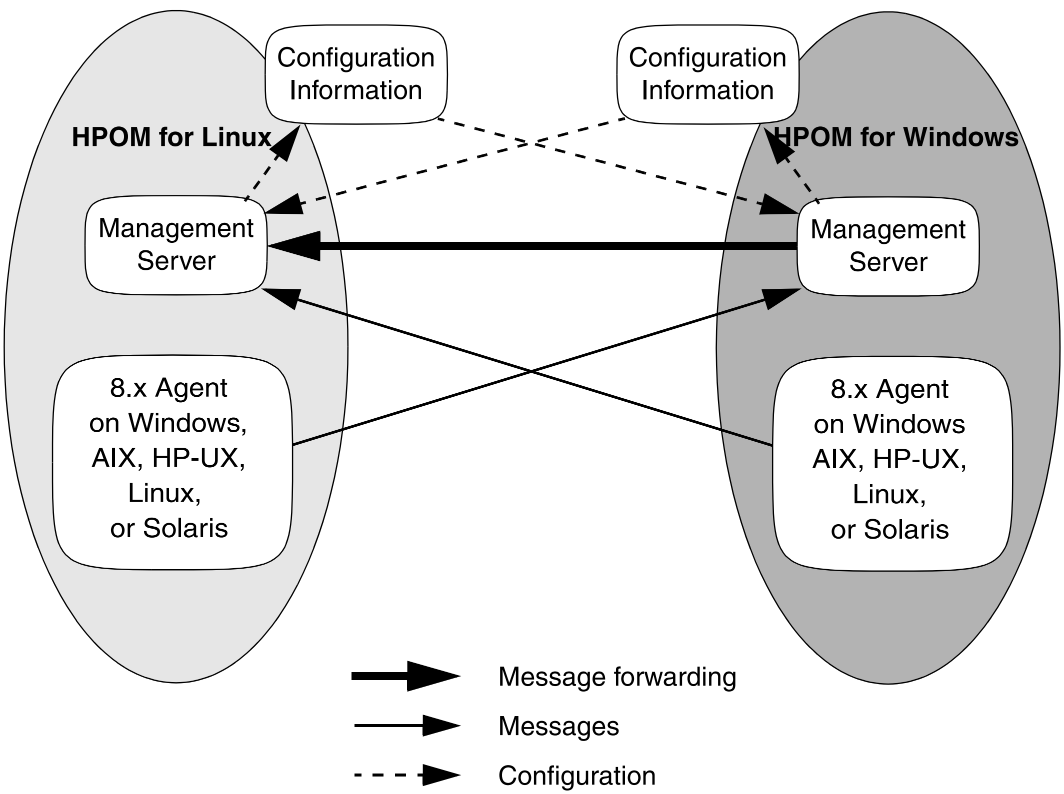
All participating HP Operations management servers should have the same major version of HPOM. However, there may be situations where one or more management servers are still running on an older version, for example when you are in the process of upgrading your HPOM environment to a newer version, with some management servers not being upgraded yet.

It is recommended that you upgrade all HP Operations management servers and managed nodes to the most recent version of HPOM in a timely manner. Mixed-version environments should remain a temporary solution.

Interoperability Between HPOM on Linux and HPOM for Windows

The HPOM management server is available for Linux platforms and for Windows platforms. Both versions of the management server can work together to manage the same nodes in your environment. The key features of interoperability as well as the configuration tasks are described in this chapter and in the HPOM for Windows online help.

Figure 4-1 HPOM on Linux and HPOM for Windows Interoperability



HPOM on Linux and HPOM for Windows provide several possibilities for exchanging messages and configuration. Figure 4-1 on page 198 shows the various communication paths between HPOM on Linux and HPOM for Windows:

- Message forwarding:

  HPOM for Windows management servers can forward messages to HPOM on Linux management servers. See “Server-to-Server Message Forwarding” on page 201 for more information.

- Messages:

  HPOM agents can send messages in the following directions:

  - HPOM on Linux agents to HPOM for Windows servers
  - HPOM for Windows agents to HPOM on Linux servers

  See “Attribute-Based Message Forwarding” on page 200 for more information.

- Configuration:

  You can synchronize HPOM configuration information such as policies and nodes between HPOM on Linux and HPOM for Windows using the upload and download tools provided with each version of the management server. See “Management-Server Synchronization” on page 209 for more information.

Attribute-Based Message Forwarding

HPOM's flexible management feature enables you to configure managed nodes to send messages to different management servers, based on time and message attributes. This is not simply forwarding all messages from one management server to another, but rather specifying which messages from a managed node should be sent to which management server.

Additional configuration provided by agent-based flexible-management policies includes specifying which management server is allowed to execute actions on this managed node and which management server can become the primary management server of this managed node.

Refer to the HPOM for Windows online help for more information.

Server-to-Server Message Forwarding

HPOM provides the following methods for forwarding messages from HPOM for Windows management servers to HPOM on Linux management servers:

- Server-based message forwarding:

  Server-based flexible management is the recommended message forwarding solution for HPOM for Windows 7.50, and higher. It uses the same message forwarding and synchronizing techniques used in HPOM on Linux. It allows the forwarding of messages directly from one management server to other management servers, including HPOM on Linux management servers.

  For more information about server-based message forwarding, see "Configuring Server-Based Message Forwarding" on page 201.

- Agent-based message forwarding:

  Agent-based, server-to-server message forwarding is the message forwarding solution used in previous versions of HPOM for Windows. HPOM for Windows 7.5 introduces a new message forwarding solution, server-based flexible management, which is now the recommended message forwarding solution. Agent-based, server-to-server message forwarding is only available to support backward compatibility.

  See "Configuring Agent-Based Message Forwarding" on page 203 for more information.

Configuring Server-Based Message Forwarding

To set up message forwarding between HPOM management servers, perform the following high-level steps:

1. Exchange security certificates between the HPOM management servers.

   You exchange security certificates between HPOM management servers by exporting and importing the certificates using the `ovcert` command, as follows:

   ```
   ovcert -exporttrusted -ovrg server -file <certificate>
   ```

`ovcert -importtrusted -ovrg server -file <certificate>`

2. Add the management server to the node bank.

   If not already present, add the management server that *receives* the forwarded messages to the node bank of the management server that *forwards* the messages.

3. Add the hosts sending messages to the node bank.

   Make sure that the hosts where messages originate are present in the node bank of the HPOM management server that is forwarding messages.

4. Set up a message-forwarding policy.

   You can set up server based message forwarding automatically (using a policy) or manually (editing a file), as follows:

   - Automatic:

     Configure and deploy the server-based message-forwarding policy on the management server that is forwarding the messages.

   - Manual:

     HPOM includes examples and templates that you can use to configure server-based message forwarding manually. The default templates are located in the following directory:

     `/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs`

     Make a copy of the file, modify the contents, and move the modified file to the following directory: `/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs`.

5. Restart the HPOM management server processes.

   To notify the management servers of the new configuration, restart the HPOM server process. Enter the following command in a command shell as user root:

   `#` **`opcsv -start`**

Agent Support in Mixed HPOM Environments

HPOM on Linux and HPOM for Windows support different kinds of the HTTPS agent; note the usage restrictions summarized in the following table:

Table 4-1 **Agent Support in Mixed** HPOM **Environments**

HTTPS Agent HPOM Server	8.1x	8.50	8.51
HPOM for Unix 8.2x (x<9)	✔	✔ [a]	✔ [a]
HPOM for Unix 8.29+	✔	✔ [a]	✔
HPOM for Windows 8.0		✔	

a. *Operational and policy deployment only*: HPOM message sending to HPOM server, action launch, action response, policy deployment, and so on, but *not* HTTPS agent software installation

NOTE At least the HPOM for Unix 8.29 server patch level is required to install the 8.51 HTTPS agent patches on the HPOM for Unix server.

Configuring Agent-Based Message Forwarding

To configure an HPOM for Windows management server to forward messages to HPOM on Linux, perform these procedures:

1. Configure HPOM for Linux to accept messages forwarded from a HPOM for Windows management server.

   For detailed instructions, see “Forwarding Messages from HPOM for Windows to HPOM on Linux” on page 204.

2. Configure the HPOM for Windows agent.

   For detailed instructions, see “Configuring the HPOM for Windows Agent” on page 207.

3. Optional: Configure the Windows registry

For detailed instructions, see "Changing the Default Name of the WMI Policy" on page 208.

Message Forwarding on an HPOM for Windows Management Server

By setting up message forwarding from an HPOM for Windows management server, you establish the following conditions:

- ❏ Managed node:

  The node on which the HPOM for Windows management server is running sends messages to, and accepts actions from, the HPOM for Windows management server and the HPOM on Linux management server. The installed agent is an HPOM for Windows agent.

- ❏ OV_Messages:

  All HPOM messages with the property `Type` set to `ForwardToVP` are sent to the HPOM on Linux management server. All other messages go to the HPOM for Windows management server. This configuration is established through the HPOM on Linux management server with a policy for flexible-management configuration.

- ❏ WMI interceptor:

  To mark messages that should be forwarded to HPOM on Linux, the WMI interceptor of the HPOM for Windows agent is used to intercept these messages. Then, messages with the updated value of property `Type` will be sent to the HPOM on Linux server.

Forwarding Messages from HPOM for Windows to HPOM on Linux

1. Inform the HPOM on Linux management server about the HPOM for Windows management server that is forwarding messages.

   To set up the HPOM on Linux management server to accept messages forwarded from an HPOM for Windows management server, perform the following steps:

   a. Add the host on which the HPOM for Windows server is running to HPOM as a controlled managed node by using the `opcnode` command line interface. For more information about command options and parameters, see the *opcnode(1m)* reference page.

b. Update the HPOM on Linux configuration for the HPOM for Windows node manually using the following command:

`# /opt/OV/bin/OpC/opcsw -installed <node>`

The `opcsw` command returns the hexadecimal value of the node's IP address, for example: `f887b88`. Make a note of the value returned by the `opcsw` command; you will need it to set up the flexible-management configuration policy. For more information about the `opcsw` command, see the reference page *opcsw*(1M).

c. Start heartbeat polling for the HPOM for Windows node manually using the following command:

`# /opt/OV/bin/OpC/opchbp -start <node>`

2. Inform the HPOM for Windows management server where to forward the messages to and what, if any, actions or operations are allowed.

To configure a message-forwarding file from an existing default policy, perform the following steps:

a. Create a file and name it with the hexadecimal value returned by the command `opcsw`, for example: `f887b88`.

b. Copy the template below and paste it into the newly created file.

```
#
# Template for message forwarding to an HPOM server
#
#TIMETEMPLATES
# None
#
# Responsible Manager Configurations
#
#RESPMGRCONFIGS
# Responsible HPOM Manager: bigunix
# Responsible HP Operations Manager for Windows
#Manager: bignt
RESPMGRCONFIGS

RESPMGRCONFIG
   DESCRIPTION "Responsible managers in an HPOM
environment"
   SECONDARYMANAGERS
      SECONDARYMANAGER
         NODE IP 0.0.0.0 "bigunix"
         DESCRIPTION "HPOM Manager"
```

```
        SECONDARYMANAGER
            NODE IP 0.0.0.0 "bignt"
            DESCRIPTION "HP Operations Manager for Windows
Manager"
    ACTIONALLOWMANAGERS
        ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 "bigunix"
            DESCRIPTION "HPOM Manager"
        ACTIONALLOWMANAGER
            NODE IP 0.0.0.0 "bignt"
            DESCRIPTION "HP OpenView Operations for
Windows"
    MSGTARGETRULES
        # Responsible Manager is the HPOM Manager
        MSGTARGETRULE
            DESCRIPTION "All messages with
            MsgType='ForwardToVP' should be sent to the
            HPOM Server"
            MSGTARGETRULECONDS
                MSGTARGETRULECOND
                    DESCRIPTION "Message that should be
                    forwarded to HPOM"
                    MSGTYPE "ForwardToVP"
                MSGTARGETMANAGERS
                    MSGTARGETMANAGER
                        TIMETEMPLATE "$OPC_ALWAYS"
                        OPCMGR IP 0.0.0.0 "bigunix"
        # Responsible Mgr is the HP Operations Manager for
Windows Mgr
        MSGTARGETRULE
            DESCRIPTION "Message for the
            HP Operations Manager for Windows server"
            MSGTARGETRULECONDS
                MSGTARGETMANAGERS
                    MSGTARGETMANAGER
                        TIMETEMPLATE "$OPC_ALWAYS"
                        OPCMGR IP 0.0.0.0 "bignt"
```

c. Search through the text you paste into the newly created message-forwarding file and replace all instances of the example server names `bigunix` (HPOM on Linux server) and `bignt` (HPOM for Windows server) with the server names you are using in your environment.

d. To ensure that any changes you make to the file meet syntax requirements for the template structure, run the HPOM on Linux policy validation tool `opcmomchk(1)` on the finished configuration file, as follows:

```
# /opt/OV/bin/OpC/opcmomchk <filename>
```

For more information about the `opcmomchk` utility, see the reference page *opcmomchk(1)*.

e. Copy the file you created to the following directory on the HPOM on Linux server:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs
```

3. Inform HPOM for Windows of the name of the HPOM on Linux management server to which you want to forward messages.

   Run the tool `Switch management server for Windows nodes`, located in the HPOM for Windows management server console under `Tools > OpenView Tools`.

IMPORTANT The status of the tool remains on "starting", if the switch was successful.

   When prompted by the script, enter the name of the HPOM on Linux management server.

4. To distribute the created flexible-management configuration to the Windows node of the HPOM for Windows server, use the `opcragt` command with the following parameters:

```
# opcragt -distrib -templates -force \
<name_of_HPOM_Windows_management_server>
```

5. Run the tool `Switch management server for Windows nodes` again on the HPOM for Windows management server.

   When prompted by the script, enter the name of the HPOM for Windows management server.

Configuring the HPOM for Windows Agent

To configure the HPOM for Windows agent, deploy the following policy to the HPOM for Windows management server:

```
Policy management\Samples\Forward to VP
```

Changing the Default Name of the WMI Policy

The WMI policy used to define the messages to be forwarded to HPOM on Linux is named `ForwardToVP`. If you want to use some other name for the policy, you must rename the policy and then indicate the new name in the Windows registry on the HPOM for Windows management server.

To change the default name of the WMI policy, create the following registry entry:

```
REGEDIT4 [HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OV
Enterprise\Agent\OvMsgActFM] "Forward To VP Policy"="<New
Name>"
```

Changing the Default Property Type of All Messages Forwarded to HPOM on Linux

The WMI interceptor sets the property **message type** of all messages to be forwarded to HPOM on Linux. The default message type is `ForwardToVP`. If you want to use some other message type, you must change the type in the `ForwardtoVP` policy and create the following registry entry on the HPOM for Windows management server:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OVEnterprise\
Agent\OvMsgActFM] "MsgType in Forwarded Messages"="<New
Type>"
```

Refer to the HPOM for Windows online help to learn how to change the message type of a policy.

NOTE If you change this default property type of all messages to be forwarded to HPOM on Linux, you must adjust the flexible management policy accordingly. As you can see in the sample policy in “Forwarding Messages from HPOM for Windows to HPOM on Linux” on page 204, the default value `ForwardToVP` is used in `MSGTYPE ForwardToVP` to match the forwarded messages.

Management-Server Synchronization

You can exchange the configuration of one HPOM management server with other management servers. This is useful if you want to develop policies and other configuration data centrally and then deploy the configuration to multiple management servers.

Configuration synchronization is also helpful if you want to forward messages to (and synchronize messages between) management servers. You can easily synchronize node configuration and instruction text configuration between the forwarding management servers. This synchronization enables you to set up a working message-forwarding environment. For more information about synchronizing the configuration of HPOM servers, refer to the HPOM for Windows online help.

5 Application Integration with HPOM

In this Chapter

This chapter explains how to integrate applications into HP Operations Manager (HPOM). It also describes several integrations that are available with HPOM. For more information on a particular product which is integrated with the HPOM, see the documentation provided with this product. In this chapter, you can find detailed information about the following topics:

For more detailed information on the elements and the windows you can use to carry out the integration, refer to the *HPOM Concepts Guide*. Refer also to the *HPOM Application Integration Guide* available within the HP Operations Manager Developer's Toolkit.

Application Integration

HP Operations Manager (HPOM) enables operators to invoke applications. Applications can include default tools installed with the product, any custom applications you write and integrate, or applications installed by a Smart Plug-in (SPI).

Application Assignment

You can assign a different set of applications to each operator, as needed.

Pre-Integrated HP Applications

If you have purchased an application that is already prepared for HPOM integration (for example, HP Data Protector), you can integrate it quickly and easily using the upload-configuration utility, `opccfgupld(1M)`. For more information about the options available with the `opccfgupld` command, run `opccfgupld` with the `-h(elp)` option.

Application Integration with HPOM Components

You can integrate applications into the following HPOM components:

- ❏ Java GUI
- ❏ Broadcasts
- ❏ Actions (automatic, operator-initiated, and scheduled)
- ❏ Monitoring
- ❏ Logfile encapsulation
- ❏ SNMP trap and message interception

Integrated Applications in the Java GUI

You can add your own applications, and assign them to an operator. The applications are then invoked when the operator clicks the application name under the `Tools` folder of the Java GUI `Object Pane`.

HPOM Application Integration

Typically, HPOM applications are utilities that provide services of a general nature, they help build a set of management tools. You can pass information (for example, selected nodes) as arguments to the applications. Users then start the applications by selecting them in the `Tools` folder of the Java GUI `Object Pane`.

Applications and application groups integrated into HPOM can be managed using the `opcappl` command line tool. For more information about command options and parameters, refer to the *opcappl(1m)* reference page. HPOM provides a selection of default applications and application groups.

Integrated Applications as Broadcast Commands

You can launch applications on multiple systems at the same time using the HPOM broadcast command facility in the Java GUI.

Integration Requirements

To launch an application on multiple systems, you must first meet the following requirements:

- UNIX systems:

  The application must be accessible from your *$PATH* settings.

- All systems:

  The path must be fully qualified on the `Broadcast Command` window.

NOTE In all cases, the application you want to launch must be available on the managed node.

Application Distribution to Managed Nodes

You can distribute simple and widely used applications to managed nodes through HPOM. For details, see “HPOM Agent-Configuration Distribution” on page 169.

Integrated Applications as Actions

You may configure an application or script to run as an automatic action, operator-initiated action, or scheduled action:

❏ Automatic action:

Action triggered by a message received in HPOM.

❏ Operator-initiated action:

Action enabled by a message received in HPOM and executed by an operator.

❏ Scheduled action:

Actions configured by the HPOM administrator. These actions execute a routine task at a preconfigured time.

Action Agent

Actions are always performed by the HPOM action agent, which operates as root on UNIX systems, as HP ITO Account on Windows systems. To be executed, the action must be available on the managed node.

NOTE The HP ITO Account is part of the Administrator, Domain Administrator, and User Administrator groups. If an action is prohibited for one of these groups, the HP ITO Account is not able to perform that action.

Requirements for Integrating Applications as Actions

To integrate applications as action, the applications must meet the following requirements:

- UNIX systems:

  The application must be accessible from the *$PATH* settings of the root.

- All systems:

The path must be fully qualified in the corresponding message condition.

Distributing Actions to Managed Nodes

You can distribute simple and widely used actions to managed nodes through HPOM. For details, see "HPOM Agent-Configuration Distribution" on page 169.

Integrating Monitor Applications

You can use applications for monitoring purposes by configuring them to deliver the monitored object status using the `opcmon(1)` command or `opcmon(3)` API.

Requirements for Integrating Monitored Applications

To integrate a monitored application into HPOM, the application must meet the following requirements:

- UNIX systems:

  The application must be accessible from the *$PATH* settings of the root.

- All systems:

  The path must be fully qualified in the corresponding message condition.

NOTE In all cases, the application you want to launch must be available on the managed node.

Distributing Monitored Applications to Managed Nodes

You can distribute simple and widely used monitoring applications to managed nodes through HPOM. For details, see “HPOM Agent-Configuration Distribution” on page 169.

Monitoring Application Logfiles

You can monitor applications by observing their logfiles. You can suppress logfile entries or forward them to HPOM as messages. You can also restructure these messages or configure them with HPOM-specific attributes.

NOTE Most applications running on Windows systems use **Eventlogs**. The information in these databases can be extracted by the logfile encapsulator, but there are some differences in the setup procedure. For more information, refer to the *HPOM Concepts Guide*.

Intercepting Application Messages

To monitor applications, HPOM uses the following messages:

- Logfiles
- SNMP traps
- `opcmsg(1)` command
- `opcmsg(3)` API

Depending on how you have configured HPOM, you can suppress messages or forward them to HPOM. You can also restructure these messages or configure them with HPOM-specific attributes.

Message-Stream Interface API

You can use the Message-Stream Interface (MSI) API to register applications to receive messages on the management server. The MSI lets you plug in event-correlation engines and statistical-analysis tools to establish a link to other network and system-management applications.

Messages are intercepted before they are added to the HPOM database and before they are displayed in the HPOM message browsers. For further information, see the documentation available with the HP Operations Manager Developer's Toolkit.

Applications and Broadcasts on Managed Nodes

Before it starts an application or broadcast command on the managed node, HPOM verifies the profile of the executing user.

Restrictions on Applications and Broadcasts

The following restrictions apply to applications and broadcasts:

❑ Commands and applications:

The HPOM action agent broadcasts commands and starts applications.

Applications are configured as follows:

- `Window (Output Only)`
- `Window (Input/Output)`
- `No Window (eg X Application)`

During the execution of a user profile, `stdin`, `stdout` and `stderr` are not available. For this reason, avoid commands reading from standard input or writing to standard output or error. In particular, avoid commands such as the following:

- `stty`
- `tset`
- Startup of window (input/output) applications

❑ Delays and inactivity:

If a delay of more than two seconds occurs during application output or input, HPOM assumes that an error has occurred and stops application execution. For example, an HPOM error can occur if a program runs for more than two seconds without generating output.

NOTE Applications do not require a separate terminal window.

User Profile Configuration

When setting up user profiles, take note of the following guidelines:

- ❏ User Input:

  Do not ask for specific user input in the profile. Instead, provide a default value that users can confirm by pressing **Return**. For example, the following examples show good and bad ways to write scripts that require user confirmation:

  — Not recommended:

  The following script for HP-UX 11.x produces an endless loop if no valid answer is specified:

```
#!/usr/bin/sh
TERM=""
while [ -z "${TERM}" ]
do
 echo "Type of terminal (hp|vt100): \c"
 read TERM
 if [ "${TERM}" != "hp" -a "${TERM}" != "vt100" ]
 then
   TERM=""
 fi
done
```

  — Recommended:

  The following script shows the correct way to prompt the user to confirm a default value. If no valid answer is specified, a default value is used:

```
#!/usr/bin/sh
echo "Type of terminal (hp=default|vt100): \c"
read TERM
if [ "${TERM}" != "hp" -a "${TERM}" != "vt100" ]
then
  TERM=hp
fi
```

- ❏ Questions:

  Do not ask more than four questions in the user’s profile. HPOM only answers up to four prompts with **Return**.

- ❏ Logout messages:

Do not add a logout message to the user's profile. HPOM adds the message at the end of the application's output. In addition, do not use sequences of escape characters in the profile. Escape characters are also added to the application output, thereby garbling the output.

NNM 7.xx and HPOM

HPOM provides an integration with the HP Network Node Manager (NNM) installed on the remote system. This integration enables users to execute HP Software applications from the HPOM Java GUI.

Some applications that are a part of Network Node Manager (NNM) are automatically integrated into HPOM. For a list and description of the default NNM application groups and applications, see “Default Applications and Application Groups” on page 69.

NOTE Events are forwarded from NNM 7.xx to HPOM using the `opctrapi` mechanism. For the newer NNMi 8.xx integration, incidents are forwarded from NNMi to HPOM using the HP Incident Web Service (IWS). See “NNMi and HPOM” on page 228.

Installation of NNM 7.xx Integration Software

The information in this section refers to the installation of NNM on the HPOM agent. The integration with NNM 7.xx is supported on the following HPOM agent platforms:

❏ HP-UX 11i v3

❏ Solaris 10 for SPARCstation

NOTE NNM cannot be installed on the same system hosting the HP Operations management server.

Installing NNM 7.xx Integration Software

To make use of the HPOM integration with a remote instance of Network Node Manager (NNM), perform the following steps:

1. Install NNM on the remote system.

   For NNM installation and configuration instructions, consult the relevant NNM documentation.

2. Install the HP Operations agent on the system hosting the NNM management-server instance.

   For more information about hardware and software prerequisites as well as instructions for installing the HPOM agent, see Chapter 1, "Agent Installation on HPOM Managed Nodes," on page 25.

3. Assign the subagent policy HPOvOUOvwMgr to the managed node hosting the instance of the NNM management server.

   You can assign policies using the `opcnode` command with the `-assign_pol` parameter, as follows:

   ```
   # opcnode -assign_pol pol_name=HPOvOUOvwMgr \
   pol_type=Subagent version=1.0 node_name=<node_name> \
   net_type=NETWORK_IP
   ```

   <node_name> Name of the system hosting the instance of the NNM management server.

4. Install the HPOM subagent package on the managed node hosting the instance of the NNM management server.

   The `HPOVOUOVWMGR` package enables the integration of HPOM with NNM 7.xx. The `HPOVOUOVWMGR` package is included in the HPOM subagent package and is automatically installed during the subagent installation on the managed node. For more information about the subagent installation procedure, see "Subagent Installation on Managed Nodes" on page 49.

Operator Control of HPOM Agents

By default, only an HPOM administrator is allowed to start or stop HPOM agents on the managed nodes through the HPOM Java GUI. However, operators can make changes to this policy by updating the `HPOM Status` application, which HPOM provides in the application bank as a preconfigured HPOM application.

Enabling HPOM Operators

To enable operators to control HPOM agents, follow these steps:

1. Create a new application called `HPOM Agent Start`.

   Create a copy of the default application `HPOM Status` and call the new copy `HPOM Agent Start` using the following command:

```
# opcappl -copy_app app_name="HPOM Status" \
new_name="HPOM Agent Start"
```

For more information about permitted parameters and options, refer to the *opcappl(1m)* reference page.

2. Modify access permissions for the new application `HPOM Agent Start`.

   To enable an operator to *start* the HPOM agents, change the startup parameters for the new `HPOM Agent Start` application, as follows:

```
# opcappl -chg_app app_name="HPOM Agent Start" \
app_call= "/opt/OV/bin/OpC/opcragt -start $OPC_NODES" \
desc="Starting of HPOM Agents" user_name=<user_name>
```

3. Create a new application called `HPOM Agent Stop`.

   Create a copy of the default application `HPOM Status` and call the new copy `HPOM Agent Stop` using the following command:

```
# opcappl -copy_app app_name="HPOM Status" \
new_name="HPOM Agent Stop"
```

4. Modify access permissions for the new application `HPOM Agent Stop`.

   To enable an operator to *stop* the HPOM agents, change the startup parameters for the new `HPOM Agent Stop` application, as follows:

```
# opcappl -chg_app app_name="HPOM Agent Stop" app_call=
"/opt/OV/bin/OpC/opcragt -stop $OPC_NODES" desc="Stopping
of HPOM Agents" user_name=<user_name>
```

5. Assign the new applications to the operators.

   For example:

```
# opccfguser -assign_app_user -user <user_name> -app
-list "HPOM Agent Start" "HPOM Agent Stop"
```

   For more information about permitted parameters and options, refer to the *opccfguser(1m)* reference page.

NNMi and HPOM

This section describes how to install, configure, and use the HP Network Node Manager i-series Software (NNMi) integration on HPOM management servers. The HP NNMi integration forwards incidents from NNMi to the HPOM message browser and provides easy access to the NNMi console from within HPOM.

The NNMi integration software is installed automatically with HPOM. However, you need to configure the HPOM agent or web-service implementation before you can use the integration, as follows:

❏ HPOM agent implementation:

The HPOM agent implementation of the NNMi–HPOM integration is available from NNMi version 8.12. This implementation is the preferred solution for integrating HPOM with NNMi. For more information about the agent implementation, see “NNMi Integration: Agent Implementation” on page 229.

❏ HPOM web-service implementation:

The *web-service* implementation of the NNMi–HPOM integration is available from NNMi version 8.03. Note that the HPOM agent implementation is the preferred solution for integrating HPOM with NNMi. For more information about the web-service implementation, see “NNMi Integration: Web-Service Implementation” on page 233.

NOTE

If the HPOM-agent and the web-service implementations of the NNMi–HPOM integration both forward messages to the same HPOM management server, you might not see all messages from both implementations in the HPOM message browser. For this reason, HP does not support running both implementations of the NNMi–HPOM integration to the same HPOM management server concurrently.

You can see the forwarded NNMi incidents in the HPOM message browser. Since forwarded messages in the HPOM browser are associated with the original incidents reported in NNMi, you can launch the NNMi incident browser within HPOM and display the original incident. Each NNMi incident has a unique identity, so that even where HPOM is consolidating events across multiple NNMi management servers, you can trace a particular incident back to its origin in NNMi and investigate it.

Some of the tools in the NNMi tools group are integrated by default into HPOM. This means you can access NNMi tools from nodes in the HPOM console, and from the active and history message browsers. For more information, see "NNMi Tools" on page 236.

Supported Versions

For up-to-date information about supported product versions for the NNMi–HPOM integration, see the support matrices at the following location:

`http://support.openview.hp.com/selfsolve/document/KM323488`

NNMi and HPOM must be installed on separate computer systems. The operating system of the NNMi management server and the HPOM management server are independent of each other. They can use the same operating system, although this not a requirement. For example, an NNMi management server can run on the HP-UX platform, while the HPOM management server runs on a Windows operating system.

NNMi Integration: Agent Implementation

When using the HPOM agent implementation, the HP NNMi integration forwards NNMi incidents as SNMPv2 traps to an HPOM agent on the NNMi management server. The HPOM agent filters the SNMPv2 traps and forwards them to the HPOM active messages browser. The configuration of the HPOM agent determines which HPOM management server receives the message.

The HPOM agent implementation of the HP NNMi–HPOM integration is available as of NNMi version 8.12. This implementation is the preferred solution for integrating HPOM with NNMi.

In NNMi, incidents can be generated directly by NNMi (called management events) or generated from SNMP traps. The NNMi northbound interface makes these incidents available as SNMPv2 traps. The HPOM agent listens at the northbound interface for these SNMPv2 traps. An SNMP Trap policy determines how the agent filters and processes the SNMPv2 traps.

The SNMP Trap policy is based on an SNMP trap policy file that you generate on the NNMi management server. The SNMP trap policy file includes an SNMPv2 trap definition for each of the management events and SNMP traps in the current NNMi configuration. The HPOM agent sends traps that pass the filters of the policy as messages to the HPOM management server.

The HP NNMi–HPOM integration provides a one-way flow of NNMi incidents to HPOM. When the lifecycle state of an incident changes to closed in NNMi, NNMi forwards a close event to HPOM. HPOM acknowledges the message for the original incident in the HPOM message browser. NNMi sends only one copy of each management event or SNMP trap to the HPOM agent.

If you configure the HP NNMi–HPOM integration to forward all received SNMP traps and the HPOM management server receives SNMP traps directly from devices that NNMi manages, HPOM receives duplicate device traps. You can set the policies to correlate SNMP traps from NNMi with those that HPOM receives directly from managed devices.

You can see the forwarded NNMi incidents in the HPOM message browser. The tools in the NNMi tools group provide access to NNMi views in the context of the selected message. Information embedded in each message supports this cross-navigation:

- The `nnmi.server.name` and `nnmi.server.port` custom message attributes in the message identify the NNMi management server.
- The `nnmi.incident.uuid` custom message attribute identifies the incident in the NNMi database.
- The original trap source appears in the Object column of the HPOM message browser and in the `nnm.source.name` custom message attribute.

Configuring the Agent Implementation

The NNMi integration is installed automatically with HPOM. The NNMi–HPOM integration uses the NNMi-northbound integration module and the `nnmopcexport.ovpl` tool, which are part of NNMi 8.12 or higher.

NOTE For details about installation and configuration tasks that you must carry out on HP Network Node Manager i-series Software (NNMi) management servers, see the *HP NNMi Software Deployment Guide*.

1. Generate an SNMP policy file on the NNMi management server.

   On the NNMi management server, use `nnmopcexport.ovpl` to generate an SNMP trap policy file (`NNMi_policy.dat`), which you can then transfer to the HPOM management server. For information about how to generate an SNMP-trap policy file, see the *HP NNMi Software Deployment Guide* for details.

2. Enable HPOM to receive messages from NNMi.

   To enable HPOM to receive messages from NNMi, perform the following steps on the HPOM management server:

   a. Add a node for the NNMi management server and install an agent on the node.

      For the prerequisites and installation instructions for the HP Operations agent, see the Chapter 1, “Agent Installation on HPOM Managed Nodes,” on page 25.

   b. Import the `NNMi_policy.dat` file into HPOM, as follows:

      i. Run the following command to create a directory structure for upload tree:

```
# mkdir -p /tmp/trap/C/TEMPLATES/TRAP
```

      ii. Run the following command to create an index file for `opccfgupld`:

```
# cat > /tmp/trap/C/trap.idx << EOF
HEADER
CHARACTER_SET ASCII
ADMIN_UUID "5e30d5740cbc.02.0f.88.78.18.00.00.00";
CONTENTS SELECTED;
ENTITY TRAP_TEMPLATE * ;
.
EOF
```

      iii. Run the following command to copy your trap template to the upload tree:

```
# cp /tmp/NNMi_policy.dat \
/tmp/trap/C/TEMPLATES/TRAP/
```

iv. Run the following command to upload the data:

```
# opccfgupld -replace -upgrade C /tmp/trap
```

c. Deploy the `NNMi Management Events` policy to the NNMi managed node.

d. Add an external node to catch all forwarded NNMi incidents.

You can set up one external node to catch all forwarded NNMi incidents, eliminating the need to configure each system in HPOM as a separate managed node. For initial testing, set the node filter to `<*>.<*>.<*>.<*>` (for an IP filter) or `<*>` (for a name filter). After you validate the integration, restrict the external node filter to match your network.

NOTE If you do not set up an external node for the NNMi incident source nodes, then all incidents forwarded from the NNMi server will be discarded by the HPOM management server.

3. Allocate a port to the HPOM agent on the NNMi management server.

   On the NNMi management server, allocate a custom port number to the HPOM agent to enable the agent to receive SNMP traps from NNMi. For more information about setting up the HPOM agent to receive SNMP traps from NNMi, see the *HP NNMi Software Deployment Guide*.

4. Configure NNMi incident forwarding to HPOM.

   On the NNMi management server, configure NNMi to forward incidents to HPOM. For more information about setting up incident forwarding in NNMi, see the *HP NNMi Software Deployment Guide*.

5. *Optional*. On the HPOM management server, add custom message attributes for NNMi incidents to the message browser.

   a. In the browser, right-click any column heading, and then click `Customize Message Browser Columns`.

   b. In the Custom tab, select from the `Available Custom Message Attributes`, and then click `OK`.

- The custom message attributes for NNMi incidents begin with the text `nnm`.
- The most interesting attributes for NNMi incidents are as follows:

  `nnm.name`

  `nnm.server.name`

c. *Optional.* To change the order in which the custom message attributes appear in the messages browser, drag a column heading to the new location.

6. *Optional*. On the HPOM management server, install additional NNMi tools.

   For details, see “Installing Additional NNMi Tools” on page 240.

NNMi Integration: Web-Service Implementation

The NNMi–HPOM integration uses a web services-based integration module to forward incidents automatically from NNMi into the message browser in HPOM server installations. You can also configure filters that limit the criteria under which NNMi forwards incidents to HPOM. The integration synchronizes incidents between NNMi and HPOM. It also provides easy access to the NNMi console and NNMi forms, views, and tools from within HPOM.

The forwarded incidents appear in the HPOM message browser. These messages in the HPOM browser are associated with the original incidents reported in NNMi.

NOTE Incidents are forwarded from NNMi to HPOM using Incident Web Service. For the older integration for NNM 7.xx, events are forwarded from NNM to HPOM using the opctrapi mechanism. See “NNM 7.xx and HPOM” on page 225 for more information.

Configuring the Web-Service Implementation

The NNMi–HPOM integration is installed automatically with the HPOM installation. HP Incident Web Service (IWS), a pre-requisite for the integration, is also an integral part of the HPOM installation.

NOTE For details about installation and configuration tasks that you must carry out on HP Network Node Manager i-series Software (NNMi) management servers, see the *HP NNMi Software Deployment and Migration Guide*.

1. On the NNMi management server, perform the following configuration steps:

   a. Configure NNMi incident forwarding to HPOM.

   b. Customize the integration.

   Refer to the *HP NNMi Software Deployment and Migration Guide* for details.

2. In HPOM, create a managed node for each NNMi node that will be named as a source node in the NNMi incidents that are forwarded to this HPOM management server. Also create a managed node for each NNMi management server that will forward incidents to this HPOM management server.

   Alternatively, you can create one external node to catch all forwarded NNMi incidents. For more information about configuring external nodes using the command-line interface, see the *opcnode(1m)* reference page.

NOTE Make sure that the NNMi nodes, from which the corresponding NNMi incidents originated, are configured in the HPOM database. If you do not set up these NNMi nodes in the HPOM database, then all incidents forwarded from the NNMi server will be discarded by the HPOM management server.

3. In HPOM, add the custom message attributes for NNMi incidents to the active messages browser, as follows:

   a. In the browser, right-click any column heading, and then click `Customize Message Browser Columns`.

   b. On the Custom tab, select from the `Available Custom Message Attributes`, and then click `OK`.

- The custom message attributes for NNMi incidents begin with the text `nnm`.
- The most interesting attributes for NNMi incidents are as follows:

  `nnm.assignedTo`

  `nnm.category`

  `nnm.emittingNode.name`

  `nnm.source.name`

c. *Optional*. To change the order in which the custom message attributes appear in the messages browser, drag a column heading to the new location.

4. *Optional*. On the HPOM system, install additional NNMi tools.

   For details, see "Installing Additional NNMi Tools" on page 240.

Synchronization of Incident Updates

When configured to do so, NNMi forwards incidents to one or more HPOM servers. NNMi will acknowledge or unacknowledge an incident to one or more HPOM installations if that incident's lifecycle state changes to or from closed, respectively. Updates to these forwarded incidents are sent from the HPOM server back to the NNMi server to synchronize the lifecycle state of the incident.

Incident lifecycle state changes are synchronized from NNMi to HPOM and back to NNMi as shown in Table 5-1:

Table 5-1 Synchronization of Incident Lifecycle State Changes

Trigger	Result
Message is acknowledged in HPOM.	Corresponding NNMi incident's lifecycle state is set to Closed.
Message is unacknowledged in HPOM.	Corresponding NNMi incident's lifecycle state is set to Registered.
Incident's lifecycle state is set to Closed in NNMi.	Corresponding HPOM message is acknowledged.

Table 5-1 Synchronization of Incident Lifecycle State Changes

Trigger	Result
Incident's lifecycle state is changed in NNMi from Closed to any other state.	Corresponding HPOM message is unacknowledged.

NNMi Tools

HPOM enables you to launch the NNMi console showing the original incident. You can launch the console in the context of an incident forwarded from NNMi or in the context of an NNMi node that is set up as a managed node in HPOM.

NOTE For the HP NNM 7.xx integration and the HP NNMi *agent* implementation, it is mandatory to deploy an HPOM agent to the NNM management server. The NNMi *web-service* integration does not require the deployment of the HPOM agent to the NNM management server.

Each NNMi incident has a unique identifier. Even where HPOM is consolidating NNMi incidents across multiple NNMi server installations, you can trace a particular incident back to its origin in NNMi and investigate it.

The integration enables you to access NNMi forms, views, and tools from within HPOM. Note that you must configure the integrated NNMi tools before you can use them. For more information about configuring NNMi tools in HPOM, see “Installing Additional NNMi Tools” on page 240.

The NNMi integration with HPOM provides the following tool groups, each of which is described in more detail in the tables that follow:

❏ `NNMi/By Incident`:

  Tools in the `NNMi/By Incident` group require an incident (or message) context to run in. All the information required (incident identifier, source NNMi server name, and port number) is contained in the message forwarded to the HPOM message browser. For more information about the tools in the `NNMi/By Incident` group, see Table 5-2 on page 237.

- `NNMi/By Node` (<*short host name*>):

  Tools in the `NNMi/By Node` group require a node context to run them. For more information about the tools in the `NNMi/By Node` group, see Table 5-3 on page 238.

- `NNMi/General` (<*short host name*>):

  Tools in the `NNMi/General` group are for the use of general NNMi functions, such as starting the NNMi console, looking at open incidents, or checking the status of NNMi processes and services. No context is needed to run these tools. For more information about the tools in the `NNMi/General` group, see Table 5-4 on page 239.

- `NNMi Int-Admin`:

  The `NNMi Int-Admin` group contains a tool, Create Server Apps, that you use to install additional NNMi tools (those in groups `By Node` and `General`) for a specific NNMi server from the HPOM console.

Before you can use the tools in the `By Node` and `General` groups, you need to install them. The installation procedure requires you to specify the NNMi host name and a port number. For more information about installing NNMi tools, see "Installing Additional NNMi Tools" on page 240.

Table 5-2 on page 237 lists the NNMi tools included in the `By Incident` group created during the integration procedure.

Table 5-2 **Tools in the By Incident Group**

Tool	Action Performed
Incident Form	Launches an incident form corresponding to the selected message in a web browser.
Layer 2 Neighbors	Launches a troubleshooting view in a web browser, showing the layer-2 neighbors of the node from which the corresponding NNMi incident originated.
Layer 3 Neighbors	Launches a troubleshooting view in a web browser, showing the layer-3 neighbors of the node from which the corresponding NNMi incident originated.

Table 5-2 Tools in the By Incident Group (Continued)

Tool	Action Performed
Node Form	Launches a node form in a web browser, showing the NNMi setup information for the node from which the corresponding NNMi incident originated.

Table 5-3 on page 238 lists the NNMi tools included in the `By Node` group created during the integration procedure.

Table 5-3 Tools in the By Node Group

Tool	Action Performed
Comm. Configuration	Launches the real-time results of the ICMP and SNMP configuration report in a web browser, showing the communication configuration of a selected node.
Configuration Poll	Launches the configuration poll of a selected node, showing the real-time results of a node's configuration in a web browser.
Layer 2 Neighbors	Launches a Troubleshooting View in a web browser, showing the Layer 2 Neighbors of a selected node.
Layer 3 Neighbors	Launches a Troubleshooting View in a web browser, showing the Layer 3 Neighbors of a selected node.
Node Form	Launches a Node Form in a web browser, showing details about the selected node for troubleshooting purposes.

Table 5-3 **Tools in the By Node Group (Continued)**

Tool	Action Performed
Ping	Launches the `ping` command and shows the real-time results of the ping from the NNMi server to a selected node in a web browser.
Status Poll	Launches the real-time check and results of a node's status in a web browser.
Traceroute	Launches the real-time results of the Trace Route command in a web browser.

Table 5-4 on page 239 lists the NNMi tools included in the `General` group created during the integration procedure.

Table 5-4 **Tools in the General Group**

Tool	Action Performed
My Incidents	Launches the My Open Incidents view in a web browser.
NNMi Console	Launches the NNMi console.
NNMi Status	Launches a report of the current status of all NNMi server processes and services in a web browser.
Open RC Incidents	Launches the Open Root Cause Incidents view in a web browser.
Sign In/Out Audit Log	Displays the current configuration for a node in a web browser (tracks log-in and log-out activity for each user account).

Installing Additional NNMi Tools

You can also install additional NNMi-specific tools in the main NNMi tools group. The additional tools are placed in the following groups:

- `General`:

  For more information about the `General` tools group and the NNMi-specific tools it contains, see Table 5-4 on page 239.

- `By Node`:

  For more information about the `By Node` tools group and the NNMi-specific tools it contains, see Table 5-3 on page 238.

- `By Incident`:

  For more information about the `By Incident` tools group and the NNMi-specific tools it contains, see Table 5-2 on page 237.

You can install the additional tools for a specific NNMi management server using one of the following methods:

- NNMi application-installation script:

  For more information about the NNMi Application Installation script see “NNMi Application Installation Script” on page 240.

- `Create Server Apps` tool:

  For more information about the `Create Server Apps` tool, which you can start in the HPOM console, see “Create-Server-Applications Tool” on page 242

NNMi Application Installation Script HPOM provides a dedicated script, NNMi Application Installation, that enables you to install additional tools. You can execute the script with or without specifying the server parameters. For example, if you want to choose your own short host name for labeling the tools group you are installing, execute the script *without* entering the server parameters.

Installing NNMi Application with Server Parameters

To run the NNMi Application Installation script by specifying the server parameters, use the `create_nnm_appls.sh` script as follows:

```
# /opt/OV/contrib/OpC/NNMi-Appls/create_nnm_appls.sh
<fully qualified host name> <server port number>
```

This script specifies the fully qualified host name and the server port number.

The tools group is created in the main NNMi group, and is identified by the short host name. The short host name is created automatically using the first part of the fully qualified host name (truncated at the first dot).

Installing NNMi Application without Server Parameters

To run the NNMi Application Installation script without specifying the server parameters, perform the following steps:

1. Create NNMi applications by running the following script:

   ```
   # /opt/OV/contrib/OpC/NNMi-Appls/create_nnm_appls.sh
   ```

2. Specify the NNMi server by responding to prompts for information, for example: the fully qualified host name of the NNMi server system, a short host name, and the port number to use for connections and communication, for example:

   ```
   # create_nnm_appls.sh
   Full qualified name of the NNMi system:
   nnmsv1.example.com

   Short name of the NNMi system [nnmsv1]:
   Server 1

   Port to access the NNMi system [8004]:
   8004
   ====================================================
   System Name: nnmsv1.example.com
   Short Name:  Server 1
   Port:        8004
   ====================================================
   Are these parameters correct?
   Press [ENTER] to proceed or [^C] to cancel.
   Done
   ```

3. Verify that the information you entered is correct, and press ENTER to install the tools.

The new tools group created in the main `NNMi` group is identified by the short host name which you provided in response to the prompt during installation. You can move the group to a more suitable place if desired.

4. Assign the created tools or tools groups to the appropriate operators.

   Operators might be required to reload the configuration if they are working in the user interfaces, when the change takes place. To reload the configuration to a running interface, use the feature `File -> Reload Configuration`.

Create-Server-Applications Tool You can install the additional NNMI tools directly from within the HPOM console by using the `Create Server Apps` tool. The new tools group is created in the main `NNMi` tools group and is identified by the short host name. The short host name is created automatically using the first part of the fully qualified host name (truncated at the first dot).

Creating NNMi Tools from the HPOM Console

To install the additional NNMi tools using the `Create Server Apps` tool, perform the following steps:

1. In the HPOM console, double-click `Tools`, and then double-click `NNMi Int-Admin`.
2. Right-click `Create Server Apps` and select `Start Customized`.

NOTE If you try to start the `Create Server Apps` tool by double-clicking, an error is reported in the output window.

3. In the dialog box that opens, select the node on which you want to run the `Create Server Apps` tool. Click `Next` to continue.
4. Enter additional information needed to run the tool.

   In the Additional Parameters field, enter the fully qualified host name of the NNMi server and its port number. Click `Finish` to end the installation of the additional NNMi tools.

5. Select `File –> Reload Configuration`.

   The Configuration Status window opens. Click `OK` when the reload is done.

Launching NNMi Tools from the HPOM Console

The tools listed in the section "NNMi Tools" on page 236 can only be run after you install them. For more information about installing NNMi tools, see "Installing Additional NNMi Tools" on page 240. For more information about using the tools you install, see the follow sections:

- "Launching an NNMi Incident Form" on page 243
- "Launching the NNMi Console" on page 243

Launching an NNMi Incident Form To launch an NNMi Incident Form from within the HPOM console, perform the following steps:

1. Browse the list of messages in the HPOM Message Browser and locate a message forwarded from NNMi.
2. Right click the NNMi message, and select the following menu option: `Start` **->** `NNMi` **->** `By Incident` **->** `Incident Form`

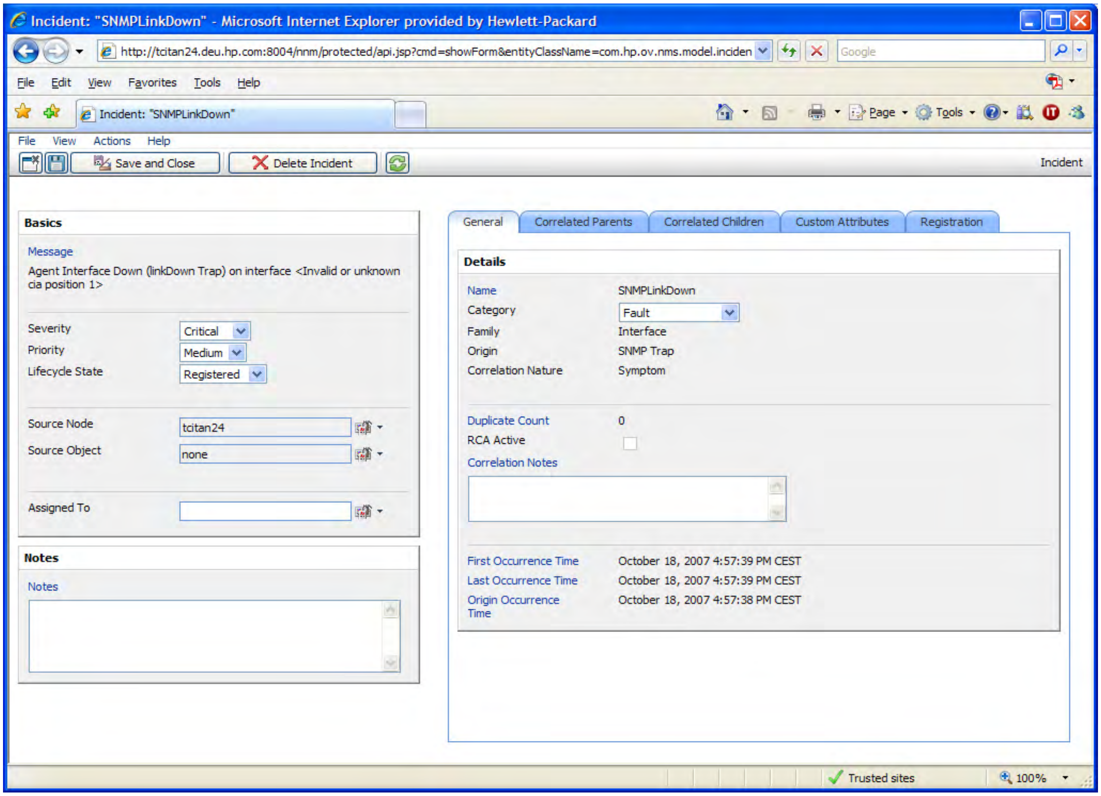
   The first time you run the tool, the log-in screen for NNMi opens and prompts for login credentials.
3. Enter a user name and password and click `Sign-In`. The NNMi Incident Form opens as illustrated in Figure 5-1 on page 244.

Launching the NNMi Console To launch the NNMi console from the HPOM user interface, perform the following steps:

1. Select the following menu option: `Tools -> NNMi`
2. Select the following tool: `General (<host>)`, where **<***host***>** is the short host name of the NNMi server that you want to log in to.
3. Select the following tool: `NNMi Console`

   When NNMi displays the log-in screen, enter the `User Name` and `Password` and then click `Sign-In` to open the NNMi console.

Figure 5-1 NNMi Incident Form



Web Browser Settings

You must configure the web browser settings for the console according to operating-system platform, as follows:

- ❏ Windows platforms:

  Configure the console to use either an external web browser or the Internet Explorer ActiveX control.

- ❏ Other platforms:

  Configure the console to use an external web browser.

NOTE Choose a web browser that is supported by HP NNMi 8.xx.

Modifying Web-Browser Settings

To check or change the web-browser settings for the console, perform the following steps:

1. In the Toolbar, click `Edit`, then click `Preferences`.
2. Click the `Web Browser` tab in the Preferences dialog box.
3. Select the browser settings as appropriate for your platform.
4. Click `OK`.

HP Performance Agent Integration with HPOM

HPOM supports the HP Performance Agent, which is provided as a separate installation package and you can deploy directly from the HPOM management server. You can accept default configurations or set parameters to collect data for specific conditions

HP Performance Agent collects, summarizes, time stamps, and detects alarm conditions on current and historical resource data across your system. It provides performance, resource, and end-to-end transaction response time measurements, and supports network and database measurement information.

The HP Performance Agent integration must be installed on the same system as the HPOM management server. For detailed instructions on the HP Performance Agent installation, configuration, and usage, see the documentation provided with the HP Performance Agent, for example:

❏ *HP Performance Agent Deployables Installation Guide*

❏ *HP Performance Agent Deployables User Guide*

NOTE HP Performance Agent documentation is available in the `Performance Agent` directory at the following location:

http://support.openview.hp.com/selfsolve/manuals

Installing the HP Performance Agent Integration

To make use of the HPOM integration with HP Performance Agent, you must install and configure it, as follows:

1. Install HP Operations management server.

   For information about the installation and configuration of the HPOM management server installation, refer to the *HPOM Installation Guide for the Management Server*.

2. Install the HP Performance Agent on the management server system.

   For information about installation prerequisites and installation instructions, refer to the *HP Performance Agent Deployables Installation Guide*.

   After installing HP Performance Agent deployables on the management server, you can perform the following tasks from the management server:

   - Deploy HP Performance Agent to the managed nodes.
   - Configure the HP Performance Agent from the management server using a set of configuration (ConfigFile) policies.
   - Manage the HP Performance Agent from the management server using a set of pre-configured tools.

3. Assign the platform specific subagent policy `PA_Deploy_`*`<platform>`* to the node where you want to have HP Performance Agent using the following command:

   ```
   # opcnode -assign_pol pol_name=PA_Deploy_<platform>
   pol_type=Subagent version=1.0 node_name=<node_name>
   net_type=NETWORK_IP
   ```

<platform>	Name of the operating system on the managed node (for example, AIX).
<node_name>	Name of the node where you you want to install the HP Performance Agent.

4. Deploy the HPOM subagent package on one or more systems.

The package responsible for the integration of the HPOM with HP Performance Agent is supplied with HPOM subagent and is installed during the subagent installation on the managed node. For the subagent installation procedure, see the “Subagent Installation on Managed Nodes” on page 49.

See the *HP Performance Agent Deployables User Guide* for further information about configuring, managing, and removing the HP Performance Agent.

Data Integration with HP Performance Agent

Data collected outside HP Performance Agent can be integrated using data source integration (DSI) capabilities. For example, network, database, and your own application data can be integrated through DSI. The data is treated the same as data collected by HP Performance Agent. All DSI data is logged, time stamped, and can be alarmed on.

Data Analysis with HP Performance Agent

All of the data collected or received by HP Performance Agent can be analyzed using spreadsheet programs, HP analysis tools such as HP Performance Manager, or third-party analysis products. HP Performance Manager is optionally provided on separate media.

Data Logging with HP Performance Agent

The comprehensive data logged by HP Performance Agent enables you to perform the following actions:

- ❏ Characterize the workloads in the environment.
- ❏ Analyze resource usage for load balancing.
- ❏ Perform trend analysis to isolate and identify bottlenecks.
- ❏ Perform service-level management based on transaction response time.
- ❏ Perform capacity planning.
- ❏ Respond to alarm conditions.
- ❏ Solve system management problems before they arise.

6 Notification Services and Trouble-Ticket Systems

In this Chapter

This chapter explains what you need to consider when configuring a link between HPOM and an external notification service or an external trouble-ticket system. The information in this chapter explains how to write scripts and programs to automatically call an external notification service or an external trouble-ticket system when a message is received on the management server. It also describes the high-level steps used to integrate an external notification service or trouble-ticket system into HPOM. Finally, this chapter describes the parameters provided by HPOM to call a notification service, and to forward a message to a trouble-ticket system.

The information in this section covers the following topics:

Notification Services and Trouble-Ticket Systems

You can configure HPOM to automatically call an external notification service or an external trouble-ticket system when a message is received on the management server. You can set up programs and scripts to notify users by modem, telephone, or email. You can also send event-specific details to a trouble-ticket system you have predefined.

- Notification service:

  A notification service can be any form of communication that is used to inform an operator of a very important event. For example, you could use a pager, send a Short Messaging Service (SMS), or an email. HPOM allows you to set up different notification mechanisms for each of your operators. In addition, you can schedule your external notification services according to a timetable.

- Trouble-ticket system:

  Trouble-ticket systems are used to document, track, and help resolve reported problems.

- HP service desk:

  HP Service Desk is enables yo to manage all aspects of your business processes. Service Desk has been tightly integrated with HPOM. You can configure HPOM to send all events or specific events to Service Desk. The event information is mapped to a Service Desk incident. The first time an event is sent an incident is created in Service Desk. Service Desk is then the owner of that event. The import mapping in Service Desk defines which event attributes will be imported into the Incident fields. See `www.openview.hp.com` for more information about this integration.

Scripts and Programs

HPOM enables you to write your own script or program that calls an external interface such as a notification service or a trouble-ticket system. The script serves as a link between HPOM and the notification service or trouble-ticket system.

HPOM provides an example script that shows you how to call and make use of an external notification service or trouble-ticket system. The following script sends an email to all operators responsible for the message that is configured to call the service or trouble-ticket system:

`/opt/OV/bin/OpC/extern_intf/ttns_mail.sh`

Guidelines for Writing Scripts and Programs

When writing your script or program, note the following important guidelines:

- ❏ Default directory:

  For scripts and programs calling external interfaces, you can use the following default directory provided by HPOM:

  `/opt/OV/bin/OpC/extern_intf`

CAUTION If you place your scripts and programs in this directory, they will be erased when you de-install HPOM.

- ❏ Shell scripts:

  Scripts are executed under the account of the user who started the HPOM server processes. In most cases this is the user root.

  If your script is a shell script, the first line must contain a statement such as the following:

  `#!/usr/bin/sh`

  This statement ensures that the shell for which your script is designed is used during execution, and not the shell of the user who executes the script.

CAUTION If the first line of your shell script does not contain this statement, the execution of your script or program may fail.

- ❑ Default Parameters:

  HPOM sends its own message parameters to the external interface. You may *not* use a command that requires additional parameters. For a list of the parameters provided by HPOM, see “Parameters for Notification Services and Trouble-Ticket Systems” on page 257.

Integration of Notification Services and Trouble-Ticket Systems

This section explains how to integrate an external notification service or trouble-ticket system with HPOM. The high-level steps described in this section provide you with an overview of the following configuration tasks:

- ❏ "Configuring Notification Services" on page 254
- ❏ "Configuring Trouble-Ticket Systems" on page 255

Configuring Notification Services

To configure an external notification service for integration with HPOM, perform the following steps:

1. Set up the notification service.

   To set up a notification service, do the following:

   a. Write a script or program that calls the notification service.

      For details, see "Guidelines for Writing Scripts and Programs" on page 252.

   b. Set up a notification method by using the `opcnotiservice` command. For more information about command options and parameters, refer to the reference page for the *opcnotischedule(1m)* command.

2. Set the notification schedule.

   To set a notification schedule, use the `opcnotischedule` command and configure the following values:

   a. The schedule that your external notification services must adhere to, according to a defined timetable.

   b. The notification services used and at what time during the week.

   For example, you could schedule a phone call at work during working hours, and a phone call at home during evenings and weekends. For more information about command options and parameters, refer to the reference page for the *opcnotischedule(1m)* command.

3. Set external notification for a message condition:

   Configure messages to be forwarded to the external notification service according to the schedule you set. Define which messages send external notifications by setting a switch in the corresponding condition in the policy.

TIP Instead of modifying each condition separately, you can set up a global flexible-management policy for service hours and scheduled outages. The global policy defines which messages are forwarded to the notification service. See “Forwarding Messages to a Trouble Ticket or Notification Interface” on page 111 for more information.

Configuring Trouble-Ticket Systems

To configure a trouble-ticket system for integration with HPOM, perform the following steps:

1. Set up the trouble-ticket system.

   a. Write a script or program that calls the trouble-ticket system.

      For details, see “Guidelines for Writing Scripts and Programs” on page 252.

   b. Set up a trouble-ticket call by using the `opctt` command with the `-enable` parameter, as follows:

      ```
      /opt/OV/bin/OpC/opctt -enable /opt/OV/bin/OpC\
      /extern_intf/ttns_mail.sh
      ```

      For more information about the `opctt` command and permitted parameters, refer to the `opctt(1m)` reference page.

2. Forward messages to a trouble-ticket system.

   Configure messages to be forwarded to the trouble-ticket system. For example, define which messages are forwarded to the trouble-ticket system by setting a switch in the corresponding condition in the policy.

TIP

Instead of modifying each condition separately, you could also set up a global flexible-management policy for service hours and scheduled outages to define which messages are forwarded to the trouble-ticket system. See "Forwarding Messages to a Trouble Ticket or Notification Interface" on page 111 for more information.

Sending event-specific details to a predefined trouble-ticket system offers no scheduling functions. This feature is always active unless you choose to disable it by using the `opctt` command.

Parameters for Notification Services and Trouble-Ticket Systems

To call a notification service or forward a message to a trouble-ticket system, HPOM uses the parameters listed in Table 6-1 on page 257.

Table 6-1 Permitted Parameters for Notification Services and Trouble-Ticket Systems

Parameter	Description	Example
1	Unique message number.	`c1c79228-ae12-71d6-1a8f -0f887ebe0000`
2	Message node name.	`hpbbxyz3.bbn.hp.com`
3	Node type.	`HP 9000 PA-RISC`
4	Date (`mm/dd/yyyy`) on which the message was received on the managed node in the time zone (system-specific `TZ` variable) of the management server.	`08/02/2002`
5	Time (`hh:mm:ss`) at which the message was received on the managed node. This time uses a 24-hour clock in the time zone (system-specific `TZ` variable) of the management server.	`16:22:04`
6	Date (`mm/dd/yyyy`) on which the message was received on the management server in the time zone (system-specific `TZ` variable) of the management server.	`08/02/2008`

Table 6-1 Permitted Parameters for Notification Services and Trouble-Ticket Systems (Continued)

Parameter	Description	Example
7	Time (`hh:mm:ss`) at which the message was received on the management server. This time uses a 24-hour clock in the time zone (system-specific `TZ` variable) of the management server.	`16:22:05`
8	Application name.	`/bin/su(1) Switch User`
9	Message group.	`Security`
10	Object name.	`root`
11	Message severity	`unknown`, `normal`, `warning`, `minor`, `major` or `critical`
12	List of responsible HPOM operators. Names are separated with one space.	`opc_op Bill John`
13	Message text. Note that text is *not* enclosed in quotes ("").	`Succeeded switch user to root by charlie`
14	Instructions (empty string if not available). The instructions are passed without quotation marks (""), backslashes (\), or other characters that might be interpreted by a UNIX shell.	`This is the instruction text for the appropriate message condition. It is available for the operator when a message matching this condition displays in the Message Browser.`
15	Custom message attributes (empty string if not available). Multiple *`name=value`* pairs are separated with two semi-colons (`;;`).	`Customer=Hewlett-Packard;;Country=United States of America`

Table 6-1 Permitted Parameters for Notification Services and Trouble-Ticket Systems (Continued)

Parameter	Description	Example
16	Number of suppressed duplicate messages. The number is `0` unless at least one of the following parameters has been set to `TRUE` using the `ovconfchg` command-line tool: • `OPC_NOTIF_WHEN_DUPLICATE` Passes duplicates to the interfaces with a 16th parameter containing the duplicate counter. The counter is zero if it is the first message or this feature is not switched on. • `OPC_TT_WHEN_DUPLICATE` Passes messages to trouble-ticket systems even if they are duplicates of other messages.	`14`

7 HPOM Language Support

In this Chapter

The information in this chapter describes the language dependencies of the HP Operations Manager (HPOM) management server processes, managed node commands and processes, and the Java GUI. You can also find information about the languages, `LANG` settings, and character sets that the various HPOM platforms support.

Language Support on the Management Server

On the HP Operations management server, localization considerations determine the following:

- ❏ Language:

  Language used to display status messages from the HP Operations server and managed nodes in the HPOM Java GUI.

- ❏ Character set:

  Character set used for internal processing.

Setting the Language on the Management Server

HPOM uses the `LANG` environment variable to determine the language of the message catalog and most HP Operations management server processes.

When you start the HP Operations management server processes (with `ovc -start` or `opcsv -start`), HPOM evaluates the currently set locale and selects the related message catalog to be used. The evaluation and the selection usually take place during the system boot.

The `opcsv -start` command is run on the management server from within the shell script `omu500`, which you can find in the following location:

- ❏ HP-UX:

  `/sbin/init.d/omu500`

- ❏ Linux:

  `/etc/rc.d/init.d/omu500`

- ❏ Solaris:

  `/etc/init.d/omu500`

At this point, the `LANG` variable is set to `C` or not yet set.

If you want the HP Operations server processes to send their status messages in a different (supported) language, set `LANG` before `opcsv -start` is called, or restart the services after you have changed the locale.

Because of certain platform restrictions, it is possible that some messages are still displayed in the original installation language.

Types of Language Variables for the Management Server

With HPOM, only UTF-8 encoding is supported. UTF-8 encoding enables the usage of multilingual characters in different HPOM elements, and eliminates the problems derived from the character set incompatibility. Therefore, you must set up a UTF-8 based locale to ensure the proper operation of the management server.

The settings for the `LANG` variable listed in Table 7-1 are supported for the management server. HPOM has been verified to run in these languages.

Table 7-1 LANG Settings for the HP Operations Management Server

Language	LANG (HP-UX)	LANG (Solaris)
Czech	`cs_CZ.utf8`	`cs_CZ.UTF-8`

English	`C` [a]
	`C.utf8`
	`en_US.utf8`
		`C` [a]
		`en_US.UTF-8`

French	`fr_FR.utf8`	`fr_FR.UTF-8`
German	`de_DE.utf8`	`de_DE.UTF-8`
Italian	`it_IT.utf8`	`it_IT.UTF-8`
Spanish	`es_ES.utf8`	`es_ES.UTF-8`
Japanese	`ja_JP.utf8`	`ja_JP.UTF-8`
Korean	`ko_KR.utf8`	`ko_KR.UTF-8`
Russian	`ru_RU.utf8`	`ru_RU.UTF-8`
Simplified Chinese	`zh_CN.utf8`	`zh_CN.UTF-8`
Traditional Chinese (Taiwan)	`zh_TW.utf8`	`zh_TW.UTF-8`

a. ASCII is a subset of UTF-8. If only English ASCII characters will be used, it is possible to use `C` as `LANG`. However, even in this case, the usage of the UTF-8 locale is recommended. Otherwise, any multilingual data may be lost, or cause errors.

Setting the Database Character Set on the Management Server

The database character set specified during the HPOM installation determines the character set used for internal processing of data on the management server. Note that HPOM supports only the `AL32UTF8` character set for the database. *All* data on the management server must be entered with UTF-8 encoding.

In most cases you can accept the default value for the Oracle-database character set used by HPOM, which is `american_america.AL32UTF8`. If you use another value for `NLS_LANG`, the desired value must use the `AL32UTF8` character set. Make sure that you specify the desired value for the Oracle-database character set *before* starting the HPOM installation. You can specify the character set that HPOM uses with the following command:

```
# export NLS_LANG=<value>
```

HPOM supports the Oracle database character sets listed in Table 7-2.

Table 7-2 Supported Database Character Sets and `NLS_LANG` Values

Language	Character Set	NLS_LANG Value
US English	AL32UTF8	american_america.AL32UTF8
Spanish	AL32UTF8	spanish_spain.AL32UTF8
Japanese	AL32UTF8	japanese_japan.AL32UTF8
Korean	AL32UTF8	korean_korea.AL32UTF8
Simplified Chinese	AL32UTF8	simplified chinese_china.AL32UTF8[a]
Other	AL32UTF8	american_america.AL32UTF8

a. The space in `NLS_LANG` is required.

Setting Up the User Environment

All the elements in the environment that are used to access the HPOM management server must be configured to accept UTF-8 input and output. When setting up the user environment, consider the following:

❑ Keyboard:

  The keyboard layout (and code page) for the keyboard used to provide information sent to the HPOM management server must be able to input UTF-8 characters.

❑ Terminal program:

  If you use a terminal program to access the HPOM management server, you must configure it to correctly to send the user input as UTF-8. The terminal program must be able to interpret the management server's response as UTF-8 as well.

  Depending on the context, you must enable certain options, for example: by starting the terminal with special parameters, or even recompiling the terminal program with a multi-byte option.

❑ Fonts:

  A font capable of displaying Unicode characters must be used for the terminal that accesses the HPOM management server.

For detailed information about configuring the keyboards and terminal programs that are used to access the HPOM management server, refer to the system documentation for the program or operating system you are using.

Language Support on Managed Nodes

Table 7-3 and Table 7-4 show the languages HPOM supports for HPOM internal messages on managed nodes.

Table 7-3 Language Support for HPOM Internal Messages

Management Server OS	Managed Node OS	English	Japanese
HP-UX, Linux Sun Solaris	AIX	✔	✔
	HP-UX	✔	✔
	Linux	✔	✔
	Solaris	✔	✔
	Windows	✔	✔

Table 7-4 Language Support for HTTPS Agents Only

Management Server OS	Managed Node OS	Spanish, Korean, Simplified Chinese
HP-UX, Linux Sun Solaris	HP-UX	✔
	Linux	✔
	Solaris	✔
	Windows	✔

NOTE Windows managed nodes use the System Language. A *LANG* environment variable is not available.

Language Settings for Messages on Managed Nodes

The managed-node processes use the value of the locale variable to determine the language of HPOM messages. For example, if you want the managed-node processes to generate messages in Japanese, you must set the locale and language variable accordingly before you call `opcagt -start`.

NOTE HPOM generates only English and Japanese internal HPOM messages on the managed nodes. If you have policies in any other language, make sure that the HPOM agents use the English message catalogs.

Setting the Language of Messages on a Managed Node

To set the language of messages on a managed node, perform the following steps:

1. Set the locale for the HPOM agents in the system-startup script.
2. Set `START_LANG` for the locale in which you want the HPOM agent to start.
3. Restart the agents.

Locations of System Resource Files

For the location of the system resource files adapted by HPOM on all supported agent platforms, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

Character-Set Synchronization on the HPOM Agent

The output of HPOM agent commands (for example, `opcagt -status`) uses the internal character set configured for the agent. For this reason, when the locale of the terminal window in which you execute the command is different from the internal character set of the agent, the output is not readable. If the agent has the internal UTF-8 character set, use a UTF-8 terminal window.

File-Set Requirements on Managed Nodes

Some operating systems require the installation and availability of a specific file set to convert code sets. See the *HPOM Software Release Notes* for software requirements on all managed node platforms.

Character-Set Settings on the Managed Nodes

The character sets available on platforms supported by HPOM can differ from the character set used in the HPOM database. Consequently, when a message is generated on a managed node, it must often be converted before it can be sent to the management server and stored in the database. HPOM takes care of this conversion. If necessary, automatic character set conversions take place through HPOM managed node processes before a message is sent to the server.

NOTE UTF-8 is the recommended character set, especially for environments that use multilingual characters.

Character-Set Types in English or Spanish Environments

Table 7-5 shows the character sets for the English and Spanish languages that are supported for HPOM managed nodes.

NOTE HPOM automatically sets the default of the internal agent character set to the character set supported by the lowest version of the operating system.

Table 7-5 Verified Character Sets on Managed Nodes (English/Spanish)

HPOM	Platform	Character Set
Management server on HP-UX, Linux, and Sun Solaris	HP-UX, Solaris	UTF-8, ISO 8859-15, ISO 8859-1, ROMAN8, ASCII
	AIX, Linux, Solaris	UTF-8, ISO 8859-15, ISO 8859-1, ASCII
	Windows	UTF-8, multilingual ANSI Code Page 1252[a], ASCII

a. Code Page 1252 is analogous to ISO 8859-1.

Character Sets in Japanese Environments

Table 7-6 shows the character sets for the Japanese language that are supported for HPOM managed nodes.

Table 7-6 Verified Character Sets on Managed Nodes (Japanese)

HPOM	Platform	Character Set
Management server on HP-UX, Linux, and Sun Solaris	HP-UX, Solaris	UTF-8, Shift JIS, EUC[a], ASCII
	Linux	UTF-8, EUC[a], ASCII
	Windows	UTF-8, Japanese ANSI Code Page 932 [b], ASCII
	AIX	UTF-8, Shift JIS, EUC[a], ASCII

a. 2-byte Extended UNIX Code.
b. Code Page 932 is analogous to Shift JIS.

External Character Sets on Managed Nodes

All commands for HPOM managed nodes (for example, `opcmsg(1M)` or `opcmon(1M)`) as well as the APIs of the Developer's Toolkit use the locale setting to interpret the character set of their command-line arguments. This character set can be different from the database character set and the managed-node processing character set. All command input is also converted before it is acted on by any managed-node processes.

NOTE UTF-8 is the recommended character set, especially for environments that use multilingual characters. If UTF-8 is selected as the external character set, the internal character set of the node should also be UTF-8.

Character-Set Types in English-Language Environments

Table 7-7 shows the values of *LANG* and the related *external* character set in an English-language environment on HPOM.

Table 7-7 External Character Sets in English/Spanish Environments

Node Platform	LANG	External Character Set
AIX	<*lang*>.8859-15 C <*lang*>.ISO8859-1 <*lang*>.IBM-850 <*lang*>.UTF-8	ISO 8859-15 ASCII ISO 8859-1 OEM Code Page 850 UTF-8
HP-UX 11.x	<*lang*>.iso885915 <*lang*>.iso885915@euro C <*lang*>.roman8 <*lang*>.iso88591 C.utf8 / <*lang*>.utf8	ISO 8859-15 ISO 8859-15 ASCII ROMAN8 ISO 8859-1 UTF-8
Linux	<*lang*>@euro C <*lang*> <*lang*>.UTF-8	ISO 8859-15 ASCII ISO 8859-1 UTF-8
Solaris	<*lang*>.ISO8859-15 C <*lang*> <*lang*>.UTF-8	ISO 8859-15 ASCII ISO 8859-1 UTF-8
Windows	*LANG* variable not available	OEM Code Page 850 OEM Code Page 437 ANSI Code Page 1252 ASCII UTF-8

The <*lang*> variable refers to any language that is supported by the operating system. Although it is possible to specify literally any language in this field, you can receive HPOM internal messages only in a language supported by HPOM. HPOM only uses the value of *LANG* to determine the external character set.

External Character Sets in Japanese Environments

Table 7-8 shows the values of *LANG* and the related external character set in a Japanese-language environment.

Table 7-8 External Character Sets (Japanese)

Node Platform	LANG	External Character Set
AIX	C ja_JP ja_JP.IBM-932 ja_JP.IBM-eucJP ja_JP.UTF-8	ASCII Shift JIS EUC UTF-8
HP-UX	C ja_JP.SJIS ja_JP.eucJP ja_JP.utf8	ASCII Shift JIS 2-byte EUC UTF-8
Linux	C ja_JP ja_JP.eucJP ja_JP.UTF-8	ASCII EUC EUC UTF-8
Solaris	C ja_JP.PCK ja ja_JP.UTF-8	ASCII Shift JIS EUC UTF-8

Table 7-8 External Character Sets (Japanese) (Continued)

Node Platform	LANG	External Character Set
Windows	*LANG* variable not available	ANSI Code Page 932 ASCII UTF-8

The <*lang*> variable refers to any language that is supported by the operating system. Although it is possible to specify literally any language in this field, you can receive HPOM internal messages only in a language supported by HPOM.

Character Sets Supported by the Logfile Encapsulator

The HPOM Logfile Encapsulator can monitor files with different character sets. You can specify a character set for each file monitored by HPOM. The character set can be different from the character set defined for that managed node but must be compatible.

NOTE If you are using ASCII as the character set for internal processing, you must also specify ASCII as the character set for the monitored logfile messages.

ASCII is a subset of Shift JIS. You risk loss of data if you monitor Shift JIS logfiles by running the HPOM agent in ASCII mode.

Table 7-9 shows all the supported character sets for various logfile messages.

Table 7-9 Character Sets Supported by the Logfile Encapsulator

Character Set	Windows Nodes		HP-UX, Solaris, Linux, AIX, Nodes		Net Ware Nodes	Other Nodes
	English Spanish	Japanese	English Spanish	Japanese	English	English
ASCII	✔	✔	✔	✔	✔	✔
ISO 8859-15			✔		✔	✔
ISO 8859-1			✔		✔	✔
ROMAN8			HP-UX			
American EBCDIC			HP-UX			
Multilingual OEM code page 850	✔		AIX		✔	
OEM US code page 437	✔				✔	
Multilingual ANSI code page 1252	✔				✔	
Japanese ANSI code page 932		✔				
Shift JIS				✔		
EUC (2-byte Extended UNIX code)				✔		

NOTE Code Page 932 or Code Page 1252 are the only character sets valid for the Event Log.

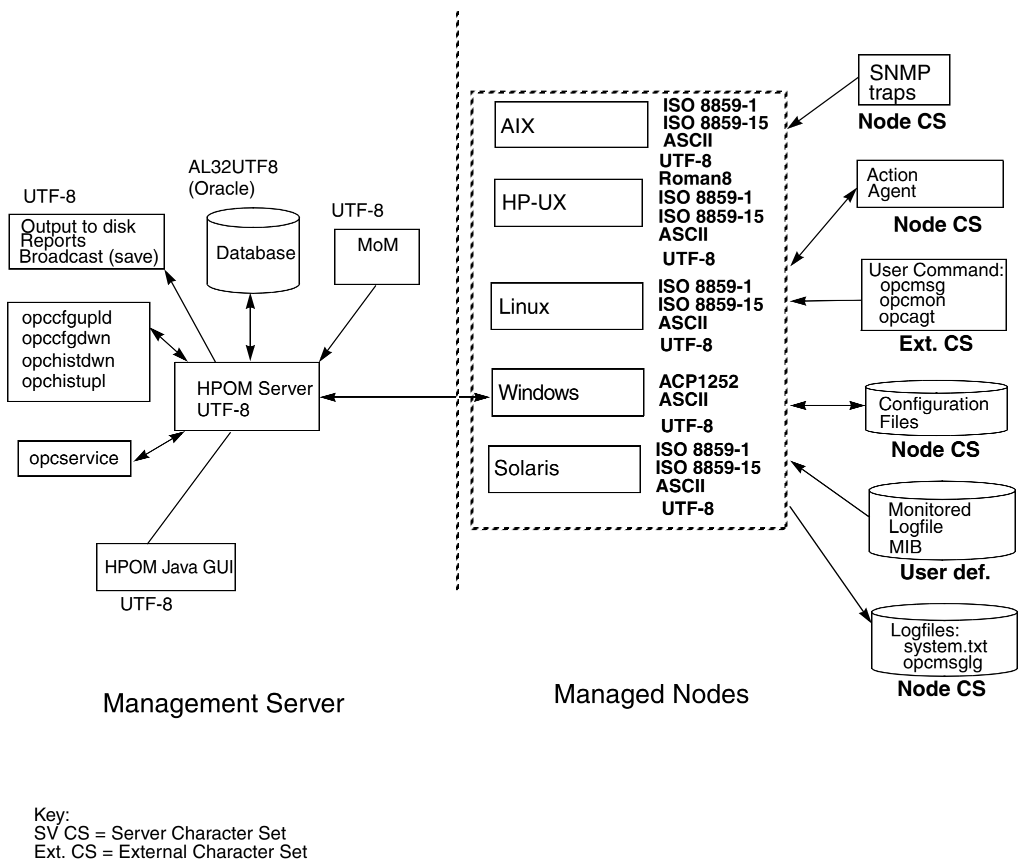
Character-Code Conversion in HPOM

The information in this section describes how to configure HPOM and related character sets in English- and Japanese-language environments.

English-language Management-Server Configuration

Figure 7-1 shows the HPOM configuration and related character sets on an English-language management server.

Figure 7-1 Configuration and Related Character Sets (English)



Management-Server Files

On an English-language management server, HPOM uses the UTF-8 character set to do the following:

- ❏ Process local logfile entries (`System.txt`), temporary queue file, and so on.
- ❏ Upload and download the HPOM configuration.
- ❏ Upload and download the HPOM history messages.
- ❏ Service Navigator configuration management with `opcservice`.

Managed-Node File Conversion

In an English-language environment using the ROMAN8 or ROMAN9 character sets, HPOM does not perform a run-time conversion on the management server. HPOM performs a runtime conversion only for managed node configuration files if the HPOM agents on HP-UX are running with the ROMAN8 character set.

Managed-Node File Processing

In an English-language environment, HPOM processes managed node files as follows:

- ❏ SNMP events:

  Interprets incoming SNMP events in ASCII format.
- ❏ User commands:

  Converts user commands from the external character set to the node character set.
- ❏ Configuration files:

  Does not convert input for configuration files. HPOM always processes configuration files in the node processing character set.
- ❏ Local logfiles:

  Does not convert output for local HPOM logfiles. HPOM always processes the contents of logfiles in the node processing character set.
- ❏ MIB processing:

  Processes MIB files in the HPOM node processing character set.

- ❏ Action agents:

  Before actions are started, action agents receive their input in the management server character set, and convert it into the node processing character set.

For example, in an English-language environment where the character set for the HPOM agent is set to ROMAN8 and the language variable LANG is “de_DE.iso88591”, HPOM processes the contents of managed-node files and `opcmsg` messages as follows:

Input	HPOM converts the `opcmsg` from ISO8859-1 to ROMAN8 before the HPOM message interceptor evaluates the message attributes.
Output	Before forwarding the message to the management server, HPOM converts characters from ROMAN8 to UTF-8 (the database character set).

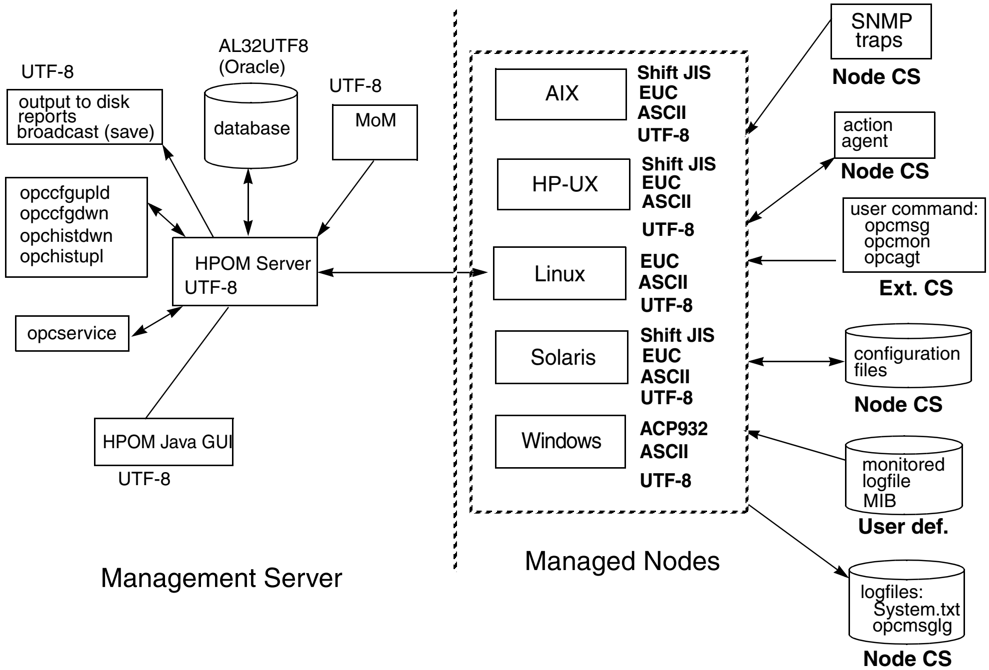
TIP You can use a different character set for each managed node. You determine the managed-node character set by the character sets used in your environment.

On HP-UX, you can define different character sets for different managed nodes. Define the character set most frequently used on each managed node. For example, if you use mostly monitor logfiles with ISO 8859-15 characters, you should use ISO 8859-15 for your managed nodes. When in doubt, use UTF-8.

Japanese-Language Management Server

Figure 7-1 shows the configuration and related character sets on an HPOM management server running in a Japanese-language environment.

Figure 7-2 Configuration and Related Character Sets (Japanese)



Management-Server File Processing with UTF-8

On a Japanese-language management server, HPOM uses the UTF-8 character set to process the contents of files and messages in the following way:

❏ Process local logfile entries (`System.txt`), temporary queue file, and so on.

❏ Upload and download the HPOM configuration.

❏ Upload and download the HPOM history messages.

❏ Service Navigator configuration management with `opcservice`.

File Processing on Managed Nodes

In a Japanese-language environment, HPOM processes managed node files according to the follow rules:

- SNMP events:

  Interprets incoming SNMP events in ASCII format.

- User commands:

  Converts user commands from the external character set to the node character set.

- Configuration files:

  Does not convert input for configuration files. HPOM always processes configuration files in the node processing character set.

- Local logfiles:

  Does not convert output for local HPOM logfiles. HPOM always processes the contents of logfiles in the node processing character set.

- MIB files:

  Processes MIB files in the HPOM node processing character set.

- Action agents:

  Before actions are started, action agents receive their input in the management-server character set and convert it into the node processing character set.

IMPORTANT In a Japanese-language environment, HPOM performs a run-time conversion for managed-node configuration files only if the HPOM agents on HP-UX, Solaris, or AIX are running with the EUC character set. HPOM does not perform a run-time conversion on the management server in a Japanese-language environment.

For example, in an Japanese-language environment where the character set for the HPOM agent on an HP-UX managed node is set to EUC and the language variable LANG is “ja_JP.SJIS”, HPOM processes the contents of managed-node files and `opcmsg` messages as follows:

Input	HPOM converts the contents of the `opcmsg` from Shift JIS to EUC.
Output	Before forwarding the message to the management server, HPOM converts the contents from EUC to UTF-8 (the database character set).

TIP You can use a different character set for each managed node. You determine the managed node character set by the character sets used in your environment.

On HP-UX, you can define different character sets for different managed nodes. Define the character set most frequently used on each managed node. For example, if you use mostly monitor logfiles with Shift JIS characters, you should use Shift JIS for your managed nodes. When in doubt, use UTF-8.

Flexible-Management Configuration in a Japanese-Language Environment

If your management server runs in a Japanese-language environment with the character set UTF-8, you must do one of the following:

❏ Convert the flexible-management configuration files on the management-server from UTF-8 to EUC.

NOTE If the UTF-8 file contains the characters that are not available in EUC, problems may occur when converting the flexible-management configuration files on the management server from UTF-8 to EUC.

❏ Convert the managed nodes from EUC to UTF-8.

Converting Configuration Files

To convert flexible-management configuration files on the management server from UTF-8 to EUC, enter the following:

1. On HP-UX management servers:

   ```
   # /usr/bin/iconv -f utf8 -t euc <mom_orig> > <mom_new>
   ```

2. On Sun SOLARIS management servers:

   ```
   # /usr/bin/iconv -f utf8 -t eucJP <mom_orig> > <mom_new>
   ```

Note the following in the example commands above:

<*mom_orig*> The name of the original flexible-management configuration file in UTF-8

<*mom_new*> The IP address of the managed node in hexadecimal, as returned by the command `opc_ip_addr`.

Troubleshooting Language Environments

The information in this section includes details of specific cases where HPOM functionality does not work as expected in international environments. For more information about installing the HP Operations management server in international environments, see the *HPOM Installation Guide for the Management Server*.

Windows Managed Nodes

In the localized versions of the Windows operating system, the user `Administrator` has been localized. Consequently, the installation of the HP Operations agent software on Windows managed nodes fails because HPOM is trying to install as user `Administrator` while the user has a different name in the Windows operating system.

To avoid problems of this kind, run the `inst.sh` script, and when asked for the user name, enter the localized name of the user.

PC Virtual-Terminal Applications

The application PC Virtual Terminal does not work and is not supported on Windows.

Broadcast-Command Output

The output of the broadcast command is not always readable. This is the case if the command is run in an MS-DOS window that uses an MS-DOS code page that is different from the Windows code page.

Localization of Object Names

Although you can localize most of the HPOM-specific configuration, you must observe a few restrictions. For example, it is mandatory to use ASCII characters when naming the following objects:

- Managed nodes
- Files:

  Examples of files include automatic actions, scheduled actions, monitor scripts and programs, the fully qualified trouble ticket interface, notification services, and the physical console.
- Monitored objects:

  For example, when using `opcmon` to forward values for objects you are monitoring with HPOM.
- Operator names:

  Operator names are used to create corresponding subdirectories and must therefore not be localized.
- Operator passwords
- HPOM administrator password

HPOM uses the name of objects (for example: the policy name, message group name, or node-group name) as an internal identifier. For this reason, you should not localize the names of HPOM objects themselves. Instead, enter the localized string in the Label field. If a label is present, it is shown in the Java GUI instead of an internal name.

8 HPOM Java GUI

In this Chapter

The information in this chapter describes the Java-based graphical user interface (Java GUI) for the HP Operations Manager (HPOM) operator and explains how the HPOM Java GUI is integrated with HP Network Node Manager (NNM). In this section, you can find information about the following topics:

For more detailed information about installation requirements and instructions, refer to the *HPOM Installation Guide for the Management Server*.

Java GUI Overview

This section provides an overview of how the HPOM Java-based operator GUI handles the message browsers. It also describes how windows are refreshed and users are viewed. For more detailed information about the HPOM Java-based operator GUI functionality, refer to the *HPOM Java GUI Operator's Guide*.

The HP Operations Manager Java-GUI provides HPOM operators with a graphical user interface that is extremely easy to use. The Java GUI can runs on any platform where the Java Runtime Environment (JRE) is installed. HPOM enables operators to connect to HPOM running on a variety of platforms. In addition, HPOM operators can access HPOM or the Network Node Manager (NNM) from anywhere, for example: from a laptop on the road, from home, or from a workstation at the office. The Java GUI provides the following high-level features:

❏ Refreshing windows:

  The Java GUI automatically updates the status of nodes, message groups, messages, and services if applicable at a preset interval. In the Java GUI, you can reconfigure this refresh interval. When you press the `[Acknowledge]` button in the `Message Properties` window, the node coloring in the object pane is not immediately updated. However, you can manually refresh the node coloring by pressing the `Refresh` toolbar button or by selecting the menu `View: Refresh`. Or can wait until the next automatic refresh is completed.

❏ Viewing users:

  The Java GUI does not create an entry in the database table `opc_op_runtime` for currently active HPOM users. As a result, the reports listing `Unmonitored` and `Working HPOM Users` do not include Java GUI users.

Message Browsers

The Java GUI message browser provides the following features and functionality:

❏ Customizing message columns:

The HPOM Java GUI lets you resize, move, hide, and change the order of the columns in the message browsers. The Java GUI also lets you sort messages according to message attributes. For example, you can sort messages by date and Time, by node, or by application.

- Displaying messages:

  In the Java GUI, you can choose between displaying all messages or only the most recent messages. You can define the number of messages displayed.

- Setting flags:

  Java GUI does not immediately update the flags in the SUIAONE columns, which indicate message severity, ownership, action availability and status, and so on. In exceptional circumstances, it is possible for an operator-initiated action to complete before the status in the browser is set to started.

- Acknowledging messages:

  To acknowledge messages based on severity, open a View Message Browser, choose a level of severity as the filtering criteria, and acknowledge all messages in the current view. Alternatively, click the `Severity` column in the browser to sort the messages by severity, select the messages with level of severity you want, and acknowledge all messages in the current view.

- Owning messages:

  The Java GUI enables you to own only selected messages. If you want to own *all* messages in a message browser, change the preferences settings so the browser displays all messages, then select and own them all.

Startup Options

This section describes the configuration options evaluated by the Java GUI when it is started with the `ito_op` startup script. When the Java GUI starts, it reads environment options first, then evaluates any command-line options passed with the startup script, and finally considers the contents of the `itooprc` file.

Starting the Java GUI with the ito_op Script

To start the Java GUI with the `ito_op` script, enter the following command:

```
# /opt/OV/www/htdocs/ito_op/ito_op &
```

For more information about the options you can set in the ito_op script and how you can use them to control the look, feel, layout and content of the Java GUI, see the following tables:

- ❏ Table 8-1 on page 289: Communication, security, and display.
- ❏ Table 8-2 on page 292: Layout, content, and workspace.

Table 8-1 shows the options evaluated by the Java GUI in the startup scripts. The options include: settings for communication (ports, proxies, and servers), security, passwords, and so on.

Table 8-1 Startup Script Options Evaluated by the Java GUI

Option	Format	Default Value	Description
`apisid`	<*string*>	OV_JGUI_API	Sets a session ID for the particular Java GUI instance at its startup.
`bbc.http:proxy`	<*string*>	“”	Configures a proxy server for HTTPS-based communication.

Table 8-1 Startup Script Options Evaluated by the Java GUI (Continued)

Option	Format	Default Value	Description
colored_message_lines	yes|no	no	Decides whether whole messages or only the severity column are colored in the message browser.
def_browser	<*filename*>	“”	Specifies the path to the default web browser on localhost.
def_look_and_feel	<*string*>	Windows: com.sun.java.swing.plaf.motif.Motif LookAndFeel	Defines the appearance of the Java GUI.
display	<*host.domain*>:0	<*localhost*>:0	Specifies hostname to which the X application redirects the display.
initial_node	<*string*>	<*localhost*>	Defines hostname of the HPOM management server to which the Java GUI connects.
locale	<*lang_territory*>		Sets locale name.
max_limited_messages	<*int*>	50	Specifies maximum number of messages displayed in a browser
nosec	true|false	false	Starts the SSL Secure Java GUI in standard mode without SSL functionality

Table 8-1 Startup Script Options Evaluated by the Java GUI (Continued)

Option	Format	Default Value	Description
`passwd`	*<string>*	“”	Defines password of the HPOM operator used for login
`port`	*hostname<port_number>* or server *hostname<port_number>*	2531	Sets the port number the Java Gui uses when connecting to the HPOM management server.
`refresh_interval`	*<int>* (seconds)	30	Defines the frequency with which the contents of the message browser are refreshed.
`server`	*<string>*	*<localhost>*	Specifies the hostname of the HPOM management server to which the Java GUI will connect.
`title_suffix`	*<string>*	“”	Displays the string next to the title in the main window.
`trace`	`true|false`	false	Enables the appearance of tracing messages in the terminal.
`user`	*<string>*	“”	Specifies the name of the HPOM operator used to log in.

Table 8-2 on page 292 shows the options and attributes that you can use to control the layout and content of the Java GUI in the startup scripts. The options include: look and feel, layout, the workspace, browser types, and so on.

Table 8-2 Attributes Controlling the Layout and Content of the Java GUI

Name	Value	Default	Overrides	Details
gui.dftllayout	boolean	false		Controls the base layout. [a]
gui.objectpane	boolean			Show or hide Object Pane
gui.shortcutbar	boolean			Show or hide Shortcut Bar
gui.workspace	<name>	Default names as generated for new workspaces.		Create new workspaces
gui.msgbrw.type	active | history | pending	active		Opens a browser with active, history, or pending messages
gui.msgbrw.workspace	<name>	Default – first - workspace		Opens a browser in specified workspace.
gui.msgbrw.brwpane	<boolean>		gui.msgbrw.workspace	Opens a browser in browser pane
gui.msgbrw.filter.name	<name>		gui.msgbrw.filter.<ANY>	A saved filter name overrides all filter attribute values
gui.msgbrw.filter.nodes	<name_list>			
gui.msgbrw.filter.services	<name_list>			

Table 8-2 Attributes Controlling the Layout and Content of the Java GUI

Name	Value	Default	Overrides	Details
gui.msgbrw.filter.apps	<name_list>			
gui.msgbrw.filter.msggrps	<name_list>			
gui.msgbrw.filter.objects	<name_list>			
gui.msgbrw.filter.msgtext	<string>			
gui.msgbrw.filter.time.start	<date/time>	today 0:00:00		date / time format as specified by the system locale setting
gui.msgbrw.filter.time.end	<date/time>	today 23:59:59		date / time format as specified by the system locale setting
gui.msgbrw.filter.time.relative.start	<string>			the relative time syntax [+|-]<int>[d|h|m|s]
gui.msgbrw.filter.time.relative.end	<string>			the relative time syntax [+|-]<int>[d|h|m|s]
gui.msgbrw.filter.owned	not | me | others			

Table 8-2 Attributes Controlling the Layout and Content of the Java GUI

Name	Value	Default	Overrides	Details
gui.msgbrw.filter.severity	<severity_list> enum {unknown, normal, warning minor, major, critical}			
gui.svcgraph.name	<service_name>	top level service		All services assigned to operator.
gui.svcgraph.calcid	<calc_id> (0 | 1)	0		service status calculation id
gui.svcgraph.workspace	<name>	Default (first) workspace		opens a graph in specified workspace.
gui.svcmap.name	<service_name>	top level service		All services assigned to operator
gui.svcmap.calcid	<calc_id> (0 | 1)	0		service status calculation id
gui.svcmap.workspace	<name>	Default (first) workspace		opens a map in specified workspace.

a. The attribute controls the base layout of the Java GUI to which the new objects, controlled by other attributes, will be added. If set to false (default), layout is blank. Additionally, if the message browser is opened on the browser pane, it will take 100% of the GUI (the horizontal splitter, dividing the workspace pane and browser pane will be on the top-most position). If a service graph is opened in the workspace, then the GUI is shared equally between the workspace and browser pane. If set to “true”, the Java GUI is opened as today: if session-specific settings are found they are used, otherwise the global defaults are used.

Time-Zone Settings in the ito_op.bat File

The Java GUI displays time-related information according to the format and settings defined by the local time zone of the client. If the Java GUI and the HP Operations management server are located in different time zones, you can force the Java GUI to use the time zone of the management server by setting the `-Duser.timezone=<time_zone>` switch in the `ito_op.bat` file.

For example, to use the time zone `Australia/Sydney`, add the text `-Duser.timezone=Australia/Sydney` to the `ito_op.bat` file (example extract):

```
:: Starting JavaGUI
for %%p in (true TRUE on ON yes YES) do if "%%p"=="%TRACE%" echo on
for %%p in (true TRUE on ON yes YES) do if "%%p"=="%PLUGIN%" goto :PLUGIN
%START% .\j2re1.4.2\bin\%JAVA% -Duser.timezone=Australia/Sydney -Xmx128m
com.hp.ov.it.ui.OvEmbApplet initial_node=%ITOSERVER% user=%USER% passwd=%PASSWD%
trace=%TRACE% display=%DISPLAY% locale=%LOCALE%
max_limited_messages=%MAX_LIMITED_MESSAGES% refresh_interval=%REFRESH_INTERVAL%
apiport=%APIPORT% apisid=%APISID% https=%HTTPS% %BBCPARM%
goto END
```

Valid time zones are listed in the directory `<JRE_HOME>\lib\zi`, for example `GMT`, `Asia/Singapore`, or `Europe/Warsaw`. If you specify an invalid time zone, `GMT` is used.

Resource Files

The Java GUI resource file `itooprc` resides in the home directory of the user who starts the Java GUI and is used to store operator preferences. Each defined option must be listed in a separate line and followed by its parameter. The `itooprc` file is updated automatically after each click of the `[OK]` button in the `Preferences` dialog.

CAUTION The `itooprc` file should be edited only by experienced administrators or operators.

Table 8-3 on page 296 lists the configuration options that you can define in the Java GUI resource file, shows the required format, and briefly describes the result.

Table 8-3 itooprc Options and Parameters

Option	Format	Description
`apisid`	<*string*>	Sets a session ID for the particular Java GUI instance at its startup.
`bbc.http:proxy`	<*string*>	Configures a proxy server for HTTPS-based communication.
`colored_message_lines`	`on|off|true|false|yes|no`	Enables you to color the entire message row in the message browser with the severity color of that message
`def_help_url`	<*url*>	Path to the help pages on the management server.
`def_look_and_feel`	<*look_and_feel*>	Defines the appearance of Java GUI: Metal, Motif, or Windows.
`default_browser`	<*path_to_browser*>	Path to the web browser on a local host.
`display`	<*hostname*>	Hostname of the exported display where X applications will be launched.

Table 8-3 itooprc Options and Parameters (Continued)

Option	Format	Description
global_settings_poll_interval	<*number*>	Determines how frequently the Java GUI checks for changes to the global property files. Default is five minutes.
initial_node	<*hostname|ip*>	Hostname of the HPOM management server to which the Java GUI will connect.
install_dir	<*path*>	For HP internal use only.
locale	<*locale_setting*>	Presets the locale name.
max_limited_messages	<*number*>	Determines how many messages to display in the message browsers.
message_notification_dlg	on|off|true|false|yes|no	Shows a warning dialog when a message event occurs.
message_notification_dlg_app	on|off|true|false|yes|no	Starts a local application that will be executed when a message event occurs.
message_notification_dlg_app_path	<*path*>	Path to the local application that will be started when a message event occurs.
message_notification_show_all	on|off|true|false|yes|no	Sends event notification either for the first message to arrive or for every new message.
nosec	on|off|true|false|yes|no	Starts the SSL Secure Java GUI in standard mode without SSL functionality.
passwd	<*password*>	Password of the HPOM operator used for login.
port	<*number*>	Port number the Java GUI uses to connect to the management server.
prompt_for_activate	on|off|true|false|yes|no	For HP internal use only.

Table 8-3 itooprc Options and Parameters (Continued)

Option	Format	Description
`reconnect_interval`	<*number*>	Time (in seconds) the Java GUI allocates for reconnecting to the management server.
`reconnect_timeout`	<*number*>	Time (in seconds) after which the Java GUI will stop reconnecting to an unreachable management server.
`refresh_interval`	<*number*>	Determines how frequently the Java GUI refreshes automatically. Default is 30 seconds.
`secure_port`	<*number*>	Port number the Secure Java GUI uses to connect to the management server.
`severity_label`	`text|both|icon`	Determines whether the message browsers display icons, text, or both in the severity column.
`shortcut_tree_icon_width`	<*number*>	Controls the size (in pixels) of icons. Default is 32 pixels.
`show_at_severity`	`0|1|2|3|4|5`	Defines the severity of the message for which event notification takes place: `0` = Unknown `1` = Normal `2` = Warning `3` = Minor `4` = Major `5` = Critical
`subproduct`	<*subroduct_string*>	For HP internal use only.

Table 8-3 itooprc Options and Parameters (Continued)

Option	Format	Description
`tailored_applications_start`	`on|off|true|false|yes|no`	Enables you to include only applications related to the selected message in the pop-up menus.
`title_suffix`	`<`*`title`*`>`	Displays the string next to the title in the main window.
`trace`	`on|off|true|false|yes|no`	Enables display of tracing messages in the terminal.
`user`	`<`*`username`*`>`	HPOM operator name used for login.
`web_browser_type`	`external|auto|manual`	Type of web browser to use in the workspace pane: • External: On non-ActiveX tabs in the workspace pane, selects a web browser external to the Java GUI. On ActiveX tabs in the workspace pane, selects the Microsoft Internet Explorer ActiveX control. • Auto: Selects the internal web browser provided with the Java GUI. • Manual: Custom selection of web browser. See the `which_browser` option.
`which_browser`	`1|2`	Type of web browser to use: `1` = ActiveX Internet Explorer `2` = Internal web browser

Cockpit View

The HPOM cockpit view is a web-based interface that displays the state of the environment monitored by HPOM. The cockpit view helps users to quickly assess the current health of the monitored environment and its readiness to support the business. For a detailed description of the cockpit view, refer to the *HPOM Java GUI Operator's Guide*. Note that you can configure as many cockpit views as you need. The information in this section describes and explains the following aspects of the cockpit view:

❏ "Configuring the Cockpit View" on page 300
❏ "Layout Configuration Files" on page 301
❏ "Valid Layout Configuration Files" on page 319
❏ "Sample Layout Configuration File" on page 320

Configuring the Cockpit View

To configure the cockpit view, perform the following steps:

1. Configure a layout configuration file for each cockpit view that you want to display.

   For more information about the contents of a cockpit view's layout-configuration file, see "Layout Configuration Files" on page 301.

2. Validate your layout configuration files against the Document Type Definition (DTD).

   For more information about a validating a cockpit view's layout configuration, see "Valid Layout Configuration Files" on page 319.

3. On the management server, store your layout configuration files in the following directory:

   `/opt/OV/www/htdocs/ito_op/assets/xml`

4. Start a cockpit view on the client system, type the following URL:

   `# http://<management_server>:3443/OvCgi/\`
   `ito_op_applet_cgi.ovpl?cockpitview=true&view=<layout>`

<management_server> is the hostname of your management server, and *<layout>* is the name of the layout configuration file. (Omit the `.xml` file type extension.)

For example, the following URL starts the sample cockpit view provided by HP:

```
# http://<management_server>:3443/OvCgi/\
ito_op_applet_cgi.ovpl?cockpitview=true
```

Layout Configuration Files

The layout configuration files (*<layout>.xml*) determine the colors, layout, and contents of the indicator panel of a cockpit view. On the management server, layout configuration files are located in the following directory:

`/opt/OV/www/htdocs/ito_op/assets/xml/<layout>.xml`

TIP The `xml` directory contains a sample layout configuration (`layout_simple.xml`) which you can use to get started. If you want to use the sample layout, do not edit the sample file itself. First, make a copy of the sample file, and edit the copy. For more information about the sample-layout configuration file, see “Sample Layout Configuration File” on page 320.

In layout configuration files, you can use the available tags to specify values for the following elements:

- ❏ “Style Configuration Options” on page 302
- ❏ “Free-Text Configuration Options” on page 305
- ❏ “Image Configuration Options” on page 306
- ❏ “Message-Filter Groups” on page 308
- ❏ “Health-Gauge Configuration” on page 313

CAUTION To see the changes you make to a layout configuration file, exit the web browser and restart the cockpit view. It is not sufficient to only refresh the web browser.

Cockpit views calculate the height of the area reserved for the indicator panel of a cockpit view based on the specifications in the layout configuration files. The Java GUI is added below the indicator panel. It may be hidden from view if the indicator panel takes up all available space. Use the vertical scroll bars of the web browser to access the Java GUI.

Style Configuration Options

The `<styles>` tag enables you to specify global styles for the elements of a cockpit view.

`<styles>`

Colors and font styles for a cockpit view.

`<bg_color>`

Background color of a cockpit view.

Example:

```
<bg_color value="#2e62fe" />
```

`<filter_name_font>`

Size and color of the font used for message filters.

Example:

```
<filter_name_font size="12" color="#ffffff"
/>
```

`<filter_value_font>`

Size and color of the font used for values in message filters.

Example:

```
<filter_value_font size="11" color="#000000"
/>
```

`<filter_group_font>`

Size and color of the font used for message filter groups.

Example:

```
<filter_group_font size="13" color="#ffffff"
/>
```

`<health_gauge_font>`

Size and color of the font used for health gauges.

Example:

```
<health_gauge_font size="10" color="#ffffff"
/>
```

`<showLabelBackground>`

Whether the background of text areas of message filters and message filter groups displays in color to indicate status. Possible values are true or false.

If set to true, the color of the font used for message filters and message filter groups automatically changes to the color specified for `<filter_name_font>`.

Example:

```
<showLabelBackground value="false"/>
```

`<showUnowned>`

Whether one or two message bars display. Possible values are `true` or `false`.

If set to `false`, only one message bar is displayed. This message bar shows the total number of all messages by severity.

If set to `true`, two message bars display. The upper bar shows the total number of all messages by severity. The lower bar shows the number of all unowned messages by severity.

Example:

```
showUnowned value="false"/>
```

`<showSeverityIcons>`

Whether state and color indicate the status of message filters and message filter groups. Possible values are `true` or `false`.

Example:

```
<showSeverityIcons value="false"/>
```

<state_color>

Whether state and color indicate the status of message filters and message filter groups.

You can define the following attributes:

`state`	State of the message filter or message filter group.
`value`	Color indicating the state of the message filter or message filter group.

Examples:

```
<state_color state="critical" value="#fe0000"
/>
<state_color state="major" value="#ff9428" />
<state_color state="minor" value="#ffde53" />
<state_color state="warning" value="#4ababc"
/>
<state_color state="normal" value="#94cf65"
/>
<state_color state="unknown" value="#79a7e2"
/>

<state_color state="unowned_critical"
value="#fe0000" />
<state_color state="unowned_major"
value="#ff9428" />
<state_color state="unowned_minor"
value="#ffde53" />
<state_color state="unowned_warning"
value="#4ababc" />
<state_color state="unowned_normal"
value="#94cf65" />
<state_color state="unowned_unknown"
value="#79a7e2" />
```

```
<state_color state="no_unowned_messages"
value="#b3b3b3" />
<state_color state="no_owned_messages"
value="#dddddd" />
<state_color state="no_messages"
value="#eeeeee" />
```

Free-Text Configuration Options

The `<freeTexts>` tag enables you to place single lines of text anywhere in a cockpit view. You can define the position of the line of text, the text itself, and the format of the text.

NOTE All styles and attributes not marked *Optional* are required.

`<freeTexts>` *Optional.* Defines lines of text.

`<text>` Single line of text.

You can define the following attributes:

- `x` Position of the text line on the *x*-axis, in pixels, for example: `x="10"`
- `y` Position of the text line on the *y*-axis, in pixels: `y="10"`
- `tooltip` *Optional.* Tool tip to display additional information about the line of text, for example:

  `tooltip="More information."`

  To access the tool tip of a line of text, hover the cursor over the text. If you do not specify a tool tip, or if the attribute is empty, a tool tip is not available.

`<font>` *Optional.* Size and color of the font used for the text. You can define the following attributes:

- `size` *Optional.* Size of the font used for the line of text. For example: `size="10"`

`color`	*Optional.* Color of the font used for the line of text. For example: `color="#ff0000"`

If you do not specify the size and color of the font, the following defaults will be used: `size="10"` and `color="#FFFFFF"`.

`<b>`	*Optional.* Bold format, for example: `<b>This text appears bold.</b>`
`<u>`	*Optional.* Underline format, for example: `<u>This text appears underlined.</u>`
`<i>`	*Optional.* Italic format, for example: `<i>This text appears in italics.</i>`

NOTE You cannot limit the width of a text area (for example, by using line breaks). If a line exceeds the available display area, the cockpit view adds a horizontal scroll bar to the indicator panel of the cockpit view.

Image Configuration Options

The `<images>` tag enables you to place images anywhere in a cockpit view.

NOTE All styles and attributes not marked *Optional* are required.

`<images>`	*Optional.* Defines images.
`<image>`	Image. Defines the following attributes:

`source`	Name of the image file. For more information about the location of the image file, see "Image Location" on page 307.

Supported image formats are GIF, JPEG, PNG, SVG, and SWF.

Examples:

	source="../ITO_OP/images/hp.jpg " source="http://mymanager.com/hp .jpg"
width	Width of the image in pixels, for example: width="200"
height	Height of the image in pixels, for example: height="200"
x	Position of the image on the *x*-axis in pixels, for example: x="10"
y	Position of the image on the *y*-axis, in pixels, for example: y="10"

Image Location Depending on the location of the image, you can specify the *absolute* or *relative* path to an image on the management server, or use the HTTP protocol to access images:

❑ Image location on the management server

If the image resides in the /opt/OV/www/htdocs/ito_op/images directory on the management server, specify the following path in the layout configuration file:

../ITO_OP/images/<*image*>

Example use in a layout configuration file:

source="../ITO_OP/images/hp.jpg"

If the image resides in another location on the management server, specify the absolute path or the relative path, starting from the layout configuration file.

❑ Image location on any server

If the image resides on a web server other than the management server, perform the following steps:

1. Create a cross-domain policy file in the following directory on the management server:

   /opt/OV/www/htdocs/ito_op/crossdomain.xml

2. Add the following lines to the crossdomain.xml file:

```
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM
"http://www.macromedia.com/xml/dtds/cross-domain-poli
cy.dtd">
<cross-domain-policy>
   <allow-access-from domain="<domain>" />
</cross-domain-policy>
```

Replace <*domain*> with the server that hosts the images you want to access, for example `www.mymanager.com`.

Example use in a layout configuration file:

```
source="http://www.mymanager.com/hp.jpg"
```

For more information about cross-domain policy files, see **http://www.adobe.com**.

Message-Filter Groups

The `<messageFilterGroups>` tag enables you to collect message filters into groups and to specify their name, label, position, and other attributes.

NOTE All styles and attributes not marked *Optional* are required.

`<messageFilterGroups>`

Optional. Defines message filter groups and message filters.

`<group>`

Name of the message-filter group. You can define the following attributes:

`name`

Name of the message-filter group. The name must be unique in the HPOM environment. Note that the group name is not the same as the message-filter name. Filter groups cannot be specified in the Java GUI.

Example:

`name="corp_srvs"`

`label`

Optional. Label of the message filter group. If you do not specify a label, the group name displays.

Example:

`label="Corporate Servers"`

`tooltip`

`Optional`. Tool tip to display additional information about the message filter group. To access the tool tip of a message filter group, hover the cursor over the label or the group summary.

If you do not specify text for the tool tip, or if the attribute is empty, the label will be displayed. If no label is specified, a tool tip is not available.

Example:

`tooltip="Corporate servers are servicing the company."`

`textAlign`

Alignment of the name (or label) of the message filter group relative to the message bars. Possible values are `top`, `bottom`, `left`, or `right`.

Example:

`textAlign="top"`

`text_width`

Width of the area reserved for displaying the name (or label) of message filters, in pixels.

Example:

`text_width="130"`

`bar_width`

Width of the area reserved for displaying the number of messages by severity, in pixels.

Choose a suitable width for message bars, depending on the amount of available space and on the number of messages expected. A cockpit view requires a minimum of space to display message numbers in a human-readable format.

If the specified width is too small, the message bars are shaded to indicate that some information is hidden. In addition, cockpit views truncate the message bars. You can view the complete information by accessing the tool tip of a truncated message bar.

To completely hide message bars, specify a negative value (for example, `bar_width="-1"`).

Example:

`bar_width="200"`

`x`

Position of the message filter group on the *x*-axis, in pixels.

Example:

`x="10"`

`y`

Position of the message filter group on the *y*-axis, in pixels.

Example:

`y="10"`

`historyMessages`

Whether to display active or history messages. Possible values are `true` or `false`.

Example:

`historyMessages="true"`

`calculateGroupStatus`

Whether to display a summary status line of all messages of the group. Possible values are `true` or `false`.

Example:

`calculateGroupStatus="true"`

`showLabelBackground`

Optional. Whether to display the background of text areas of message filters and message filter groups in color to indicate status. Possible values are `true` or `false`.

If set to true, the color of the font used for message filters and message filter groups automatically changes to the color specified for `<filter_name_font>`.

You can also specify `showLabelBackground` globally in the `<styles>` section of a layout configuration file. However, any settings that you make at group level override global settings.

Example:

`showLabelBackground="false"`

`showSeverityIcons`

Optional. Whether to display icons for message filters and message filter groups. Possible values are `true` or `false`.

You can also specify `showSeverityIcons` globally in the `<styles>` section of a layout configuration file. However, any settings that you make at group level override global settings.

Example:

`showSeverityIcons="false"`

`showUnowned`

Optional. Whether one or two message bars display. Possible values are `true` or `false`.

If set to `false`, only one message bar is displayed. This message bar shows the total number of all messages by severity.

If set to `true`, two message bars display. The upper bar shows the total number of all messages by severity. The lower bar shows the number of all unowned messages by severity.

TIP You can also specify `showUnowned` globally in the `<styles>` section of a layout configuration file. However, any settings that you make at group level override global settings.

Example:

`showUnowned="false"`

`<filter>`

Message filters.

You can define the following attributes:

`name`

Name of the message filter. The name must correspond to the name of the filter specified in the Java GUI. For details, see the *HPOM Java GUI Operator's Guide*.

Example:

`name="corp_srv"`

`label`

Label of the message filter.

Example:

`label="Corporate Server"`

`tooltip`

Optional. Tool tip to display additional information about the message filter. To access the tool tip of a message filter, hover the cursor over the label.

If you do not specify text for the tool tip, or if the attribute is empty, the label displays. If no label is specified, a tool tip is not available.

Example:

`tooltip="This corporate server is servicing the company."`

Health-Gauge Configuration

The `<healthGauges>` tag enables you to define the appearance of the health gauge including: size, position, levels, and scales. For more information about setting the scales of health gauges, see "Defining the Scale of Health Gauges" on page 317.

NOTE All styles and attributes not marked *Optional* are required.

```
<healthGauges>
```

Optional. Defines health gauges.

`<gauge>`

Health gauge.

You can define the following attributes:

`name`

Name of the message filter. The name must correspond to the name of the filter as specified in the Java GUI. For details, see the *HPOM Java GUI Operator's Guide*.

Example:

```
name="corp_srv"
```

`label`

Label of the health gauge.

Example:

```
label="Corporate Health"
```

`tooltip`

Optional. Tool tip to display additional information about the health gauge. To access the tool tip of a health gauge, hover the cursor over the label.

If you do not specify text for the tool tip, or if the attribute is empty, the label displays. If no label is specified, a tool tip is not available.

Example:

```
tooltip="Health gauges show the
health of the company."
```

`sense`

Orientation of the scale. Possible values are `positive` or `negative`.

Example:

`sense="positive"`

`reference`

Maximum value of the scale.

Example:

`reference="100"`

`level_1`

Maximum value of the *first* segment on the scale.

Example:

`level_1="20"`

`level_2`

Maximum value of the *second* segment on the scale.

Example:

`level_2="40"`

`level_3`

Maximum value of the *third* segment on the scale.

Example:

`level_3="60"`

`level_4`

Maximum value of the *fourth* segment on the scale.

Example:

`level_4="80"`

`width`

Diameter of the health gauge, in pixels.

Example:

`width="150"`

`x`

Position of the health gauge on the *x*-axis, in pixels.

Example:

`x="20"`

`y`

Position of the health gauge on the *y*-axis, in pixels.

Example:

`y="405"`

`historyMessages`

Whether to display active or history messages. Possible values are `true` or `false`.

Example:

`historyMessages="true"`

`showLabelBackground`

Optional. Whether to display the background of text areas of health gauges in color to indicate status. Possible values are `true` or `false`.

If set to true, the color of the font used for health gauges automatically changes to the color specified for `<filter_name_font>`.

TIP

You can also specify `showLabelBackground` globally in the `<styles>` section of a layout configuration file. However, any settings that you make at gauge level override global settings.

Example:

`showLabelBackground="false"`

`showSeverityIcons`

Optional. Whether to display icons for health gauges. Possible values are `true` or `false`.

TIP

You can also specify `showSeverityIcons` globally in the `<styles>` section of a layout configuration file. However, any settings that you make at gauge level override global settings.

Example:

`showSeverityIcons"false"`

Defining the Scale of Health Gauges

To define the scale of a health gauge, you must decide the following:

1. General orientation of the scale (positive or negative)
2. Maximum value of the scale
3. Thresholds that define the individual segments of the scale

The `sense` attribute determines the orientation of the scale. A positive orientation means that a lower value is more critical than a higher value, with the reference value being the maximum, the best value. If you choose a negative orientation, higher values are considered to be more critical than lower values.

The `level` attributes define the individual segments of the scale.

Figure 8-1 shows health gauges with a *positive* orientation:

```
sense="positive"
reference="100" (normal: 80 through 100)
level_1="20" (critical: 0 through 19)
```

```
level_2="40" (major: 20 through 39)
level_3="60" (minor: 40 through 59)
level_4="80" (warning: 60 through 79)
```

Figure 8-1 Health Gauges with a Positive Orientation

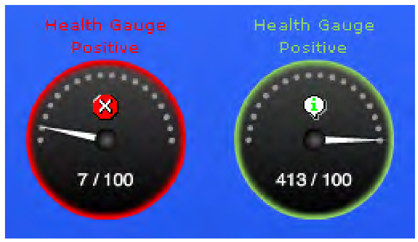


Figure 8-1 on page 318 shows health gauges with a *positive* orientation; in a positive orientation, 0=bad, 100=good. The current value of the gauge on the left is `7`, which means that the current status is critical. When the value reaches or exceeds `100`, as shown in the gauge on the right, the status changes to normal because the best possible condition has been reached.

Figure 8-2 shows health gauges with a *negative* orientation:

```
sense="negative"
reference="100" (critical: 80 through 100)
level_1="20" (normal: 0 through 19)
level_2="40" (warning: 20 through 39)
level_3="60" (minor: 40 through 59)
level_4="80" (major: 60 through 79)
```

Figure 8-2 Health Gauges with a Negative Orientation

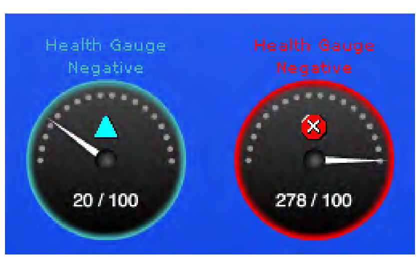


Figure 8-2 on page 318 shows health gauges with a *negative* orientation; in a negative orientation, 0=good, 100=bad. The current value of the gauge on the left is 20, which indicates a current status of “warning”. When the value reaches or exceeds 100, as shown in the gauge on the right, the status changes to critical because the worst possible condition has been reached.

NOTE If the current value of a health gauge exceeds the reference value, the status of the gauge remains the same as it was when it reached the reference value. The reference value is: “normal” for health gauges with a positive orientation and “critical” for health gauges with a negative orientation.

Valid Layout Configuration Files

On the management server, the Document Type Definition (DTD) for the layout configuration files is available at the following location:

`/opt/OV/www/htdocs/ito_op/assets/xml/cockpitviewLayout.dtd`

HP recommends that you validate your layout configuration files against the DTD provided for this purpose. You must make sure that layout configuration files are well formed XML documents and that conform to the rules of the DTD.

To ensure that the DTD validation tool can locate the cockpit-view DTD (`cockpitviewLayout.dtd`.), insert a reference to the DTD in your XML files, for example:

```
<!DOCTYPE cockpitLayout SYSTEM "/opt/OV/www/htdocs/ito_op/
assets/xml/cockpitviewLayout.dtd">
```

You can find validation tools at the following locations:

- XML Pad:

  http://www.wmhelp.com/

- Eclipse Ganymede (Eclipse IDE for Java Developers):

  http://www.eclipse.org/downloads/packages/release/ganymede/r

- Validome:

http://www.validome.org/xml/validate/

- ❑ W3Schools:

  http://www.w3schools.com

Sample Layout Configuration File

The following sample layout configuration file is available on the management server:

`/opt/OV/www/htdocs/ito_op/assets/xml/layout_simple.xml`

To successfully view the sample layout configuration file, create the following two message filters in the Java GUI:

- ❑ Filter `Main Terminal`

  General
  with Severity
  is Critical
  Symbols and Objects

- ❑ Filter `WebShop DB`

  General
  with Severity
  is Normal
  Symbols and Objects

TIP Do *not* edit the sample layout-configuration file directly. First make a copy of the file, and then edit the new copy.

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE cockpitLayout SYSTEM "/opt/OV/www/htdocs/ito_op/
assets/xml/cockpitviewLayout.dtd">

<cockpitLayout>
<layoutVersion version="001.001" />

<styles>
   <bg_color value="#2e62fe" />
   <filter_name_font size="12" color="#ffffff" />
   <filter_value_font size="11" color="#000000" />
   <filter_group_font size="13" color="#ffffff" />
   <health_gauge_font size="10" color="#ffffff" />
   <showLabelBackground value="false" />
```

```
    <showSeverityIcons value="true" />
    <showUnowned value="true" />
    <state_color state="critical" value="#fe0000" />
    <state_color state="major" value="#ff9428" />
    <state_color state="minor" value="#ffde53" />
    <state_color state="warning" value="#4ababc" />
    <state_color state="normal" value="#94cf65" />
    <state_color state="unknown" value="#79a7e2" />
    <state_color state="unowned_critical" value="#fe0000" />
    <state_color state="unowned_major" value="#ff9428" />
    <state_color state="unowned_minor" value="#ffde53" />
    <state_color state="unowned_warning" value="#4ababc" />
    <state_color state="unowned_normal" value="#94cf65" />
    <state_color state="unowned_unknown" value="#79a7e2" />
    <state_color state="no_unowned_messages" value="#b3b3b3"
/>
    <state_color state="no_owned_messages" value="#dddddd" />
    <state_color state="no_messages" value="#b3b3b3" />
</styles>

<freeTexts>
    <text x="110" y="380">
        <u>
            <b>Lorem ipsum</b>
        </u>
        dolor sit amet,
        <u>consectetuer</u>
        <font size="14" color="#ff0000">adipiscing</font>
        elit
    </text>
</freeTexts>

<messageFilterGroups>
    <group name="Corporate Servers" label="Corporate Servers"
    text_width="120" bar_width="200" x="10" y="10"
    calculateGroupStatus="true">
        <filter name="WebShop DB" label="WebShop DB" />
        <filter name="Main Terminal" label="Main Terminal" />
    </group>
</messageFilterGroups>

<healthGauges>
    <gauge name="Main Terminal" label="Main Terminal"
    sense="positive" reference="12" level_1="60" level_2="70"
    level_3="80" level_4="100" width="110" x="20" y="205" />
    <gauge name="WebShop DB" label="WebShop DB"
```

```
sense="negative"
   reference="10" level_1="30" level_2="35" level_3="40"
   level_4="44" width="110" x="210" y="205" />
</healthGauges>

<images>
   <image source="../ITO_OP/images/hp.jpg" width="100"
   height="60" x="0" y="350" />
</images>

</cockpitLayout>
```

NNM Access from the Java GUI

The information in this section describes how the Java GUI handles the integration between HPOM and NNM. You can find detailed information about the following topics:

Overview

The information in this section describes how the Java GUI handles the integration between HPOM and NNM. By default, the HPOM Java GUI provides integrated access to Network Node Manager (NNM). The NNM integration with HPOM enables users to highlight nodes in the IP Map of NNM systems and execute NNM applications directly from the HPOM Java GUI.

HPOM provides a Java GUI integration with NNM 7.xx that requires that the NNM instance is installed on a system other than the system hosting the HPOM management server. A `HPOVOUOVWMGR` package responsible for the integration of the HPOM with NNM 7.xx is installed on the remote NNM 7.xx system during the HPOM subagent installation. To find out how to install subagents, see "Subagent Installation on Managed Nodes" on page 49. Also, the `HPOVOUOVWMGR` policy should be assigned to the node with the installed NNM. For details on NNM 7.xx integration with the HPOM, see "NNM 7.xx and HPOM" on page 225.

NNM Access from a Remote System

As NNM is installed on a system other than the HP Operations management server, operators can access NNM from the Java GUI.

To access to a remote NNM system, make sure the following requirements are met:

- ❏ HPOM agent on a remote NNM system:

  The integration with NNM 7.xx is supported on the following HP Operations agent platforms:

  — HP-UX 11i v3

  — Solaris 10 for SPARC

- ❏ HPOM subagent package on a remote NNM system:

  The `HPOVOUOVWMGR` policy should be assigned to the system where NNM is installed. The `HPOVOUOVWMGR` package responsible for the integration of the HPOM with NNM 7.xx is installed on the remote NNM 7.xx system as a part of the HPOM subagent.

- ❏ NNM node-mapping tools:

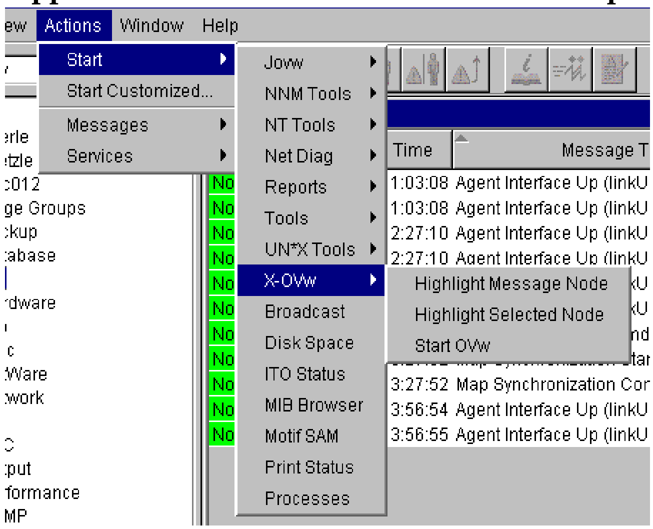
  Tool `opcmapnode` has been configured on the management server, to determine information about which NNM nodes are available on the system domain.

NOTE No operator-specific registration directory is used for remote NNM systems. The Java GUI server process `opcuiwww` cannot create this directory on a remote client. However, you can preconfigure multiple registration directories, then use different directories for different operators.

NNM Applications in the Java GUI

Operators can choose from a number of applications that provide access to NNM. These applications are included in the application group `X-OVw`, as shown in Figure 8-3.

Figure 8-3 Applications Contained in the X-OVw Group



NOTE When an operator starts an application from the Java GUI for the first time, the operator's private map is used. By default, the map is opened in read-write mode.

Types of HP Applications Available from the Java GUI

In the Java GUI, operators can choose from the following applications:

❑ `Highlight Message Node:`

Maps the node related to a selected message to an NNM system, and highlights the node in an ovw session of that NNM system. NNM cannot be installed on the same system as the HP Operations management server.

❑ `Highlight Selected Node:`

Maps the selected node to an NNM system, and highlights the node in an ovw session of that NNM system. NNM cannot be installed on the same system as the HP Operations management server.

- ❏ `Start ovw`:

  Starts an ovw session on a remote NNM system.

opcctrlovw Command

When an HP application is started from the Java GUI, the Java GUI server process calls the `opcctrlovw` command on the management server's agent. The command will always be run with the UNIX user account `opc_op`.

You start the `opcctrlovw` command with the following syntax:

```
opcctrlovw
     -display <display>
     -user <user>
     -action <appl> <action> {<node1>, <node2>...}
```

The `opcctrlovw` command recognizes the following variables:

<display>	Configured X display of the Java GUI.
<user>	HPOM operator name.
<appl>	Application registration name of the HP application to be started.
<action>	Action of the HP application to be started.
<node1>, *<node2>*, ...	IP hostnames of all selected nodes from the node tree of the Java GUI.

Access to NNM with Command-line Tools

HPOM provides the following command-line tools that enable you to configure access to NNM:

`opcctrlovw` Controller tool.

For more information, see "OVW-Process Controller Tool" on page 327.

`opcmapnode` Node-mapping tool.

For more information, see “NNM Node-Mapping Tools” on page 328.

OVW-Process Controller Tool

The `opcctrlovw` tool is used to control an associated `ovw` process. When provided with startup information as a command-line argument, the controller tool `opcctrlovw` calls the process `ovw`, based on that startup information. The controller tool is responsible for one `ovw` process. If the controller tool process stops for any reason, the `ovw` process is terminated automatically.

Controller-Tool Command Syntax

The command-line syntax for the controller tool is as follows:

```
opcctrlovw
[-display <display>]
[-user <username>]
[-stop | -highlight <node> | -action <reg-appl> <reg-action>
{<node>}]
```

For more information about command options and parameters, see the reference page *opcctrlovw(1m)*.

Controller-Tool Configuration

You can configure the controller tool `opcctrlovw` by writing a configuration file, which contains user-specific settings. You should place this configuration file on the management server, then distribute it to each managed node station.

The user name provided on the command line is used as a key. For each user name, you can configure a configuration entry containing the map, registration directory, and read-only or read-write–only mode,

The configuration file is based on the Extensible Markup Language (XML), with the following Document Type Definition (DTD):

```
<!ENTITY Config (Default?,User*) >
<!ENTITY User (Name,Map?,Dir?,(ReadOnly | ReadWrite)? >
<!ENTITY Default (Map?,Dir?,(ReadOnly | ReadWrite)? >
<!ENTITY Name (#PCDATA) >
<!ENTITY Map (#PCDATA) >
```

```
<!ENTITY Dir (#PCDATA) >
<!ENTITY ReadOnly EMPTY >
<!ENTITY ReadWrite EMPTY >
```

For example:

```
<?xml version="1.0" ?>
<Config xmlns="http://www.hp.com/OV/opcctrlovw">
 <Default>
     <Map>hugomap</Map>
     <ReadOnly/>
 </Default>
 <User>
     <Name>opc_op</Name>
     <Map>mymap</Map>
     <Dir>/sdlflf/sdflksdjf/sdfsldk:/sdflkdsh</Dir>
     <ReadWrite/>
 </User>
 <User>
     <Name>hugo</Name>
     <Map>hugomap</Map>
     <ReadOnly/>
 </User>
</Config>
```

NNM Node-Mapping Tools

Before starting an HP application or service remotely from the HPOM GUI, you must map the target nodes on which the application will be started with the node mapping tool `opcmapnode`. This tool, which you run on the HP Operations management server, automatically determines information about available NNM nodes on the system domain at startup time.

Pattern Matching in Node Names

The node mapping tool uses pattern matching to return a node name on `stdout`. When the problem node has been highlighted in the Node Bank, the node-mapping tool uses pattern matching to look up the specified node name on the corresponding NNM system. In this way, it locates the hostname or IP address patterns in a match table.

The pattern-matching procedure is carried out from the top of the file to the bottom, until the first pattern matches. If a pattern matches, the specified target node will be returned. If none of the patterns match, the output will be empty.

Node-Mapping Command Options

You use the `opcmapnode` tool as a dynamic target node command in the HPOM application, in single backquotes, as follows:

```
‘opcmapnode <node>‘
```

For more information about command options and parameters, refer to the reference page *opcmapnode(1m)*.

Node-Mapping Tool Configuration

When you run the `opcmapnode` command, the command reads the current configuration from the following file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/opcmapnode.conf
```

The configuration file contains an HPOM pattern in every line, followed by a node name, or by the variable `$MGMT_SERVER`, as follows:

```
^<*>.site1.my.domain$      system1.my.domain
^<*>.site2.my.domain$      system2.my.domain
^<*>.$                     $MGMT_SERVER
```

If `opcmapnode` is started in this configuration file, any nodes in domain site 1 are mapped to system 1, any nodes in domain site 2 are mapped to system 2, and all other nodes are mapped to the HP Operations management server.

NOTE If the mapping file does not exist, or if it contains no pattern lines, all NNM nodes will be mapped to the management server.

NNM Access with Jovw

`Jovw` is the Java-based web interface to the NNM and is integrated into the HPOM Tools tools group. By default, `Jovw` is assigned to the `itop` and `netop` operators. This section describes how to enable access to the default IP map with `Jovw`, and how to modify the integration so that other IP maps can be accessed. For more information, see the following sections:

❏ "Accessing the Default IP Map with Jovw" on page 330

❏ "Accessing Other IP Maps with Jovw" on page 331

Accessing the Default IP Map with Jovw

To access the default IP Map with `Jovw`, perform the following steps:

1. Start `ovw` on the remote NNM 7.xx system.

   When accessing `Jovw`, `ovw` must be running. As user root, enter the following command in a shell:

   `#` **`ovw`**

2. As HPOM administrator, assign the application group `Jovw` to any operators who need access to NNM from the HPOM Java GUI.

3. Start the Java-based GUI and log in.

   If you are already logged in, select `View: Reload Configuration` from the menu bar. This option retrieves the new configuration from the HP Operations management server.

4. Select `Edit: Preferences` from the menu bar.

5. Enter the path to your local web browser.

6. Highlight a node in the IP Map

   Right-click the node in the object pane, and select the `Start: Jovw: Highlight in Ip-Map` menu item from the popup menu.

IMPORTANT `Jovw` replicates the `ovw` default map. For this reason, ovw must be running when accessing Jovw.

Accessing Other IP Maps with Jovw

To access an IP map other than the default IP Map, modify the `Jovw` applications by performing the steps described in the following procedure:

1. Copy the applications `Highlight in Ip-Map` and `Jovw` in the application group `Jovw(old)`.
2. Modify the applications to use an IP map other than the default map, as follows:
   - Copy the application `Highlight in Ip-Map`:
     a. Modify the name and label to suit your needs:

        `# `**`opcappl -copy_app app_name="JOvw: Highlight in Ip-Map" new_name="New Highlight in Ip-Map"`**

     b. In the new application, change the default application call, to the name of the IP map you want to use:

        `# `**`opcappl -chg_app app_name="New Highlight in Ip-Map" app_call= <new_map>`**

        where *<new_map>* is the name of the IP map you want to use.
   - Copy the application `Jovw`:
     a. Modify the name and label to suit your needs:

        `# `**`opcappl -copy_app app_name="Jowv: Jovw" new_name="New Jowv`**"

     b. In the new application, change the default application call, as follows:

        `# `**`opcappl -chg_app app_name="New Jowv" app_call= ?MapName=<new_map>`**

        where *<new_map>* is the name of the IP map you want to use.

        For example, the application call could look like this:

`http://$OPC_MAP_NODE:3443/OvCgi/jovw.exe?MapName=new_map`

3. Create a new application group, using the following command:

   `# opcappl -add_appgrp appgrp_name=New_Group`

4. Move the new applications and the unchanged application `OVlaunch` into the new group, using the following command:

   `# opcappl -assign_app_to_grp app_name="New Highlight in Ip-Map" to_appgrp_name=New_Group`

   `# opcappl -assign_app_to_grp app_name="New Jowv" to_appgrp_name=New_Group`

   `# opcappl -assign_app_to_grp app_name="OVlaunch" to_appgrp_name=New_Group`

   `# opcappl -deassign_app_from_grp app_name="New Highlight in Ip-Map” from_appgrp_name="Jowv(old)"`

   `# opcappl -deassign_app_from_grp app_name="New Jowv” from_appgrp_name="Jowv(old)"`

5. Assign the new group to an HPOM operator, as follows:

   `# opccfguser -assign_appgrp_user -user <user_name> -appgrp -list New_Group`

6. Start `ovw` on the system where NNM 7.xx is installed.

   When accessing Jovw, `ovw` must be running. As user root, enter:

   `# ovw -map <new_map>`

<new_map>	Name of the IP map you have specified in the previous steps.

7. Start the Java GUI and log in.

   If you are already logged in, select `View: Reload Configuration` from the menu bar. This retrieves the new configuration from the HP Operations management server.

8. Select `Edit: Preferences` from the menu bar.

9. Enter the path to your local web browser.

10. Highlight a node in the IP Map.

Right-click the node in the object pane, and select the new highlight application from the popup menu.

IMPORTANT `Jovw` replicates the `ovw` map. For this reason, `ovw` must be running when you access `Jovw`.

Backup Management Servers

If the currently connected HP Operations management server suddenly becomes unavailable, for example because of a system failure, Java GUI clients can automatically reconnect to one or more backup management servers.

If the connection is disrupted, the Java GUI tries to connect to the current HP Operations management server by default three times. If all reconnects fail, Java GUI users are asked whether they want to connect to the next backup management server in the list or continue trying to connect to the current management server. If they choose the current management server, the Java GUI will try to connect until the server can be reached again or until the Java GUI is closed.

If the user names and passwords of the connecting HPOM users are known on all participating management servers, the Java GUI reconnects to a backup server without displaying the `Login` dialog box.

You can configure the number and order of backup management servers for each HP Operations management server, as well as the number of reconnect attempts of the Java GUI client by setting parameters for the `ovconfchg` command line tool:

- ❏ Backup management servers:

  The keyword `OPC_JGUI_BACKUP_SRV` enables you to create a list of HPOM backup management servers that provide connections for Java GUIs. Use commas or colons to separate the management server hostnames.

  In the following example, the HP Operations management servers `ovo1.hp.com` and `ovo2.hp.com` are configured as backup servers for all connecting Java GUIs:

  ```
  ovconfchg -ovrg server -ns opc -set OPC_JGUI_BACKUP_SRV \
  ovo1.hp.com,ovo2.hp.com
  ```

- ❏ Number of reconnect attempts:

  The keyword `OPC_JGUI_RECONNECT_RETRIES` specifies the number of times a Java GUI client attempts to connect to the primary HPOM management server before trying to connect to a backup management server.

In the following example, the maximum number of reconnect attempts is configured to be five.

```
ovconfchg -ovrg server -ns opc -set \
OPC_JGUI_RECONNECT_RETRIES 5
```

The Java GUI must be restarted after the configuration has been updated on the management server. For more information about command options and parameters, refer to the reference page *ovconfchg(1)*.

Java GUI APIs

HPOM enables you to control certain Java GUI features remotely from other Java applications using the Java GUI Remote application programming interface (API).

For more information about the concepts, integration details, and usage of the Java GUI's remote APIs, refer to *HPOM Application Integration Guide*.

For more information about the remote APIs that are available for the Java GUI, refer to the Java GUI Remote APIs Specification, which you can find on the HPOM management server at the following location:

`http://`*<management_server>*`:3443/ITO_DOC`

In this instance, *<management_server>* is the fully qualified hostname of your HPOM management server.

Global Property Files

HPOM stores custom changes to the Java GUI in a selection of property files, which reside in the home directory of the operating-system user who launches the Java GUI. The property files include the following files:

❑ Console settings:

- `HP_OV_consoleSettings_<server_name>_<user>`
- `HP_OV_consoleSettings_<server_name>`
- `HP_OV_consoleSettings`

  Refer to the *HPOM Java GUI Operator's Guide* for more information about saving console settings.

❑ Resources:

  The Java GUI resource file `itooprc`. For more information about the resource file for the Java GUI, see "Resource Files" on page 296.

❑ Browser settings:

  The browser settings are stored in the file `itoopbrw`. For more information about the location and contents of the browser settings file for the Java GUI, refer to the *HPOM Java GUI Operator's Guide*.

You can configure the Java GUI to override any individual settings and use global property files stored in a shared location. The settings configured in a global property files override any individual settings with the following exceptions:

❑ Startup parameters:

  The following parameters control the connection to the HPOM management server and are ignored in global mode:

- `initial_node`
- `user`
- `passwd`
- `port`
- `locale`

❑ Allowed users:

The Java GUI continues to use the individual property files of the administrator or operators, if such files exist in the user's home directory. See also "Individual Settings with Global Property Files" on page 339.

Enabling Global Property Files

To enable global property files for the Java GUI, use the `ovconfchg` configuration tool on the HP Operations management server as follows:

1. Create a shared location where the global property files are stored.

   The shared location can be one of the following:

   - Local path:

     Examples: `'X:\share\javagui'` or `/net/share/javagui`

   - Remote path:

     Example: `'\\jacko.hp.com\share\javagui'`

   - URL:

     Must start with the string "`http:`", for example: `http://jacko:3443/ITO_OP/`

2. Copy the global property files to the shared location.

3. Configure the Java GUI to evaluate the global property files on the host operating system:

   - Windows:

     ```
     ovconfchg -ovrg server -ns opc -set \
     OPC_JGUI_GLOBAL_SETTINGS_WIN <win_shared_location>
     ```

   - UNIX:

     ```
     ovconfchg -ovrg server -ns opc -set \
     OPC_JGUI_GLOBAL_SETTINGS_UNIX <unix_shared_location>
     ```

   The Java GUI clients running on Windows systems will read the global settings from the location specified in the `OPC_JGUI_GLOBAL_SETTINGS_WIN` variable, while clients running on UNIX systems will read the global settings from the location specified in the `OPC_JGUI_GLOBAL_SETTINGS_UNIX` variable.

4. Restart all running Java GUI clients.

Individual Settings with Global Property Files

When global property files are enabled and configured, only the administrator and, if so configured, selected operators, are allowed to save and use individual settings. These users can save their settings in their home directories without affecting the global settings files.

Authorizing Access to Property Files

To grant permission to selected operators to save and use individual property files, specify their user names, separated by commas, as options for the variable `OPC_JGUI_CONF_ALLOWED_USERS`, as follows:

```
# /opt/OV/bin/ovconfchg -ovrg server -ns opc -set \
OPC_JGUI_CONF_ALLOWED_USERS opc_op,itoop
```

For all users that are treated as allowed users, the property files in their local home directories are evaluated first, if they exist. Then the global property files are loaded from the shared location.

Global Configuration Change Notifications

By default, Java GUI clients check every five minutes for changes to the global property files in the shared location. If a change is detected, the `OVO Communication Status` dialog box displays a message, which informs the operator of the changes and requests a restart of the Java GUI.

You can change the polling interval by specifying a value for the parameter `global_settings_poll_interval` in the `itooprc` file.

Setting the Change-Notification Polling Interval

To set the change-notification polling interval to one minute, add the following line to the `itooprc` file:

```
global_settings_poll_interval 1
```

Secure HTTPS-Based Communication

HTTPS-based Java GUI is a solution for providing a secure communication between Java GUI and the HP Operations management server.

The standard Java GUI supplied with HPOM 8.* has no secure link to the management server. This functionality is provided with the HTTPS-based Java GUI, that is the Java GUI which uses a HTTPS protocol with Secure Socket Layer (SSL) encryption for communication with HP Operations management server. The SSL encryption is based on the Core functionality components.

For more information about the HTTPS-based Java GUI architecture, configuring and usage, refer to the *HPOM Java GUI Operator's Guide*.

Instructions on how to install and enable the HTTPS-based Java GUI, as well as to disable the non-secure communication between the Java GUI client and the HP Operations management server are detailed in the *HPOM Installation Guide for the Management Server*.

Establishing a Secure Communication

The process of establishing a secure communication is as follows:

1. Java GUI client connects to the `opcuihttps` process, which acts as a proxy between Java GUI client and HP Operations management server using the HTTPS protocol.
2. Java GUI communicates with `opcuihttps` process using a secure HTTPS protocol on the port 35211. The `opcuihttps` then redirects the HTTPS requests to the standard Java GUI port (2531) using socket communication.

NOTE Make sure the port to which the HTTPS requests are redirected is set to the default value 2531. The option for connecting the `opcuihttps` process to other than default `opcuiwww` port is currently *not* available.

3. All forwarded HTTPS requests are then handled by the `inetd` process (on HP-UX and Solaris) or `xinetd` process (on Linux), as well as the requests from non-secure Java GUI clients.
4. The `opcuihttps` also processes replies from the HP Operations management server and forwards them to the Java GUI using the HTTPS protocol. All communication requests in either direction between the Java GUI and the HP Operations management server become trustworthy for secure exchange of data.

For more information about how to configure `opcuihttps` settings and display a list of the parameters related to HTTPS-based Java GUI, see “opcuihttps Configuration” on page 342.

Figure 8-4 on page 342 shows the communication between client and server. Depending on the chosen communication type, the following applies:

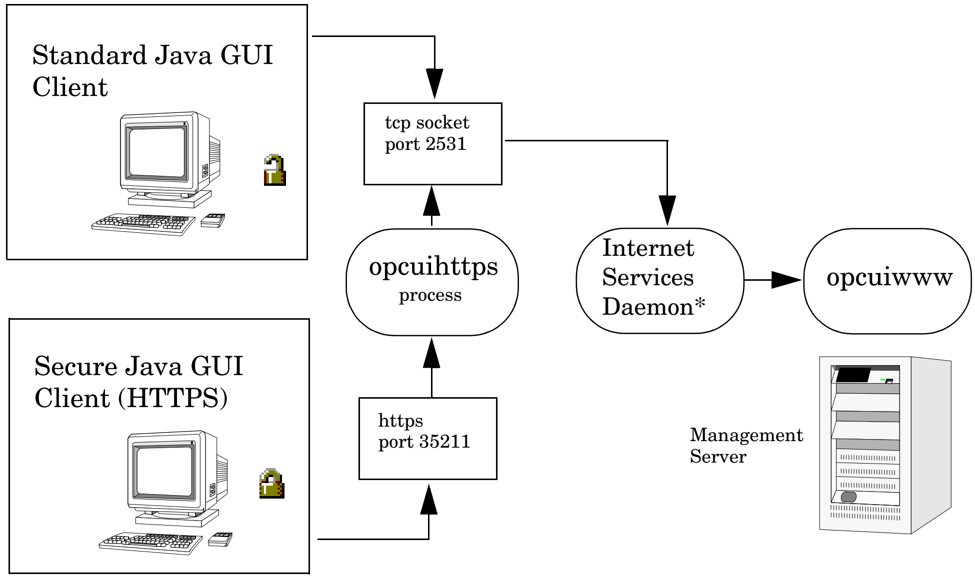
❏ HTTPS-based communication:

  If you are using the HTTPS-based Java GUI communication, a *closed* padlock icon appears on the login window and on the status bar.

❏ Standard communication:

  If you are using the standard HTTPS Java GUI communication, an *open* padlock icon appears in the GUI.

Figure 8-4 Client-server Communication



In Figure 8-4, references to the Internet Services Daemon mean `inetd` on UNIX and `xinetd` on Linux.

For more information about the authentication process that ensures the establishment of a secure communication, including the provision and installation of certificates, refer to the *HPOM Java GUI Operator's Guide*.

opcuihttps Configuration

The `opcuihttps` process acts as a proxy between the Java GUI client and the HP Operations management server. It is controlled by the OV Control process `ovcd`, which means that `opcuihttps` is started and stopped together with the other server processes.

The `opcuihttps` binary is installed in the `/opt/OV/bin/OpC` directory. The configuration parameters for `opcuihttps` are read at startup.

Changing HTTPS Parameters

To change the `opcuihttps` parameters that define the communication between HPOM management server and the Java GUI client, perform the following steps:

1. Use the ovconfchg command to set a parameter for the opcuihttps name space, as follows:

   ```
   # ovconfchg -ovrg server -ns opc.opcuihttps -set \
   <parameter> <value>
   ```

   For more information about the ovconfchg command, refer to the ovconfchg(1) reference page. See Table 8-4 on page 343 for a list of the parameters for configuring the opcuihttps process.

2. If any of the opcuihttps parameters are changed at runtime, you must restart the opcuihttps process.

Table 8-4 lists the parameters for configuring the opcuihttps process.

Table 8-4 The opcuihttps Parameters

Parameter	Format	Default value	Description
SERVER_PORT[a]	<*number*>	35211[b]	Port on which the Java GUI is listening.
OPCUIWWW_PORT	<*number*>	2531	opcuiwww port number as defined in the entry ito-e-guiin the /etc/services file.
SSL_CLIENT_ VERIFICATION_MODE	Anonymous | RequireCertificate	Anonymous	Whether the opcuihttps server accepts anonymous connections from the clients. If set to RequireCertificate, the clients require a certificate that permits full authentication[c].
MAX_CONNECTIONS	<*number*>	100	Maximum number of connections allowed to opcuihttps.

a. For troubleshooting purposes, you can also set the port in the command line, by starting opcuihttps the with the <*server_port*> parameter specified.
b. The port on which opcuihttps is listening is used to establish a secure HTTPS-based connection. The standard Java GUI uses the port 2531.
c. For full authentication, set also the startup parameter lcore_defaults to "yes".

NOTE You can check if it is possible to connect to the opcuihttps process using a web browser, such as Microsoft Internet Explorer or Mozilla. To do so, enter the following:

https://*<server>*:*<port>*/opcuihttps/info

In the example URL, *<server>* is an HP Operations management server hostname and *<port>* is the port on which opcuihttps is listening.

Secure Java GUI Connections

For the HTTPS-based Java GUI to communicate with an HPOM management server through a firewall, you can either configure one of the following:

- ❏ Firewall:

  Allow the HTTPS-based Java GUI direct access to the HPOM management server.

- ❏ HTTPS-based Java GUI:

  Use a proxy server for all communication with the HPOM management server. The default port on which the opcuihttps process is listening on the management server, is 35211. (The standard Java GUI uses port 3521.)

There are several different methods for specifying a proxy server for the HTTPS-based Java GUI:

- ❏ ito_op command-line tool
- ❏ itooprc file
- ❏ Login dialog box
- ❏ Java GUI applets
- ❏ Core functionality

For more information about the various methods for specifying Java-GUI connections through a proxy server, refer to the *HPOM Java GUI Operator's Guide*.

Operator Defaults

As an HPOM administrator, you can define default startup behavior for operator areas in Java GUI with two application groups:

❑ Shortcuts:

You can create new application groups that are added individually at the end of the Java GUI shortcut bar. These application groups can contain any kind of application.

❑ Workspaces:

You can create new application groups that are added individually after existing default workspaces in the Java GUI workspace pane. These application groups can contain any kind of application.

NOTE You can assign a set of shortcuts or workspaces to an individual operator, a group of operators, or all operators.

For more information about operator defaults assigned by the HPOM administrator, refer to the *HPOM Java GUI Operator's Guide*.

Assigning Operator Defaults

To assign operator defaults, you must be familiar with the following procedures:

1. Creating application groups using the `opcappl` command-line tool.
2. Adding applications to the application groups using the `opcappl` command-line tool.

   If you want to enable users to start applications as local applications in the Java GUI, specify the application call value as follows:

   - Windows:

     `app_call='cmd /c start` *`<application_name>`*`'`

   - Linux:

     `app_call='xterm -e` *`<application_name>`*`'`

- UNIX:

  `app_call='dtterm -e` *<application_name>*'

  For example, to enable starting `telnet` on Windows, enter the following command:

  ```
  # opcappl -add_app app_name=APP_X app_call="cmd /c start
  telnet $OPC_NODES" user_name=John passwd=xyz
  ```

3. Assigning applications and application groups using the `opccfguser` command.

NOTE When you assign an application with a hierarchical structure, that is an application group, the same structure is assigned to an operator.

For more information about command options and parameters, refer to the *opcappl(1m)* and *opccfguser(1m)* reference pages.

Custom Message-Group Icons

You can customize message-group icons by using the server-side variable `OPC_JGUI_MSGGRP_ICON` in one of the following ways:

- Icon color:

  Display the default message-group icon in monochrome (black and white). For more information about changing the icon color, see "Changing the Icon Color" on page 347.

- Icon image:

  Load a custom image. For more information about changing the icon image source, see "Changing the Icon Image" on page 347.

- Icon severity:

  Load an empty image but retain the severity status (for example, red for critical). For more information about retaining the icon severity, see "Retaining Icon Severity Status" on page 348.

Changing the Icon Color

To change the color of a default icon in the Java GUI from color to monochrome (black and white), use the `ovconfchg` command to set the OPC_JGUI_MSGGRP_ICON, as follows:

```
# ovconfchg -ovrg server -ns opc -set \
OPC_JGUI_MSGGRP_ICON=BW
```

Changing the Icon Image

To replace the default icon image with a custom image use the OPC_JGUI_MSGGRP_ICON variable to specify the path to the new image file and use the `ovconfchg` command to set the variable, as follows:

```
# ovconfchg -ovrg server -ns opc -set \
OPC_JGUI_MSGGRP_ICON=http://<HPOM_server>:3443/ \
ITO_OP/images/<file_name>.32.gif
```

<HPOM_server> Name of the HPOM management server where the custom image files are stored.

<file_server> Name of the custom image file you want to use to replace the default message-group icon.

Retaining Icon Severity Status

To load an empty image but retain the original severity status (for example, red for critical) use the `ovconfchg` command to set the OPC_JGUI_MSGGRP_ICON variable to “`nonexisting_image`”, as follows:

```
# ovconfchg -ovrg server -ns opc -set \
OPC_JGUI_MSGGRP_ICON=nonexisting_image
```

Client Version Control

The Java GUI Client Version Control feature enables the HPOM for UNIX administrator to use server-configuration variables to specify which versions of the Java GUI are required or recommended. This feature enables you to configure the HPOM management server to approve or deny connection requests from Java GUI clients on the basis of the Java GUI client version.

NOTE The Java GUI Client Version Control feature works with Java GUI client 8.26 and management server 8.27 patch levels. The functionality available with Java GUI client patch levels lower than 8.26 is limited. With Java GUI client patch level 8.21 and lower, the client version-control feature does not work.

The following server-configuration variables are available for specifying the Java GUI client version:

`OPC_JGUI_MINIMAL_VER`	The minimum *required* version of the Java GUI client that can connect to the HPOM management server.
`OPC_JGUI_RECOMMENDED_VER`	The minimum *recommended* version of the Java GUI client that can connect to the HPOM management server.

Specifying the Required Java GUI Client Version

To use the `ovconfchg` command to specify which version of the Java GUI client is *permitted* to connect to the HPOM management server, use the `ovconfig` command with the following parameters and options:

```
# ovconfchg -ovrg server -ns opc -set OPC_JGUI_MINIMAL_VER
A.08.27
```

The example shown prohibits Java GUI clients with versions lower than A.08.27 from connecting to the management server.

Specifying the Recommended Java GUI Client Version

To use the `ovconfchg` command to specify which version of the Java GUI client is *recommended* for any connection to the HPOM management server, use the `ovconfchg` command with the following parameters and options:

```
# ovconfchg -ovrg server -ns opc -set
OPC_JGUI_RECOMMENDED_VER A.08.29
```

In this example, the recommended Java GUI client version specified by the administrator is A.08.29. However, Java GUI clients with versions lower than the recommended version can still connect to the management server.

You can combine the configurations illustrated in Example and Example to make sure that the HPOM management server will only accept connections from the *recommended* Java GUI client version (A.08.29) and the *minimum* required Java GUI client version (A.08.27).

NOTE Connections from Java GUI clients that are allowed but not the recommended version display a message, which informs the operator which version of the Java GUI is recommended for connections to the selected management server. Connection requests from Java GUI clients other than the allowed or recommended versions are refused.

Specifying Exceptions to Permitted Java GUI Client Versions

To prevent Java GUI clients with versions lower than A.08.27 from connecting to the management server with the exception of A.08.26.QXCR1000xxxxxx, use the `ovconfchg` command with the following parameters and options:

```
# ovconfchg -ovrg server -ns opc -set OPC_JGUI_MINIMAL_VER
A.08.27,A.08.26.QXCR1000xxxxxx
```

NOTE The `listguis` command-line interface has been extended to show the Java GUI client version as well.

Tips and Tricks

The information in this section is designed to help you improve the overall performance of the HPOM Java-based operator GUI. The information provided covers the following areas:

- "User Sessions" on page 351
- "Security Exceptions" on page 352
- "Messages and Message IDs" on page 353

User Sessions

Before stopping the HP Operations management server or the database processes for any significant period of time, it is polite and helpful to identify the HPOM operators who are currently logged into HPOM with the Java GUI so that you can notify them of the planned outage.

Listing Java GUI Connections

To find out who is currently logged into HPOM with the Java GUI, use the `listguis` tool with the `-java` parameter as follows:

```
# /opt/OV/contrib/OpC/listguis -java
```

The command output lists the number of currently open Java GUI sessions and the following additional information:

`mode`	Process used by Java GUI connection, for example:	
	`m`	Master mode is the main process for the Java GUI for a specific user.
	`c`	Channel mode is a subprocess that forwards requests to the master (m).
`PID`	Process ID for the open connection, for example: 9110	
`Operator Name`	Name of the user logged in with the Java GUI, for example, `opc_adm`.	
`GUI hostname`	Host name of the machine where the Java GUI is running, for example: `omlux.hp.com`	

`GUI IP Address`	IP address of the machine where the Java GUI is running, for example: `15.16.17.180`.
`HTTPS`	Standard or secure connection (HTTP/S) between the Java GUI and the HPOM management server. For example, `Yes` (HTTPS) or `No` (HTTP).
`GUI Port`	Port on the HPOM management server that the Java GUI is using to connect to HPOM, for example: `35211`
`GUI Version`	Version of the Java GUI client connected to the HPOM management server, for example: `09.01.180`.
`Since`	Time at which the current connection from the Java GUI to the HPOM management server was first established, for example: `07:14`.
`%CPU`	Amount of CPU required to run the current connection, for example: `0.0`

You can use this information to contact the operators and ask them to close the Java GUI or, if necessary, kill the `opcuiwww` processes remotely.

Security Exceptions

If you receive a security exception warning when trying to run the Java GUI as an applet in a web browser, it is highly likely that the security file `identitydb.obj` is either missing or corrupt, for example, because it was not downloaded in binary mode.

Downloading the identitydb.obj Security File

To download the security file `identitydb.obj` in binary mode, follow these steps.

1. Open the file `/opt/OV/httpd/conf/mime.types`, and add the following line:

   ```
   application/x-javakey        obj
   ```

2. As user root, restart your Apache web server using the following command:

   ```
   # /opt/OV/httpd/bin/apachectl restart
   ```

3. Download the file `identitydb.obj` again.

Messages and Message IDs

By default, the Java GUI uses the complete contents of new (active) messages for all internal communication and processing instead of just the message ID. Using the complete contents of a message improves overall system performance by reducing the number and frequency of read-write requests to the database.

Configuring the Internal Use of Complete Messages

To ensure that you HPOM always uses the complete contents of new messages for internal communication rather than only the message ID, check that the configuration variable for `opcuiwww` is either not set or explicitly set to TRUE, as follows:

1. Check the current configuration settings using the `ovconfget` command, as follows:

   `#` **`ovconfget -ovrg server -ns opc`**

   The `ovconfget` command displays the content included in the `opc` section of the `local_settings.ini` file, for example:

   ```
   [opc]
   DATABASE=ov_net
   OPCUIWWW_NEW_MSG_NO_DB=FALSE
   OPC_HA=FALSE
   OPC_INSTALLATION_TIME=09/04/09 13:12:18
   OPC_INSTALLED_VERSION=09.01.180
   OPC_MGMTSV_CHARSET=utf8
   OPC_MGMT_SERVER=omlux1.hp.com
   OPC_SVCM_ADD_WARN_IF_EXISTS=TRUE
   OPC_SVCM_ERROR_CHECKING=FULL
   ```

2. Make sure that the variable OPCUIWWW_NEW_MSG_NO_DB is *not* set to =FALSE.

3. To set the variable OPCUIWWW_NEW_MSG_NO_DB explicitly to TRUE in the `opc` name space, use the `ovconfchg` command on the HPOM management server with the `-set` parameter, as follows:

   `#` **`ovconfchg -ovrg server -ns opc -set \`**
   `OPCUIWWW_NEW_MSG_NO_DB TRUE`

4. Check the new configuration settings using the `ovconfget` command, as follows:

```
# ovconfget -ovrg server opc
```

The command displays the updated content from the `opc` section of the `local_settings.ini` file including the *new* setting for the OPCUIWWW_NEW_MSG_NO_DB variable, for example:

```
[opc]
DATABASE=ov_net
OPCUIWWW_NEW_MSG_NO_DB=TRUE
...
```

For more information about the `ovconfget` and `ovconfchg` commands and the permitted parameters and options, refer to the `ovconfget(1)` and `ovconfchg(1)` reference pages respectively.

9 HPOM Processes

In this Chapter

This chapter provides a functional overview of the processes used by HP Operations Manager (HPOM) on the management-server processes and managed-node. For example, you can learn about the processes used by the message, monitor, and action agents on the managed node, and understand how they communicate with the message and action managers on the management server. You can also find out about how the management server communicates with the remote hosts running Java GUI clients.

The information in this chapter covers the following high-level topics:

❏ "Communication Flows in HPOM" on page 357

❏ "HPOM Management-Server Processes" on page 359

❏ "HPOM Managed-Node Processes" on page 364

❏ "Process Registration" on page 370

Communication Flows in HPOM

HP Operations agents and management servers communicate through Remote Procedure Calls (RPCs), based on BBC, queues, pipes, or signals. The mechanisms apply to communication between the management server and the managed nodes, as well as to communication between processes running locally on the management server.

Figure 9-1 Functional Overview of HPOM

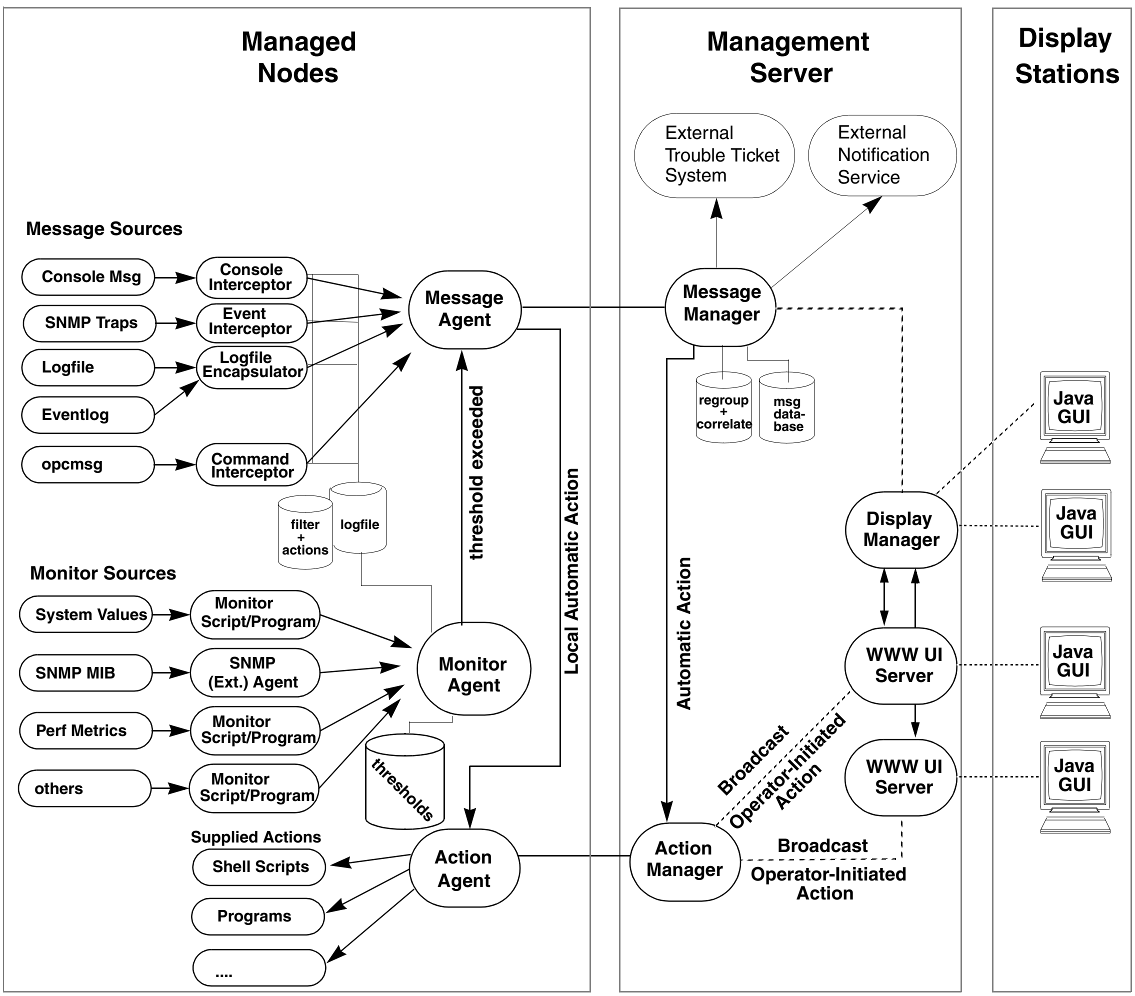


Figure 9-1 on page 357 illustrates the communication flow between the HPOM-specific processes running on the management server and the managed nodes.

For more information on how the processes communicate with one another and what each process does, see “HPOM Management-Server Processes” on page 359 and “HPOM Managed-Node Processes” on page 364.

HPOM Management-Server Processes

This section describes the HPOM processes and their associated files on the management server. In this section, you can find detailed information about the following topics:

- ❏ "Processes on the HPOM Management Server" on page 359
- ❏ "Process Files on the HPOM Management Server" on page 362

Processes on the HPOM Management Server

This following list describes the processes that run on the HP Operations management server. For more information about the queue files and pipes that the listed processes use, see "Process Files on the HPOM Management Server" on page 362:

`opcactm` — Action manager that feeds the action agents with automatic actions, operator-initiated actions, scheduled actions, and application startup and broadcasting information through the control agent. In addition, external instructions are determined using this mechanism.

`ovoareqsdr` — Request sender that informs the control agents to start, stop, or update their local HPOM agents. The request sender is also responsible for the self-monitoring of HPOM manager services, and for the heartbeat-polling of the managed nodes.

`ovcd` — Control daemon that controls and checks the status of processes and components, which are registered with it.

`opcdispm` — Display manager that serves HPOM GUIs. The display manager also feeds the action manager with operator-initiated actions, application startup information (not requiring a separate terminal), and broadcasting information issued by operators. It also serves clients connected to the MSI for message and configuration changes. Several HPOM user GUIs may be active at the same time.

`opcbbcdist`	Configuration management adapter between the HP Operations management server and the HTTPS agents that creates instrumentation from existing actions, commands, and monitors, and switches `nodeinfo` settings into the XPL format used on HTTPS nodes.
`opcecm`	Event correlation manager that connects to the server MSI to allow access to and modification of messages from the HPOM message flow by the event correlation (EC) engine. Depending on filters and conditions, the messages are then correlated and written back to HPOM. The messages display in the `Message Details` window (available from the Message Browser) with the message source MSI `opcecm`. Like all server processes, the event correlation manager is controlled by the OV Control, `ovcd`.
`opcecmas`	Annotation server that runs on the management server and obtains data from outside the ECS engine for use within correlation circuits. This process connects to the `opcecm` process using the standard annotate API. It receives annotate requests for launching external programs and returns the output to the circuit.
`opcmsgm`	Message manager that receives messages from the managed nodes through the message receiver (`opcmsgrb`). The messages can be correlated, regrouped and logged by the message manager running on the management server. The message manager is also responsible for adding annotations, triggering notifications, and forwarding the message to the trouble ticket and notification service manager for external notification and trouble ticket generation.
`opcforwm`	Message forwarding manager that relieves the message manager, `opcmsgm`, of time-consuming tasks (for example, sending messages to remote managers). This relief allows the message manager to manage messages more effectively. On the local “source” management server, the message forwarding manager receives data from the message manager (in the form of messages), the action manager (action responses), and the display manager (message operations such as

acknowledge, add annotation, and so on). The message forwarding manager sends data to the message receiver on the “target” management servers.

`opctss` Distribution manager subprocesses that transfer configuration data to the distribution agent through TCP/IP.

`opcttnsm` Trouble ticket and notification service manager that feeds the external notification interface, as well as the external trouble ticket interface, with message attributes. This manager is an auxiliary process of the message manager designed to ensure high message throughput. If external instructions are specified for a message, the trouble ticket and notification service manager evaluates the help text through the action manager.

Whenever the trouble ticket and notification service manager receives a message in its queue, it passes the message on to the trouble ticket interface or the external notification service. It does so by forking and executing the customer-defined program that receives the message (that is, the ticketing interface or the notification service).

As soon as this program is finished and exited, a `SIGCHLD` is sent to the trouble ticket and notification service manager. The manager stops processing the message queue until it receives another `SIGCHLD`.

`opcuiwww` Server process that serves the HPOM Java-based operator GUI. This process forwards all communication requests between the Java GUI and the display manager. For each Java GUI, at least one server process is started.

`opcuihttps` Server process that acts as a proxy between the Java GUI client and the HPOM management server using the HTTPS protocol.

`opcsvcm` Service engine that maintains the global (operator-independent) service status and can log service changes into the database.

By default, remote access to the service engine is disabled. See *HPOM Developer's Reference* for information on how to allow remote access to the service engine.

Process Files on the HPOM Management Server

The files used by the HPOM management-server processes reside in the following directory:

`/var/opt/OV/share/tmp/OpC/mgmt_sv`

The following list describes the queue files and pipes that the HPOM management-server processes use. For more information about the HPOM management-server processes themselves, see "Processes on the HPOM Management Server" on page 359:

`actreqp/actreqq`	Queue or pipe used by the display manager, message manager, TTNS manager, (and action manager) to pass action requests to the action manager.
`actrespp/actrespq`	Queue or pipe used by the message receiver, request sender, and action manager to pass action responses to the action manager.
`ctrlq/ctrlp`	Queue or pipe between the display manager and control manager.
`forwmgrp/forwmgrq`	Queue or pipe used by the message manager, display manager, action manager, and the forward manager to pass data to be forwarded to other management servers.
`magmgrp/magmgrq`	Queue or pipe between the message dispatcher and the request handler.
`mpicdmp/mpicdmq`	Queue or pipe used by the display manager and the message stream interfaces to transfer control sequences for message-change event handling.

`mpicmmp/mpicmmq`	Queue or pipe used by the message manager and message-stream interfaces to transfer control sequences for message handling through the Message-Stream Interface (MSI).
`mpimmp/mpimmq`	Queue or pipe used by the message manager and the message-stream interfaces to transfer messages from MSI programs to the message manager.
`msgmgrq/msgmgrp`	Queue or pipe between the message receiver and message manager.
`opcecap/opcecaq`	Queue or pipe used to pass messages from the message manager to the event correlation manager.
`pids`	Process IDs of the HPOM managers that are controlled by the HPOM control manager, which is also used for self-monitoring.
`rqsdbf`	Buffer file used by the request sender to store requests if the control agent on a given managed node cannot be accessed
`rqsp/rqsq`	Queue or pipe between the request handler and the request sender. Also used by the display manager and the action manager
`ttnsarp/ttnsarq`	Queue or pipe used by the trouble-ticket manager and action manager when message instructions have to be fetched by the trouble-ticket notification-service (TTNS) manager.
`ttnsq/ttnsp`	Queue or pipe between the message manager, trouble-ticket manager, and notification-service manager.

HPOM Managed-Node Processes

This section describes the HPOM processes and their associated files on the managed nodes. In this section, you can find detailed information about the following topics:

Processes on the Managed Node

The information in this section lists and describes the HPOM processes on the managed node. For more information about the files the managed node processes use, see "Process Files on the Managed Node" on page 366.

`coda`	Embedded performance component that collects performance counter and instance data from the operating system. Threshold monitor policies are used to access performance metrics collected by the embedded performance component.
`opcacta`	Action agent that is responsible for starting and controlling automatic actions, operator-initiated actions, and scheduled actions (that is, scripts and programs). The action agent is also used for broadcasting commands and for launching applications configured as Window (Input/Output).
`opceca`	Event correlation agent that connects to the agent MSI in the same way that the ECS runtime library is integrated into the HPOM server. This connection allows access to (and modification of) messages from the HPOM message flow on the agent. The messages modified by this process display in the `Message`

`Details` window (available from the Message Browser) with the message source "`MSI: opceca`". Like all agent processes, `opceca` is controlled by the control agent.

`opcecaas` Annotation server that runs on a managed node and obtains data from outside the ECS engine for use within correlation circuits. This process connects to the `opceca` using the standard annotate API. It receives annotate requests for launching external programs and returns the output to the circuit.

`opcle` Logfile encapsulator that scans one or more application or system-logfiles (including the Windows Eventlog) for messages or patterns specified by the HPOM administrator. The logfile encapsulator forwards the scanned and filtered messages to the message agent.

`opcmona` Monitor agent that monitors the following components:

- System parameters, for example: CPU load, disk utilization, and kernel parameters.
- SNMP MIBs
- Other parameters, if specified

The monitor agent checks the values it finds against predefined thresholds. If a threshold is exceeded, a message is generated and forwarded to the message agent. The polling interval of the monitored object can be configured by the HPOM administrator. In addition, the `opcmon(1)` command and `opcmon(3)` API can be used (asynchronously) to feed the monitor agent with the current threshold values.

The monitor agent does not immediately begin monitoring when agents are started. Instead, it waits one polling interval, and only then executes the monitor script for the first time. Typically, polling intervals are 30 seconds to 5 minutes.

`opcmsga` Message agent that receives messages from the logfile encapsulator, monitor agent, console interceptor, event interceptor and message interceptor on the local system. The messages are forwarded to the message receiver running on the management server. If the connection to the management server has been lost, the

	messages are buffered locally. The message agent triggers local automatic actions by forwarding the task to the action agent.
`opcmsgi`	Message interceptor that receives and processes incoming messages. The `opcmsg(1)` command and `opcmsg(3)` API can be used to forward messages to HPOM. Conditions can be set up to integrate or suppress chosen message types.
`opcctla`	Control agent that starts and stops all HPOM agents, and performs HPOM self-monitoring tasks. The control agent is informed of new configuration and distribution requests by the request sender.
`opctrapi`	Event interceptor that is the message interface for feeding SNMP events to HPOM. Conditions can be set to integrate or suppress selected message types.

Process Files on the Managed Node

This section describes the pipes and queue files used by the HPOM processes outlined in “Processes on the Managed Node” on page 364. The locations of these process files are listed in “Location of Process Files on the Managed Node” on page 368.

`actagtp/actagtq`	Queue or pipe for pending action requests for the action agent. The pending action requests are filled by the message agent and the control agent. The action agent polls the queue every 5 seconds.
`monagtq/monagtp`	Queue on UNIX systems between the HPOM monitor command `opcmon(1)`, the HPOM monitor API `opcmon(3)`, and the monitor agent. The monitor agent checks the queue after the termination of the triggered monitor scripts or programs every 15 seconds, if externally monitored objects are configured.
`mpicmap/mpicmaq`	Queue or pipe used by the message agent and the message stream interfaces to transfer control sequences for message handling through the MSI.

`mpimap/mpimaq`	Queue or pipe used by the message agent and the message stream interfaces to transfer messages from MSI programs to the message agent.
`msgagtdf`	File that holds any messages that cannot be passed to the management server (for example, if the network is down). The messages are read from this file after the management server is available.
`msgagtp/msgagtq`	Queue or pipe for local buffering of messages to be sent to the message receiver when the management server is not accessible.
`msgip/msgiq`	Queue or pipe (only on UNIX systems) between the HPOM message command `opcmsg(1)` or the HPOM message API `opcmsg(3)` and the message interceptor.
`opcecap/opcecaq`	Queue or pipe that passes messages from the message agent to the event-correlation agent.
`pids`	Process IDs of HPOM agents controlled by the control agent.
`trace` (plain text)	HPOM trace logfile. For more information on activating tracing, see "Tracing Problems" on page 407.
`aa*`	Temporary files used by the action agent, for example, to store the action or application output written to `stderr` and `sdtout`.
`moa*`	Temporary files used by the monitor agent.

Location of Process Files on the Managed Node

Table 9-1 shows the location of the files used by the HPOM agent processes described in "Processes on the Managed Node" on page 364. For more information about the files used by the HPOM agent processes on the managed nodes, see "Process Files on the Managed Node" on page 366.

Table 9-1 Locating Process-related Files on the Managed Nodes

Platform	File Location
AIX	`/var/lpp/OV/tmp/OpC`
HP-UX 11.x	`/var/opt/OV/tmp/OpC`
Linux	
Solaris	
Windows	`\usr\OV\tmp\OpC\<node>`

HPOM-Agent Configuration Files

Table 9-2 describes the files you can use to configure the HPOM agent, and indicates whether the contents of the files are encrypted. For more information about the locations of the agent-configuration files, see Table 9-3 on page 369.

Table 9-2 Agent Configuration Files and their Contents

File	Contents	Encrypted?
`le`	Logfile encapsulation configuration	✓
`mgrconf`	Flexible-management configuration file	✗
`monitor`	Monitor agent policy file	✓
`msgi`	Message interceptors `opcmsg(1)` and `opcmsg(3)`	✓

Table 9-2 Agent Configuration Files and their Contents (Continued)

File	Contents	Encrypted?
`nodeinfo`[a]	Node-specific HPOM configuration information (for example, the logging directory and the type of managed node internal character set).	✗
`primmgr`	MOM configuration file.	✗
`trapi`	SNMP event interceptor.	✓

a. Only on RPC-based managed nodes.

Location of HPOM Agent Configuration Files

Table 9-3 lists the locations of the HPOM agent specific configuration files described in Table 9-2 on page 368.

Table 9-3 Locating Agent Configuration Files on the Managed Nodes

Platform	Agent File Location
AIX	`/var/lpp/OV/conf/OpC`
HP-UX 11.x	`/var/opt/OV/conf/OpC`
Linux	
Solaris	
Windows	`\usr\OV\conf\OpC\`*<node>*

Process Registration

The HPOM process-control component (`ovcd`) controls all HPOM management-server processes—starting, stopping, auto-restarting—and ensures they occur in the correct order. Each server process is registered with the process-control component in one or more XML registration files. The default registration files are located on the management server in the following location: `/etc/opt/OV/share/ovc/`.

All HPOM processes are automatically registered with the HPOM control daemon, `ovcd`, and can be controlled using the `ovc` command with the `-start`, `-stop`, and `-status` options respectively. Each HPOM server process has its own XML registration file that defines how the HPOM processes are handled.

The configuration files that define the registration process for each process are stored in the following location on the management server and the managed node: `/var/opt/OV/conf/ctrl/`. On the management server, the `ctrl/` directory contains registration files for *all* HPOM process—both management-server processes and managed-node processes, if the management server is also configured as a managed node. On the managed node, the directory contains registration files only for the managed-node processes.

Custom Process Management

HPOM enables you to manage custom processes by adding them to a list of managed components and registering them with the HPOM control daemon, `ovcd`. In this way, the additional custom processes can be managed in the same way as any other HPOM process.

Adding a Custom Component to HPOM Control

To register a custom process with the HPOM control daemon, `ovcd`, perform the following steps:

1. Create an XML registration file to register the custom process.

   You can use the sample file `opccustproc1.xml` provided with HPOM as a template for y our XML registration file, as follows:

a. Copy and rename the template configuration file `/etc/opt/OV/share/ovc/opccustproc1.xml` according to your needs, for example:

```
# cp /etc/opt/OV/share/ovc/opccustproc1.xml
/etc/opt/OV/share/ovc/<my_process>.xml
```

Note that you must replace *<my_process>* with the name of the process you want to register.

b. Modify the following tags in the *<my_process>*`.xml` file according to your needs. If you need further help, see the example for the `opccustproc1.xml` file:

```
<ovc:Name>opccustproc1</ovc:Name>
<ovc:String>OMU Custproc 1</ovc:String>
<ovc:AllowAttach>false</ovc:AllowAttach>
<ovc:AutoRestart>true</ovc:AutoRestart>
<ovc:AutoRestartLimit>5</ovc:AutoRestartLimit>
<ovc:AutoRestartMinRuntime>60</ovc:AutoRestartMinRunt
ime>
<ovc:AutoRestartDelay>5</ovc:AutoRestartDelay>
<ovc:MentionInStatus>true</ovc:MentionInStatus>
<ovc:Monitored>true</ovc:Monitored>
<ovc:StartAtBootTime>false</ovc:StartAtBootTime>
<ovc:WorkingDirectory>/var/opt/OV/share/tmp/OpC/mgmt_
sv
</ovc:WorkingDirectory>
<ovc:ProcessDescription>opccustproc1</ovc:ProcessDesc
ription>
```

Under the `<ovc:Name>`**START**`</ovc:Name>` tag, modify:

```
<ovc:CommandLine>/opt/OV/bin/OpC/opccustproc1</ovc:Co
mmandLine>
```

You can delete the `<ovc:Name>`**START_CHECK**`</ovc:Name>` tag along with its subtags or modify it as follows:

```
<ovc:CommandLine>/opt/OV/bin/OpC/opcsv -available
opccustproc1</ovc:CommandLine>
```

2. Check the syntax of the new *<my_process>*`.xml` file using the `ovcreg` command with the `-check` parameter, as follows:

```
# ovcreg -check /etc/opt/OV/share/ovc/<my_component>.xml
```

3. Register the new *<my_process>*.xml file using the ovcreg command with the -add parameter, as follows:

   ```
   # ovcreg -add /etc/opt/OV/share/ovc/<my_component>.xml
   ```

4. Start, stop, and check the status of the new custom process using the ovc command with the -start, -stop, and -status parameters, respectively. For example, to start the custom process, run the following command:

   ```
   # ovc -start <my_process>
   ```

5. To cancel the registration of the custom process, use the ovcreg command with the -del(ete) parameter:

   ```
   # ovcreg -del /etc/opt/OV/share/ovc/<my_component>.xml
   ```

10 HPOM Security

In this Chapter

This chapter explains the security measures you can investigate and implement in the wider context of HP Operations Manager (HPOM) for example: system security, network security, HPOM security, log-in authentication, and best practices for system audits. The information in this chapter is organized into the following topic areas:

Security Overview

The security of your HPOM system involves much more than the configuration of the HPOM software; it requires attention to security matters in the wider environment that is monitoring, too. In particular, you should investigate how you can improve security practices in the following areas:

- System security:

  Enable the HP Operations management server and managed node to run on a “trusted” system.

  For details, see “System Security” on page 376.

- Network security:

  Protect data that is exchanged between the management server and the managed node.

  For details, see “Network Security” on page 378.

- HPOM security:

  Investigate security-related aspects of application setup and execution, operator-initiated actions, and HPOM auditing.

  For details, see “HPOM Security” on page 383 and “HPOM Audits” on page 396.

NOTE To find out how HPOM behaves in an environment protected by firewalls, see the *HPOM Firewall Configuration* white paper.

System Security

This section describes how HPOM behaves in trusted system environments.

NOTE Before installing and running HPOM on any system, you must ensure that the system-level security measures comply with your organization's system security policies. To learn about system-level security policies, see the product documentation for the relevant operating systems as well as your specific company guidelines.

Guidelines for System Security

A secure or "trusted" system uses a number of techniques to improve security at system level. Many different system security standards exist, ranging from standards with industry-wide recognition, such as the Controlled Access Protection (C2) system developed by the U. S. Department of Defense, to standards that are established and used internally in IT departments within enterprises.

NOTE Installing and running HPOM in a C2-secure environment is not certified.

Different system security standards vary in stringency and apply a variety of system security techniques, including the following:

❏ Authentication:

  System security standards may impose strict password and user authentication methods for the user login procedure. HPOM supports the authentication module (PAM) for the authentication of users during the Java GUI login sequence. PAM enables multiple authentication technologies to be added without changing any of the login services, thereby preserving existing system environments. For more information on PAM authentication, see "PAM Authentication" on page 385.

When imposing system security standards, be aware that password aging and changing can lead to problems with application startup if any passwords have been hard coded in HPOM.

❏ Auditing:

System security standards may require regular auditing of networking, shared memory, file systems, and so on. HPOM enables the auditing of any kind of user interaction within HPOM. For further details, see “HPOM Audits” on page 396.

❏ Terminal access and remote access:

System security standards may include measures to control access to terminals. If the system security policy disallows root login through the network, HPOM agents must be installed manually.

❏ File access:

System security standards may include measures to manage access to files. Some policies recommend the use of access control lists (ACLs). When maintaining the system security standard on a system running HPOM, be aware that HPOM does not use ACLs. HPOM imposes strict file access permissions, and protects important files either by encrypting them or by using digital signatures.

Network Security

In HPOM, network security is designed to improve the security of connections between processes. These secure process connections can be within a network, across multiple networks, or through routers or other restrictive devices.

For example, you could limit access to a network or a section of a network by restricting the set of nodes (with or without HPOM agents running on them) that are allowed to communicate with the management server across restrictive routers or even a packet-filtering firewall. HPOM provides robust security regardless of whether the server or the network of managed nodes are inside or outside the firewall. A management server outside your firewall can manage a network of nodes inside your firewall. Conversely, a management server inside your firewall can manage nodes outside your firewall.

One way of limiting access to a network, and consequently improving the network's inherent security, is to restrict all connections between HPOM processes on the management server and a managed node to a specific range of ports. To simplify matters, HPOM sets the default value on the managed node to "No security," and enables you to select the security configuration node by node. In this way, you can change the security of a given node, depending, for example, on whether there is a need for the node to communicate across a firewall or through a restricted router.

HTTPS Security

HTTPS 1.1 based communication is the communication technology used for HP Software products and enables applications to exchange data between heterogeneous systems.

HTTPS communication uses the Secure Socket Layer (SSL) protocol to validate access to data and encryption to secure the exchange of data. With businesses sending and receiving transactions across the Internet and private Intranets, security and authentication assume an especially important role.

HTTPS communication meets this goal through established industry standards. The HTTP protocol and SSL encryption and authentication ensure data integrity and privacy:

- By default, data is compressed, ensuring that data is not transmitted in clear text format, even for non-SSL connections.
- All remote messages arrive through the Communication Broker, providing a single port entry to the node.
- You may specify a restricted bind port range for use in configuring firewalls.
- When sending messages, files, or objects, you may configure one or more standard HTTP proxies to cross a firewall or reach a remote system.

For further information about HTTPS security in HPOM, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

HPOM Process Security

In HPOM, the management server and the managed nodes simultaneously run both RPC clients and servers. As a result, HPOM reduces the process configuration information needed to execute Remote Procedure Calls (RPC).

To execute an RPC, HPOM requires the following configuration information about a process:

- Name and password
- Security level

This configuration information must be present on both the management server and the managed node.

HPOM Security Levels

HPOM enables you to select and configure the security level that your particular environment requires for each managed node.

NOTE For HTTPS-based managed nodes, you can get this value by calling `ovconfget`, or change it by calling the `ovconfchg` command-line tool. For more details, refer to *HPOM HTTPS Agent Concepts and Configuration Guide*. Refer, also, to the *ovconfget()* and *ovconfchg()* reference pages for more information.

In this way, security on a given managed node may be changed to handle, for example, the addition of sensitive connections.

It is possible that the process fails or is required to run in the unauthenticated mode due to the temporary unavailability or poor configuration of the security service. HPOM can be configured to help you to work around such situations.

For example, HPOM generates an error message if a management-server process (such as the request sender) receives an authentication failure when calling a control agent on a managed node. This error message displays in the `Message Browser` window. As an HPOM administrator, you can then take immediate corrective action, for example, by temporarily changing the security level on the managed node in question to allow the retransmitted request to succeed.

CAUTION When correcting authentication failures, be careful. An error in the connection can, in certain circumstances, indicate that the system is under attack.

Secure Shell

The HPOM agent software can alternatively be installed using the Secure Shell (SSH) installation method. For details, see “Secure Shell Installation” on page 38.

Secure Shell (SSH) is a UNIX program that can be used to log into and execute commands on a remote computer. SSH is intended to replace `rlogin` and `rsh` and provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. The SSH provides a number of security features, such as:

- Port forwarding:

  All communication between two systems is conducted between well-known ports, thereby creating a virtual encrypted communication channel.

- RSA authentication:

  All logins, even those without a password, use RSA authentication.

- Public-key encryption:

  All traffic between systems is secured with public-key encryption.

HPOM Agent Installation Using Secure Shell

The SSH installation method provides enhanced security for installations that are performed over insecure lines (for example, over the Internet).

Files needed for agent installation are copied using SCP (Secure CoPy), and remote commands are executed using the command execution facility built into SSH. As a result, no one can eavesdrop on or alter communications between systems.

The HPOM installation procedure works with any configuration already established on the management server, regardless of security features used, as long as you have set up a automatic (password-less) login for user `root` on the managed node. The best way to set up this login is to establish an RSA-based password-less login. For more information, see "Installing HPOM Agent Software Using SSH" on page 39.

SSH-based Virtual Terminal

An SSH client is used to ensure the secure virtual terminal connection to UNIX systems. Compared to `telnet` and `rlogin`, the SSH-based virtual terminal offers a considerably higher level of secure access and communication.

Install and configure the SSH client on both the management server and the managed node to be able to use all the advantages the SSH-based virtual terminal feature offers.

NOTE The SSH client is not provided with HPOM by default.

To open secure virtual terminals on the managed nodes, run the following command:

```
# opcrlogin -h <hostname> -u <username> -ssh Y
```

In this example. *<hostname>* is the name of the managed node to which secure connection will be established, and *<username>* is the name of the user, which will be used for establishing connection.

HPOM Security

As an HPOM administrator, you need to carefully think through the security implications of your HPOM configurations. For example, managed nodes allow only those management servers that they recognize as action-allowed managers to execute operator-initiated actions.

Access to HPOM

Only registered HPOM users can access the HPOM GUI. By default, the users `opc_adm` and `opc_op` are available.

HPOM Operator Names

HPOM user names and passwords have no direct relation to UNIX user names and passwords. However, you can use UNIX user names as HPOM user names. If you decide to use UNIX user names as HPOM names and the UNIX user name is defined in the HPOM database, HPOM does not prompt the user for a password during login. This is the fastest way to open an HPOM GUI. If you use UNIX user names, you should map UNIX user names to HPOM operator names.

HPOM Operator Passwords

As an HPOM administrator, you can change the passwords defined for HPOM operators. However, you cannot see new passwords set by operators (the characters appear as asterisks). By default, operators can change their own passwords.

Preventing Operators from Changing Passwords

To remove the change-password functionality from all operators, perform the following steps:

1. Open the following `opcop` file, which you can find in the following location:

   ```
   /etc/opt/OV/share/conf/OpC/mgmt_sv/appl/registration/\
   C/opc_op/opcop
   ```

2. Add the following lines to the file:

```
Action “Change Password”
{
}
```

Java GUI Permissions

The HPOM Java-based operator GUI communicates with the HP Operations management server through port 2531. The `inetd` (on HP-UX and Solaris) or `xinetd` (on Linux) monitors port 2531 and starts the process `/opt/OV/bin/OpC/opcuiwww` when it receives a request for the service `ito-e-gui`.

By default, the HP Operations management server accepts connections from any client. On the management server, you can restrict client access to specific systems as follows:

- On HP-UX:

  Edit the `/var/adm/inetd.sec` file. Make sure to specify the systems for the service `ito-e-gui`.

- On Linux:

  Edit the `/etc/xinetd.d/ito-e-gui` file.

Program Security

The HP-UX 11.x programs `/opt/OV/bin/OpC/opc` and `/opt/OV/bin/OpC/opcuiadm` have the s-bit, which sets the user-ID on execution.

Database Security

Database security is controlled by the operating system and by the database itself. Users must have an operating-system logon to be able to access the database either remotely or locally. After a user is logged on, the security mechanisms of the database control access to the database and tables.

For more information about database security, see the vendor’s manuals supplied with the database.

HPOM Security

Starting Applications

Applications run under the account (user and password) specified by the administrator during application configuration. The action agent uses the information in this account before executing an application. The action agent switches to the user specified and then uses the name and password stored in the application request to start the application.

User Root

If the user account under which the HPOM agents are running has been switched to a user other than root, you have to carry out additional configuration steps. For more information about command options and parameters, see the reference page *opcswitchuser(1M)*.

Password Aging

Application execution can be compromised by the use of password aging. Password aging is a standard security feature that requires passwords to expire automatically, for example, if the following has occurred:

- A specified period of time has passed
- A specified date has been reached
- A specified number of unsuccessful login attempts have been made

If password aging is enabled, application startup failures can occur if the account that a given application uses is temporarily inaccessible. You can reduce the occurrence of such startup failures by implementing the HPOM plug-in interface for the PAM authentication module, which enables third-party authentication methods to be used while preserving existing system environments.

PAM Authentication

You can use a Plug-in Authentication Module (PAM) to retrieve and check user names and password information. The user information is saved in a central repository to which the PAM module has access. To set up PAM for authentication, use the `ovconfchg` command on the HP Operations management server. For more information about the `ovconfchg` command, refer to the *ovconfchg()* reference page.

PAM User Authentication

The HPOM user model requires users (humans or programs) to log on to the HP Operations management server before being able to use any further functionality. This mainly applies to the Java-based graphical user interface, but also to some of the HP Operations management server APIs and command line tools.

The log-in procedure is necessary for the following checks:

❏ Authenticate the user and verify access permission.

❏ Determine the user's capabilities.

HPOM provides the possibility to use PAM alternatively to the built-in authentication.

Using PAM has the following major advantages:

❏ Common user database:

  PAM shares a common user database with the operating system and other applications. User accounts and passwords have to be set up and maintained only in one place.

❏ High security:

  Higher security measures such as stronger encryption, password aging, account expiration, and so on are available and can be enforced.

NOTE These security measures only apply to the user-authentication process. The HPOM user accounts must still exist to determine the user's capabilities.

The following restrictions apply to PAM user authentication with HPOM:

❏ Account or session management:

  HPOM PAM does not support either the management of PAM accounts or PAM-authenticated sessions. HPOM uses PAM *only* for authentication.

- ❑ Account setup:

  Account setup and management (including password update) must be done using external tools depending on the PAM mechanism used. For example, if the UNIX `passwd` PAM module is used, the standard UNIX commands have to be used to deal with user accounts and passwords on the OS level.

  The HPOM password change facility only updates the user's password in the HPOM database. This password is *not* used for authentication when PAM authentication is enabled. Use external tools to modify or set the user's password.

- ❑ Password requests:

  It is not possible to use authentication stacks which request multiple passwords.

Configuring PAM User Authentication

To configure HPOM user authentication to use the PAM module, perform the following steps:

1. Enable PAM user authentication in HPOM. Set the variable `OPC_USE_PAM_AUTH` to `TRUE`:

   ```
   # /opt/OV/bin/ovconfchg -ovrg server -ns opc -set \
   OPC_USE_PAM_AUTH TRUE
   ```

   This setting will instruct HPOM to use PAM as authentication mechanism. It will become effective after the HP Operations management server processes are restarted.

2. Configure PAM to route HPOM authentication requests to the desired PAM module. Note the following operating-system-specific information:

   - HP-UX and Solaris:

     Add the following entry to the PAM configuration file `pam.conf`: *pam.conf(4)*:

     ```
     ovo        auth        required        <module>
     ```

     In this example entry in the `pam.conf` file, note the following:

     `ovo` HPOM application ID.

     `auth` Module used for authentication only.

HPOM Security

`required`	Authentication step must succeed.
`<module>`	Name of PAM module to be used. Technically, this a shared library which implements the authentication mechanism, for example: UNIX passwd, Kerberos, NIS, or LDAP.

- Linux:

  Edit the PAM configuration file `/etc/pam.d/ovo`.

For example, to use UNIX passwd authentication use the following entries in `pam.conf`:

- HP-UX 11.31 Itanium:

```
ovo auth required \
/usr/lib/security/hpux32/libpam_unix.so.1

ovo account required \
/usr/lib/security/hpux32/libpam_unix.so.1
```

- Sun Solaris:

```
ovo   auth      requisite   pam_authtok_get.so.1
ovo   auth      required    pam_unix_auth.so.1
ovo   account   required    pam_unix_account.so.1
```

- RHEL 5.x:

```
auth       include     system-auth
account    required    pam_nologin.so
account    include     system-auth
password   include     system-auth
session    optional    pam_keyinit.so   force   revoke
session    include     system-auth
session    required    pam_loginuid.so
```

3. *Optional*: Set user-based or module-specific flags. For more information, refer to the PAM documentation.
4. Create user names and corresponding passwords for the HPOM administrator (`opc_adm`) and each of the HPOM operators. You might have to use external tools, depending on the selected PAM mechanism.

5. Create the remaining HPOM operator accounts in HPOM and assign the required responsibilities. Log on to HPOM as opc_adm using the password specified in the previous step.

NOTE If logging into the HPOM Java GUI is configured using LDAP or Kerberos, you need to replace the original opcuiwww binary with opcuiwww.ldap. Otherwise, the Kerberos authentication fails.

Back up the original opcuiwww binary and replace it with /opt/OV/bin/OpC/opcuiwww.ldap delivered with HPOM within the HPOvOUWwwOra package.

Disabling PAM User Authentication

To disable PAM user authentication in HPOM, set the variable OPC_USE_PAM_AUTH to FALSE:

The new setting will become effective after the management server processes are restarted.

Counting Failed PAM-Authenticated Logins

You can count the number of PAM-authenticated failed logins to the Java GUI for each user/operator. The value of that counter is stored as a configuration variable in the operator's name space user.<username>.

To enable the PAM count functionality for failed logins, perform the following steps:

1. Enable PAM user authentication using the ovconfchg command with the following parameters and options:

   ```
   # /opt/OV/bin/ovconfchg -ovrg server -ns opc -set
   OPC_USE_PAM_AUTH TRUE
   ```

2. Set the counter for failed PAM-authenticated logins using the ovconfchg command with the following parameters and options:

   ```
   # /opt/OV/bin/ovconfchg -ovrg server -ns opc -set
   OPC_USE_PAM_FAILED_LOGIN_COUNTER TRUE
   ```

After the third failed login, the following configuration variables are updated in each user.*<username>* name space (the stated values are just examples):

FAILED_LOGIN_ATTEMPT_COUNTER=3 (Counter)

LAST_FAILED_LOGIN_ATTEMPT=1197559311 (Time in seconds since epoch)

LOGIN_ATTEMPT_DELAY=60 (Delay in seconds)

You can list the values by entering the following command:

```
# /opt/OV/bin/ovconfget -ovrg server user.<username>
```

NOTE After the third failed login, all further logins for this user are blocked if LOGIN_ATTEMPT_DELAY did not elapse yet.

These configuration variables can be overwritten. For example, you can reset counter, time and/or delay by using the following commands:

```
# /opt/OV/bin/ovconfchg -ovrg server -ns user.<username>\
-set FAILED_LOGIN_ATTEMPT_COUNTER 0
```

```
# /opt/OV/bin/ovconfchg -ovrg server -ns user.<username>\
-clear LAST_FAILED_LOGIN_ATTEMPT -clear\ LOGIN_ATTEMPT_DELAY
```

Remote Access

This section describes security for remote login and command execution in UNIX environments.

Application Startup and Command Broadcast

If HPOM operators do not log in with the default user account set up by the HPOM administrator, they must use the corresponding passwords for broadcasting commands or starting applications. If operators do not use the correct passwords, the command or application will fail.

I/O Application Startup

When starting applications configured as **Window (Input/Output)**, operators must do one of the following:

- ❏ Specify passwords with the application attributes.
- ❏ Provide `.rhosts` entries or `/etc/hosts.equiv` functionality.
- ❏ Specify passwords interactively.

Password Assignment on Managed Nodes

This section explains how to assign passwords on UNIX and Microsoft Windows managed nodes.

Password Assignment on UNIX Managed Nodes

On UNIX managed nodes, the default HPOM operator `opc_op` cannot login into the system through normal login, telnet, and so on because of a `*` entry in the `/etc/passwd` file and because `.rhosts` entries are not provided. If you want to provide a virtual terminal or application startup (requiring user input or output)) for the default HPOM operator, set the password or provide `.rhosts` or `/etc/hosts.equiv` functionality.

NOTE The `opc_op` password should be consistent for all managed nodes.

For example, if *$HOME* is the home directory on the managed node, the *$HOME*/`.rhosts` entry of the executing user would look like the following:

```
<management_server> opc_op
```

In this example, *<management_server>* is the name of the machine hosting the HPOM management server. The name can be short of fully qualified depending on the configuration of your network.

Passwords Assignment on Windows Managed Nodes

On Microsoft Windows managed nodes, you can assign the password for the HPOM account during installation of the agent software. If you do not assign a password for the HPOM account, a default password is created. However, a password is not assigned by default.

Configuration Distribution

The command `opctmpldwn` provides a way of bypassing the standard mechanism for HPOM policy distribution and allowing you to download and encrypt HPOM policies and configuration data on the management server and then copy the downloaded file to the target location on the managed nodes. Only assigned policies are downloaded (for example, logfile, SNMP trap, `opcmsg`, threshold monitor, scheduled action, event correlation, and flexible management).

The downloaded files are encrypted either with the default key of the managed node or with keys generated specifically for the node.

Refer to the *opctmpldwn(1M)* reference page for more information about command options and parameters.

Automatic and Operator-Initiated Actions

Action requests and action responses can contain sensitive information (for example, application password, application responses, and so on) that might be of interest to intruders. In a secure system, this is not problem. However, if the requests and responses containing sensitive data have to pass through a firewall or over the Internet, where packets may be routed through many unknown gateways and networks, then you should take measures required to improve security.

Shell Scripts

In addition, automatic actions and operator-initiated actions are normally executed as root. To prevent security holes, it is essential that you protect any shell scripts (for example, those used to switch users) by assigning minimal rights and choose carefully the commands which an application uses.

User Switch for HPOM HTTPS Agents

To further increase security, you can switch the user for HPOM HTTPS agents from user root to a specified user account or group by using the `ovswitchuser.sh` command.

For more information about command options and parameters, refer to the *ovswitchuser(1M)* reference page.

Remote Actions

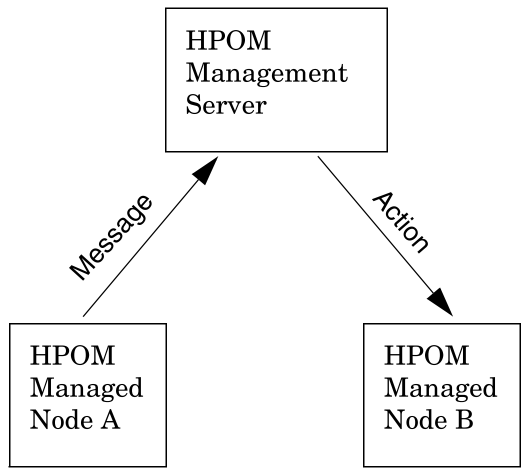
Remote actions are automatic or operator-initiated actions executed on a managed node that is controlled by HPOM but is not the originator of the message that triggered the action. The execution of such actions can be controlled with the following file:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml`.

Refer to the *HPOM HTTPS Agent Concepts and Configuration Guide* for more information.

For example, Figure 10-1 shows how managed node A sends a message to the HP Operations management server which then executes the action on managed node B.

Figure 10-1 Example of Remote Actions



Who Needs to Protect Remote Actions

HPOM offers a variety of security mechanisms that prevent the misuse of remote actions. These security measures are especially important for companies that manage systems from more than one customer with one HP Operations management server. Remote actions designed for the managed nodes of one customer may not be executed on the managed nodes of another. Some of these security mechanisms are active by default. Others must be enabled manually.

Security Mechanisms for Remote Actions

To prevent the interception and misuse of remote actions, HPOM offers the following security mechanisms:

- ❑ Assignment of configuration files:

All HPOM configuration files on the managed nodes must belong to a trusted user. By default, this trusted user is the super user. You can change the trusted user (that is, the account under which the HPOM agents run) to another user. For more information about command options and parameters, refer to the reference page *opcswitchuser(1M)*.

- Encryption of message-source templates:

  By default, HPOM message source policies that are assigned and installed on a managed node are encrypted. Encryption protects message source policies from unwanted modifications and misuse.

- Prevention of remote actions:

  If necessary, you can entirely disable remote actions for *all* managed nodes.

  A remote action is defined as an automatic action or operator-initiated action which is defined within an HPOM message sent by Managed Node A and configured to run on Managed Node B. The execution of such actions can be controlled with the file

  `/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml`

- Detection of faked IP addresses or secret keys:

  If you have installed the HPOM Advanced Network Security (ANS) extension, you can also check for mismatched sender addresses by using the command-line tool `ovconfchg` on the HP Operations management server:

  ```
  # ovconfchg -ovrg <OV_resource_group> -ns opc -set \
  OPC_CHK_SENDER_ADDR_MISMATCH TRUE
  ```

  Where *<OV_resource_group>* is the name of the management server resource group.

  This check reinforces `OPC_DISABLE_REMOTE_ACTIONS TRUE` by detecting any attempts to use faked IP addresses or secret keys that were generated by another node.

  If the check detects a mismatch between IP address and host name, all actions that are to be executed on a node other than the message originator are removed from the message. Only local actions that were already started on the message originator are not removed. Failed action requests are documented in annotations, which are added to the message automatically.

Queue Files

The opcmsg and opcmon commands use the queue files for the message interceptor (msgiq) and the monitor agent (monagtq) to communicate with their corresponding processes. The queue files grant read/write permission to all users. You can read sensitive messages by displaying these queue files as a regular user.

CAUTION The opcmsg and opcmon commands allow any user to send a message triggering an automatic action, even on another node.

HPOM Audits

HPOM auditing is based on a series of entries, written by running programs when certain actions take place. These actions can be triggered either by internal processes, or by a user in one of the following ways:

- By using the Java GUI
- By running a command line utility (CLI)
- By using the administrator's GUI (CVPL)

Audit entries contain information indicating what kind of action took place, who performed it, when, and the audit area it concerns. Each entry has a default severity level, depending on the kind of action. The severity level can be `MINOR` , `MAJOR`, `SERIOUS`, or `INTERNAL` (the highest severity level).

NOTE When upgrading from HPOM 8.xx to HPOM 9.0x, all previous audit information is lost. To create a copy of audit data, use the `opcauddwn` command-line utility. For more information about command options and parameters, refer to the *opcauddwn (1M)* reference page.

Audit Levels

As an administrator, you can enable or disable the audit system. If the audit system is disabled, nothing is logged. When the audit system is enabled, you can choose the audit level (`OFF` , `MINIMAL`, `ADVANCED`, or `FULL`).

NOTE The audit level `OFF` is not the same as disabling auditing. To disable auditing, use the `opcsrvconfig -audit -disable` command.

The HPOM Audit System

To enable or disable the audit system in HPOM, use the `opcsrvconfig` command line utility as follows:

- ❏ To enable the audit system, run the following command:

  `#` **`opcsrvconfig -audit -enable`** ***`<level>`***

- ❏ To disable the audit system, run the following command:

  `#` **`opcsrvconfig -audit -disable`**

For more information about the parameters and options you can use with the `opcsrvconfig` command, refer to the *opcsrvconfig (1M)* reference page.

The HP Operations management server checks the severity of the information written to the audit logfile. Depending on the chosen audit level, entries with the specified severity are written to the `audit.opc.txt` file. For example:

`OFF`	Logs only entries with the severity `INTERNAL`
`MINIMAL`	Logs only entries with the severity `INTERNAL` and `SERIOUS`.
`ADVANCED`	Logs only entries with the severity `INTERNAL`, `SERIOUS`, and `MAJOR`.
`FULL`	Logs all entries.

Audit Entry Severity

Like the audit level, the severity level of a certain action can be customized. Each action has an XPL variable assigned. To set a custom value for this variable, run the following command:

`#` **`ovconfchg -ns audit -set`** ***`<var> <sev_level>`***

Where *`<var>`* is the name of the variable, and *`<sev_level>`* is `MINOR`, `MAJOR`, `SERIOUS`, or `INTERNAL`.

For example:

`#` **`ovconfchg -ns audit -set OM_CFG_ADD_USER MAJOR`**

To list currently set variables, run the following command:

`#` **`opcsrvconfig -audit -list_custom`**

For more information about command options and parameters, refer to the *ovconfchg (1M)* and *opcsrvconfig (1M)* reference pages.

For more information about variables, see “HPOM Audits” on page 499.

Audit Entry Format

All audit entries are written to the /var/opt/OV/log/audit.opc.txt file as the audit entry with the format illustrated in Example 10-1 on page 398.

Example 10-1 Audit Log-File Syntax

```
Time:<Time>|Sev:<Severity>|Area:<Area>|Action:<Action>|ID:
(undefined)|Source:OMU|OS User:<User>|App
User:<User>|Text:<Text>[;<Param Type>:<Param Value>
[;<Param 2 Type>:<Param 2 Value>...]]
```

The following list describes the various parameters and variables illustrated in Example 10-1 on page 398:

<Time>	Time when the audit entry was logged.
<Severity>	HPOM severity level (MINOR, MAJOR, SERIOUS or INTERNAL).
<Area>	HPOM element or action on which the audit entry is based (Nodes, Policies, Server configuration, and so on).
<Action>	One of the following actions: Read, Write, Execute, Start, Stop, or Login / Logout.
<Source>	OMU
<OS User>	User who started the action logged in the audit log file.
<App User>	opc_adm, opc_op, or the HPOM user who created the action. If not known, N/A or Admin (N/A) is shown.
<Text>	Text describing the action that caused that entry in the audit log file.

Audit Areas

The following list provides a complete overview of all the areas covered in an HPOM audit:

- ❏ Functional:
  - Audit:
    - — Startup
    - — Shutdown

- Config

- Authorization:
    - Login
    - Logout
    - HPOM user
    - HPOM user profile
    - HPOM certificate actions
- HPOM objects:
    - HPOM message
    - HPOM node
    - HPOM application
    - External application
    - HPOM configuration
    - Other HPOM objects
- HPOM database:
    - Read
    - Write

❏ HPOM database:

- Read
- Write

❏ HPOM file access:

- HPOM script/binary access:
    - Read
    - Write
    - Execute
- HPOM configuration file access:
    - Read
    - Write

    — Execute

- ❏ HPOM processes:
    - Startup
    - Shutdown

HPOM GUI Startup Messages

According to the National Institute of Standards and Technology (NIST) 800-37 standard, usage and criticality of any application should be acknowledged before its startup, as well as allowance for its usage. Acknowledgement is achieved with a warning message that is displayed before the application starts.

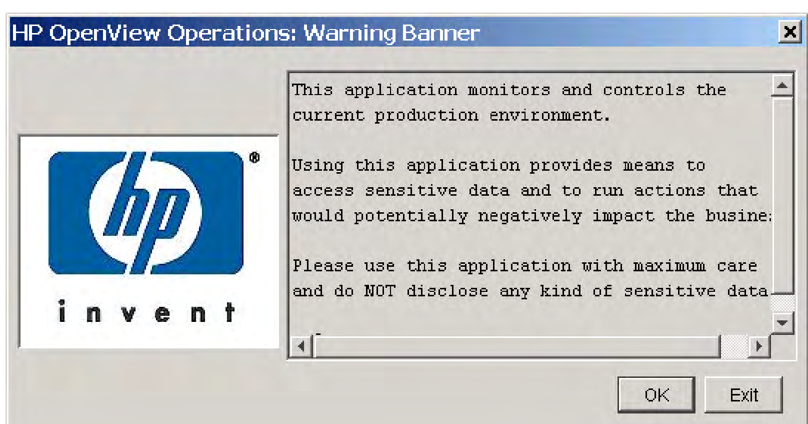
By default, the HPOM GUI startup message does *not* exist. You can create it by writing your own text in a text editor and storing the message in the database. You can also set and change its status (enabled or disabled). See “Creating an HPOM GUI Startup Message” on page 402 for details.

The HPOM GUI startup message displays, if enabled, after the Login window. If the agreement defined in this message is accepted, HPOM starts. Otherwise, the login sequence is stopped immediately.

If the HPOM GUI startup message is disabled, HPOM starts right after the Login window.

Figure 10-2 shows an example of the HPOM GUI startup message.

Figure 10-2 Example of the HPOM GUI Startup Message



HPOM GUI Startup Message

Before you create the HPOM GUI startup message, consider the following points:

❏ Customization:

The startup message is defined and enabled after the HPOM installation.

You must be user `root` to customize, edit, or change the status of the HPOM GUI startup message.

❏ Database storage:

The startup message is stored in the `opc_mgmtsv_config` table in the attribute `ovou_license_text`. Refer to the *HPOM Reporting and Database Schema* for details about the database tables.

Creating an HPOM GUI Startup Message

To create the HPOM GUI startup message, perform the following steps:

1. Write your own message in a text editor and save it.

   The length of the message must *not* exceed 2048 single-byte characters or 1024 multi-byte characters.

   To ensure that the startup message is displayed correctly in the startup message window, make sure you respect the line fields in the text editor while composing the message.

2. Use the `opcuistartupmsg` command line tool to store the customized startup message in the database and to enable it:

   ```
   # opcuistartupmsg -f <filename> -e
   ```

   For more information about the `opcuistartupmsg` tool, refer to the *opcuistartupmsg(1M)* reference page.

To display the current startup message and its status, use `opcuistartupmsg` or `opcuistartupmsg -s`.

11 HPOM Maintenance

In this Chapter

This chapter contains information for administrators who are responsible for maintaining HPOM, maintaining the HPOM databases, and who might need to change the hostname and IP address of the management server and managed nodes.

The information in this chapter includes the following topics:

❑ HPOM management server:

  Maintaining the HPOM management server includes the following high-level tasks:

  - “Configuration Data Download” on page 405
  - “Data Backup on the Management Server” on page 406
  - “Database Maintenance” on page 421
  - “HP Software Platform” on page 424
  - “HPOM Directories and Files” on page 425

❑ HPOM managed node:

  Maintaining the managed nodes includes the following high-level tasks:

  - “Managed Node Directories Containing Runtime Data” on page 428
  - “Location of Local Logfiles” on page 428

❑ Licensing and infrastructure:

  In addition, this chapter contains information about the following important tasks:

  - “HPOM Licenses” on page 430
  - “Hostnames and IP Addresses” on page 437

Configuration Data Download

You should download configuration data as part of your standard maintenance or backup routine. Before you make any significant changes to your HPOM configuration, make sure you download configuration data to the file system or use backup tools to back up your configuration data. For more information about backing up configuration data, see "Data Backup on the Management Server" on page 406.

You can download configuration data by using the `opccfgdwn(1M)` command. The configuration-download utility enables you to select the parts of the configuration that you want to download and save the data to flat files in the file system. For example, instead of downloading the entire configuration, you may choose to download only message-source policies. You specify the different parts of the configuration that you want to download in the `download.dsf` file, which you can find in the following location:

```
/var/opt/OV/share/tmp/OpC_appl/cfgdwn/download.dsf
```

Note that the `download.dsf` file is required as a parameter by the `opccfgdwn(1M)` command. For more information about the parameters and options you can use to control the `opccfgdwn(1M)` command, refer to the *opccfgdwn(1M)* reference page.

Data Backup on the Management Server

HPOM provides two methods for backing up data on the HP Operations management server:

- Offline backup:

  Use the `opcbackup_offline` utility to perform partial or full backups of data on the management server. For more information, see "Offline Backups" on page 406.

- Online backup:

  Use the `opcbackup_online` utility to perform a complete automatic backup of the database while the HPOM GUI and server processes are running. For more information, see "Online Backups" on page 409.

HPOM stores configuration data on the management server and on the managed nodes. If the restored configuration on the management server does not match the current configuration on a managed node, errors relating to missing instructions or incorrectly assigned policies may occur. After you have restored a backup, you should redistribute the policies as well as the action, command and monitor scripts to all managed nodes by using the `-force` option of `opcragt`.

When recovering data, use the recover tool corresponding to the backup tool originally used to back up the data. For example, use `opcrestore_offline` to restore data backed up with `opcbackup_offline`, and use `opcrestore_online` to recover data backed up with `opbackup_`online.

Oracle uses the archive-log mode to save data automatically and periodically. Changes to data files are stored in redo log files. These redo log files are subsequently archived. For more information about archive log mode and redo log files, refer to the Oracle documentation. To find out how to set up archive log mode in HPOM, see "Backup Prerequisites" on page 412.

Offline Backups

To help you perform a backup of installation and configuration data on the HPOM management server, HPOM provides the following scripts:

- `opcbackup_offline`:

  For more information about backing up HPOM data offline, see “opcbackup_offline Command” on page 408.

- `opcrestore_offline:`

  For more information about restoring HPOM data from an offline backup, see “opcrestore_offline Command” on page 408.

You can use the offline backup and restore tools to perform the following type of operations on the management server:

- Partial backup/restore:

  HPOM configuration data only. Includes current messages and history messages.

- Full backup/restore:

  Includes the HPOM binaries and installation defaults.

In either case, you have to shut down the Java GUI and stop all HPOM process and services.

Backing up data offline has the following advantages:

- Archive log mode:

  Offline backups do not require or make use of the archive log mode, which Oracle uses to save data automatically and periodically. Not using archive log mode increases overall backup performance and requires less disk space for the backup image.

- Backup mode:

  If you use the full backup mode, the HPOM binaries are included in the backup image.

Backing up data offline has the following disadvantages:

- Data recovery:

  You can recover data only to the state of the most recent full backup. In some cases, it is possible to recover part of the changes done in the database after the backup, but this is not granted.

- HPOM process and services:

  Before you start an offline backup, you must stop all HP services and the Java GUI.

For more information about the HPOM utilities that are available to help you perform *offline* backup and restore operations, refer to the reference pages *opcbackup_offline(1M)* and *opcrestore_offline(1M)*.

opcbackup_offline Command

You can use the `opcbackup_offline` command to create a backup of the whole HPOM system including the data, or just the configuration files. During the backup procedure the HPOM server and the database have to be stopped.

This command accepts the following command-line options:

`opcbackup_offline [-c] [-d] [-n] [-v] [-s] [-r]`

`-c` If selected, only the configuration data is backed up. If no option is selected, a full backup is done.

`-d` Use this option to add specified folders to the backup.

`-s` This option specifies connection strings to the database on which the remote manager (RMAN) will perform the backup.

The format of the string is as follows:

`user/password@`*<server>*`/dbname`

If not specified, the current HPOM database instance is used.

`-r` Use this option to specify the location where the remote manager (RMAN) will store the backup of the database. It is preferred that the folder is new and empty.

`-n` No interaction with the command.

`-v` Verbose mode.

For more information about the parameters and options available with the offline-backup utilities, refer to the *opcbackup_offline(1M)* and *opcrestore_offline(1M)* reference pages respectively.

opcrestore_offline Command

By using the `opcrestore_offline` command line tool, restoring the database is simple. You should just perform the following command:

`#` **`/opt/OV/bin/OpC/opcrestore_offline`**

For more information about command options and parameters, refer to the *opcrestore_offline(1M)* reference page.

Online Backups

To help you perform a complete automatic backup of the database while the HPOM GUI and server processes are running, HPOM provides the following scripts:

❏ `opcbackup_online`:

For more information about backing up HPOM data online, see "opcbackup_online Command" on page 410.

❏ `opcrestore_online:`

For more information about restoring HPOM data from an online backup, see "opcrestore_online Command" on page 411.

You can manage the online backups using cron jobs or through scheduled HPOM actions.

Online backups have the following advantages:

❏ HPOM GUI:

There is no need to exit the HPOM GUI, although OVW actions are not possible for a short time.

❏ Processes and services:

HPOM server processes, HPOM Operator Web GUI services, trouble ticket services, and notification services remain fully operational.

❏ Database:

Partial recovery of the Oracle database is possible.

For example, you could recover the Oracle database as follows:

- All data backed up to a given time.
- Only individual damaged tablespaces.

Online backups have the following disadvantages:

❏ Archive log mode:

Oracle archive log mode must be enabled:

- Reduces overall performance.
- Requires more disk space.

❏ Binaries:

No binaries are backed up.

For more information about the HPOM utilities that are available to help you perform *online* backup and restore operations, refer to the reference pages *opcbackup_online(1M)* and *opcrestore_online(1M)*.

opcbackup_online Command

The `opcbackup_online` command enables you to perform a backup of installation and configuration data while the HPOM database is online. You do not have to stop the database to perform an online backup. The following list describes the parameters and options you can use with the `opcbackup_online` command:

`opcbackup_online [-c] [-r] [-s] [-v]`

`-c` Connection string to the database on which the remote manager (RMAN) will perform the backup. The format of the string is as follows:

`#` **`user/password@`*`<server>`*`/dbname`**

If no connection string is specified, the current HPOM database instance is used.

`-r` Location where the remote manager (RMAN) will store the database backup files. It is preferred that the folder is new and empty.

`-s` Location of the HPOM data backup folder.

`-v` Verbose mode.

NOTE The `opcbackup_online` command stores progress information in the following file:

`/var/opt/OV/tmp/ovbackup.log`.

opcrestore_online Command

The opcrestore_online command restores a backup created with opcbackup_online.

The opcrestore_online command allows you to restore the complete Oracle database or corrupted files. You can restore the database either to the state of the backup or to the most recent state.

TIP

Before running opcrestore_online, make sure that /opt/OV/bin is included in your PATH.

Before starting, opcrestore_online verifies that no HP Software or integrated processes are running.

This command accepts the following command-line options:

```
opcrestore_online [-c] [-s] [(-b |-l)] [-v]
```

-c	Connection string to the database on which the remote manager (RMAN) will perform the backup.
-s	Folder where HPOM backup files are stored.
-l	Restore the latest recoverable state of the database.
-b	Restore the data until the time of the most recent backup.
-v	Verbose mode.

NOTE

The opcrestore_online command stores progress information in the same file as the online-backup command, opcbackup_online, namely:

/var/opt/OV/tmp/ovbackup.log.

Temporary Files in Online Backups

Temporary files (for example, queue files) are excluded from online backups. When a backup starts, the HPOM GUI pops up a notification window and some HPOM maps remain blocked for the duration of the backup. If a task cannot be completed before the backup starts, the task remains idle until the backup operation completes. After the backup completes, the suspended task resumes.

Archive Log Mode in Oracle

The scripts provided by HPOM for automated backups use the online backup method from Oracle, which requires the database run in archive log mode. The Oracle archive log mode is not the default setting for the Oracle database; you must configure archive log mode manually.

In archive log mode, Oracle stores any changes to data files between full backups in numbered redo log files. The redo log files are used in the event of a shut down to restore a configuration from the most recent, full backup. For details, see Oracle's product documentation.

For more information about enabling archive log mode, see "Backup Prerequisites" on page 412.

Backup Notification Tools

The command-line utility `opcwall(1)` enables you to notify all running HPOM GUIs of an imminent automated backup.

You can use the following parameters and options with the `opcwall` command:

`opcwall {-user <user_name>} <Message Text>`

`-user`	Single user to whom you want to send a message. If not specified, all operators receive the message.
`<user_name>`	Name of the operator you want to receive the message.
`<Message Text>`	Text of the message you want the operator to see.

Backup Prerequisites

Before performing either online or offline backups, note the following prerequisites. Before you start, it is recommended to create a pair of folders with all rights included. Backup scripts for both types of backup (online and offline) are at the following location: `/opt/OV/bin/OpC`.

If you want to perform *online* backups, use the following commands:

- ❑ opcbackup_online
- ❑ opcrestore_online

If you want to perform offline backups, use the following commands:

- ❑ opcbackup_offline
- ❑ opcrestore_offline

Backing Up and Restoring Data

To create either online or offline backups, perform the following procedure, which is the same for both types of backup:

1. Configure the remote database password for SYSTEM user.

   The remote database password is configured during the HPOM installation, but if for some reason the /etc/opt/OV/share/conf/OpC/mgmt_sv/.opcdbrem.sec file is not there you have to created it manually by using the following commands:

   ```
   # RMAN_PASSWD=manager
   # export RMAN_PASSWD
   # /opt/OV/bin/OpC/opcdbpwd -rpr
   # unset RMAN_PASSWD
   ```

2. Set the database in ARCHIVELOG mode for online backup (for offline backup it is optional).

   ```
   # su - oracle
   $ sqlplus /nolog
   SQL> conn / as sysdba
   SQL> shutdown immediate
   SQL> startup mount
   SQL> alter database archivelog;
   SQL> alter database open;
   ```

   For checking if the database is set, use:

   ```
   SQL> archive log list;
   SQL> exit
   ```

3. Grant permissions to SYSTEM user to use the remote manager, RMAN:

Note that the action described in this step occurs automatically if the following is true:

- Database has been created by HPOM (not manually) and it is not a remote database.
- You replied affirmatively to the question `Configure the database for remote login?` during setup of the HPOM database.

To grant `SYSTEM` user access to the remote manager, `RMAN`, peform the following steps:

```
# su - oracle
$ sqlplus /nolog
SQL> conn / as sysdba
SQL> alter system set \
remote_login_passwordfile=exclusive scope=spfile;
SQL> shutdown immediate
SQL> startup
SQL> exit
```

```
$ orapwd file=<ORACLE_HOME>/dbs/\
  orapw<ORACLE_SID> password=<SYSTEM_password>
```

For example:

```
$ orapwd file=/opt/oracle/product/11.1.0/dbs/\
orapwopenview password=manager
```

```
$ sqlplus /nolog
```

```
SQL> conn / as sysdba
Connected.
```

```
SQL> grant SYSDBA to SYSTEM;
Grant succeeded.
```

Check the permissions for the `SYSTEM` user:

```
SQL> select * from v$pwfile_users;

USERNAME                       SYSDB SYSOP

------------------------------ ----- -----

SYS                            TRUE  TRUE

SYSTEM                         TRUE  FALSE

SQL> exit
```

NOTE When running this command, you can safely ignore the error `OPW-00005: File with same name exists - please delete or rename`, which occasionally occurs.

4. Write down the Oracle database ID (DBID).

   The DBID is a code that identifies an Oracle database. In some catastrophic events, some manual steps may be required to recover the database, and knowing this code is important in these cases. To retrieve this code, run the following command:

   ```
   # su - oracle
   $ sqlplus /nolog
   SQL> conn / as sysdba
   SQL> select dbid from v$database
   ```

NOTE The RMAN version must be compatible with the Oracle server.

Recovering Data after an Automatic Backup

Automatic backup scripts only make a backup of configuration data and dynamic data. If binaries or static configuration files are lost, you have to recover them before restoring the database.

You can recover binaries or static configuration files in one of the following ways:

- ❑ Restore a full offline backup:

  Restore a full offline backup of the complete system, that was taken with `opcbackup_offline` with the `full` option.

- ❑ Reinstall HPOM:

NOTE When recovering binaries or static configuration files, choose this way as the last option since reinstalling server packages may cause the loss of custom configuration data.

To reinstall all packages that are installed during the server installation, perform as follows:

1. Stop all server components:

   ```
   # /opt/OV/bin/ovc -kill
   ```

2. Reinstall all packages by running the following command:

   ```
   # /opt/OV/bin/OpC/install/ovoinstall -force \
   -skip_setup_check \
   -pkgdir <package_repository_location>
   ```

   Where *<package_repository_location>* is the location where all server packages are located.

IMPORTANT If the server is already configured, *do not* continue with the configuration.

3. Start all server components:

   ```
   # /opt/OV/bin/ovc -start
   ```

Restoring a Database to the State of Its Latest Backup

Restoring the HPOM database to its state at the time of the last backup only requires the data contained in the backup. However, restoring the database in this way leaves Oracle in an inconsistent state, because the *latest* state of the database is not restored. In addition, Oracle log numbers are reset in the control files and in the online redo logs.

NOTE After successfully completing this kind of restore, you will need to create a new backup.

Restoring a Database to its Latest State

Restoring the database to the last known state is more complicated than restoring the database to its state at the time of the last backup. Restoring the database to its last known state requires not only the data contained in the backup but also data on the system itself, namely: online redo logs and archive logs written since the last backup.

NOTE Restoring a database to its *last* know state can introduce inconsistencies between the configuration files (restored to the state of the backup) and the data in the database (restored to the last known state between the last backup and the time the restore operation starts).

Before you attempt to recover a database to its last known state, make sure you perform the following checks:

1. Check the control files:

   All control files must exist. Normally, control files are mirrored and backed up. If one of the control file still exists, it can be copied from one location to the other. Control files can also be extracted from the backup. However, this should be done by an Oracle database administrator (DBA). Note that scripts can only restore to the latest state if *all* control files exist.

2. Check the redo log files:

   All online redo log files must exist. Online redo log files are backed up and can be mirrored. If one of the online redo log files in a log group still exists, it can be copied to the other locations. This should be done by an Oracle DBA. Note that scripts can only restore to the latest state if *all* redo log files exist.

3. Check the Oracle log number:

   Oracle log numbers are reset in the control files and in the online redo logs during a backup. The Oracle log number must not have been reset since the backup.

4. Check the archived redo logs:

   All archived redo logs made since the backup must still exist and be available.

5. Check the status of HPOM Users:

   No HPOM users should have been modified since the backup, which modifies files in the file system.

6. Check the event correlation (ECS) Policies:

   No ECS policies should have been added since the backup.

Removing HPOM Queue Files

HPOM queue files are neither backed up with the automated backup scripts nor deleted during the restore. In addition, the messages in the queue files at the time of the backup are *not* in the database and are processed only when the HPOM processes are next restarted.

If corrupt queue files prevent the server processes from being started, remove the queue files.

To remove the queue files, follow these steps:

1. Stop all HP Operations server processes:

   `# `**`/opt/OV/bin/OpC/opcsv -stop`**

2. Remove a selected temporary file or all temporary files:

   `# `**`rm -f /var/opt/OV/share/tmp/OpC/mgmt_sv/*`**

3. Restart the HP Operations server processes:

   `# `**`/opt/OV/bin/OpC/opcsv -start`**

Manual Recovery of the HPOM Database

In some cases, the database is damaged in such a way that it cannot be automatically recovered by HPOM scripts. These cases may also include either a loss of one or more `controlfile` copies or `SPFILE`. However, HPOM backup scripts keep separate copies of these files in the database backup folders. For example:

❏ `OPENVIEW_DBID`**`2654967530`**`_22-04-09_10.29_ctrl_6_684844242_1`

  for `controlfile`

❏ `OPENVIEW_DBID`**`2654967530`**`_22-04-09_10.29_cfg_5_684844240_1`

  for `spfile`

An additional copy of `controlfile` exists. It is kept by Oracle in its autobackup location, which is by default `$ORACLE_HOME/dbs`:

`OPENVIEW_c-`**`2654967530`**`-20090422-01_ctrlautobackup`

The files at these locations are exact copies of the missing files and can be used with `RMAN` to recover the database.

Make sure that you consider the following before performing a manual recovery of the HPOM database:

- The listener process must be up and running. Otherwise `RMAN` cannot connect to the instance.
- In certain cases `DBID` of the database may be needed. This ID code must be written down during the backup preparation steps by running the following query:

  ```
  SQL> select dbid from v$database;
  ```

NOTE `DBID` is also part of the file names in the database backup folders.

- If the Oracle instance has not been shut down yet, shut it down before making an attempt to recover it:

  ```
  # su - oracle
  $ sqlplus system/<password>@<ov_net> as sysdba
  SQL> shutdown abort
  SQL> exit
  ```

To start the manual recovery procedure, enter the following command:

```
# su - oracle
(export ORACLE_HOME / ORACLE_SID)
$ rman target system/<password>@<ov_net>
RMAN> SET DBID <DBID>
RMAN> startup nomount
```

The Oracle database instance should be running at this point, after which you can try to recover the damaged file or the damaged files:

- If the `SPFILE` is damaged, enter:

  ```
  RMAN> restore SPFILE from
  '<full path of the 'cfg' file in the backup folder>';
  ```

NOTE If `SPFILE` is not damaged and you run the above command, the RMAN-06564 error appears, which can be safely ignored. You can append `to '<PATH>'` at the end of the above command to create a copy of `SPFILE` at another location.

- If `controlfile` is damaged, enter:

```
RMAN> restore controlfile from
'<full path of the 'ctrl' file in the backup folder>';
```

If you fail to recover the damaged `controlfile` by running the above command, Oracle can attempt to recover it from an autobackup copy made over the course of the last year (the maximum time allowed). Enter the following command:

```
RMAN> restore controlfile from autobackup maxdays 366;
```

After these files have been successfully recovered, enter the following:

```
RMAN> startup mount
RMAN> restore database;
RMAN> recover database;
RMAN> alter database open resetlogs;
RMAN> exit
```

The database should be up and running at this point. It is recommended to make a new backup after you have checked that everything is in order.

NOTE

If you want to run any HPOM restore script after manually restoring the database, use the option for restoring until the latest possible time. On `opcrestore_online`, this can be done by using the `-l` option. If you use `opcrestore_offline`, you will be prompted during the restore procedure.

Database Maintenance

To ensure that your HPOM database runs efficiently, you should perform the following tasks periodically:

❏ History message browser:

  If a very large number of messages have been produced (for example, by an inappropriately configured policy), operators may find that their `Message Browser` takes a long time to open. In this case, as user root, use the command-line utilities `opcack` or `opcackmsg` to acknowledge these messages and move them to the history database. For details, refer to the *opcack(1m)* and *opcackmsg(1m)* reference pages.

❏ History messages:

  Download history messages by using the `opchistdwn` command line tool. To restore previously backed up history messages, refer to the *opchistupl(1m)* or *opcaudupl(1m)* reference page, and *opchistdwn (1M)* reference page for downloading history messages.

❏ HPOM configuration:

  Back up the HPOM configuration regularly. For details, see "Data Backup on the Management Server" on page 406.

❏ Disk space:

  The HPOM database files automatically consume the extra disk space required to cope with any growth in the backup image. If a disk runs out of space, you can use other disks to add additional files for a tablespace. For details, refer to the Oracle product information.

❏ Audit files:

  Every time a user runs the command `connect internal`, Oracle adds an audit file to the directory *$ORACLE_HOME*`/rdbms/audit`. Because the monitor policy `mondbfile` runs the `connect internal` command roughly every ten minute, you should review the files in this directory regularly and, if necessary, remove them.

Database Configuration on Multiple Disks

Although using the Oracle archive log mode helps to reduce the loss of data after backing up and restoring a database, Oracle offers additional ways to avoid data loss in the unlikely event that a disk fails.

If you can access more than one disk, you should review the following configuration tips. Use the information provided when implementing similar scenarios in your own HPOM environment.

Moving Oracle Control Files to a Second Disk

To move one or more Oracle control files to the second disk, perform the following steps:

1. Create the directories on the second disk:

   `# mkdir -p /u02/oradata/om`

   `# chown oracle:dba /u02/oradata/om`

2. Shut down the database.

3. Move selected control files to a directory on the second disk, for example, from disk `/u01` to disk `/u02`:

   ```
   # mv /u01/oradata/om/control03.ctl \
   /u02/oradata/om/control03.ctl
   ```

4. Modify the control file names in the following file:

   `$ORACLE_HOME/dbs/init${ORACLE_SID}.ora`

   Example of *old* control file names:

   ```
   control_files = (/u01/oradata/om/control01.ctl,
                    /u01/oradata/om/control02.ctl,
                    /u01/oradata/om/control03.ctl)
   ```

   Example of *new* control file names:

   ```
   control_files = (/u01/oradata/om/control01.ctl,
                    /u01/oradata/om/control02.ctl,
                    /u02/oradata/om/control03.ctl)
   ```

5. Restart the database.

Creating a Set of Mirrored Online Redo Logs

You can create a second (or even third) set of mirrored, online redo logs on the second (or even a third) disk. HPOM installs Oracle in such a way that, by default, it has three redo log groups, each containing one member.

The following procedure shows how to create a second set of redo log files in the directory. `/u02/oradata/om`. Modify the directory names (and repeat the steps) as required.

To create a second set of redo logfiles, perform the following steps:

1. Create the directories on the second disk.

   Example:

   ```
   # mkdir -p /u02/oradata/om
   ```

   ```
   # chown oracle:dba /u02/oradata/om
   ```

2. As user `oracle`, enter the following:

   ```
   # sqlplus /nolog

   SQL>connect / as sysdba

   alter database add logfile member
   '/u02/oradata/om/redo01.log' to group 1;

   alter database add logfile member
   '/u02/oradata/om/redo02.log' to group 2;

   alter database add logfile member
   '/u02/oradata/om/redo03.log' to group 3;

   exit
   ```

HP Software Platform

To maintain the HP Software platform, periodically verify that the trap daemon logfile, `trapd.log`, has not grown too large. A large trap daemon logoff can reduce the performance of HPOM.

A backup file of `trapd.log` is also provided in the following location:

`/var/opt/OV/log/trapd.log.old`

If you no longer need the entries logged in the `trapd.log` file, erase the logfile, which you can find in the following location:

`/var/opt/OV/log/trapd.log`

For details about system maintenance in HP NNM, see *Managing Your Network with HP Network Node Manager*.

HPOM Directories and Files

To maintain HPOM directories and files, follow these guidelines:

❏ Management server directory:

Important runtime data is contained in the directory `/var/opt/OV/share/tmp/OpC/mgmt_sv`. Do not clean up this directory unless you are unable to use another solution or there are too many unprocessed and old messages.

❏ Software installation file:

If you no longer need the information appended to logfiles during software installation, update, and removal, you should backup and then erase the following logfile:

`/var/opt/OV/log/OpC/mgmt_sv/install.log`.

The `inst_err.log` and `inst_sum.log` logfiles do not continuously grow because they are generated for each HPOM software installation, update, or removal.

❏ Error logfile:

You should back up and then erase the HPOM error and warning logfile and its backups (for HTTPS-based managed nodes):

— Plain text:

`/var/opt/OV/log/System.txt`

— Binary:

`/var/opt/OV/log/System.bin`

HPOM uses an automatic backup logfile mechanism having up to ten files. To save disk space, if the `System.txt` logfile size is greater than 1 MB, HPOM automatically performs the following clean-up actions:

- Moves `System.txt.008` to `System.txt.009`
- Moves `System.txt.007` to `System.txt.008`
- Moves `System.txt.006` to `System.txt.007`
- Moves `System.txt.005` to `System.txt.006`
- Moves `System.txt.004` to `System.txt.005`

- Moves `System.txt.003` to `System.txt.004`
- Moves `System.txt.002` to `System.txt.003`
- Moves `System.txt.001` to `System.txt.002`
- Moves `System.txt` to `System.txt.001`

HPOM Managed Nodes

On the managed nodes, you should periodically back up, and then erase, local HPOM logfiles (and their backups). HPOM uses 90% of the specified log directory size for local message logging, and 10% for error and warning logging. HPOM also uses an automatic backup mechanism for the logfiles (four on UNIX and Solaris).

For example, the configured size of a UNIX log directory is 10 MB. The size of a UNIX log directory is allocated in the following way:

- ❏ Message logging:

  HPOM allocates 9 MB for local message logging. Given that there are four logfiles, if the `opcmsglg` file size is greater than 2.25 MB, HPOM does the following:

  - Moves `opcmsgl2` to `opcmsgl3`
  - Moves `opcmsgl1` to `opcmsgl2`
  - Moves `opcmsglg` to `opcmsgl1`

- ❏ Error and warning message logging:

  HPOM allocates 1 MB for local error and warning message logging. If the `System.txt` (on HTTPS-based managed nodes) file size is greater than 1 MB, HPOM does the following:

  - Moves `System.txt.008` to `System.txt.009`
  - Moves `System.txt.007` to `System.txt.008`
  - Moves `System.txt.006` to `System.txt.007`
  - Moves `System.txt.005` to `System.txt.006`
  - Moves `System.txt.004` to `System.txt.005`
  - Moves `System.txt.003` to `System.txt.004`
  - Moves `System.txt.002` to `System.txt.003`
  - Moves `System.txt.001` to `System.txt.002`
  - Moves `System.txt` to `System.txt.001`

Managed Node Directories with Runtime Data

Table 11-1 shows the managed node directories that contain important runtime data.

Table 11-1 Managed Node Directories Containing Runtime Data

HPOM	Operating System on the Managed Node	Directories Containing Runtime Data

Management server on:
• HP-UX
• Linux
• Solaris
	AIX	`/var/lpp/OV/tmp/OpC`
		`/var/lpp/OV/tmp/OpC/bin`
		`/var/lpp/OV/tmp/OpC/conf`

	HP-UX 11.x
	Linux
	Solaris
		`/var/opt/OV/tmp/OpC`
		`/var/opt/OV/tmp/OpC/bin`
		`/var/opt/OV/tmp/OpC/conf`

	Windows	`\usr\OV\tmp\OpC\<node>`
		`\usr\OV\tmp\OpC\bin\intel`
		`\usr\OV\tmp\OpC\conf\<node>`

Unless there is *no* alternative, or if there are too many unprocessed and old messages, *do not* clean up these directories.

Location of Local Logfiles

Table 11-2 shows where local logfiles reside on HP-UX 10.x or 11.x and Windows HTTPS-based managed nodes.

Table 11-2 Local Logfiles on HP-UX 10.x/11.x and Windows HTTPS-based Managed Nodes

Logfile	Windows	HP-UX 10.x and 11.x
Default logfile path	`\Program Files\HP \` `OpenView\data\log`	`/var/opt/OV/log`
HPOM errors and warnings	`System.txt` `System.txt.(001-003)`	`System.txt` `System.txt.(001-003)`
HPOM messages	`opcmsglg,` `opcmsgl(1-3)`	`opcmsglg` `opcmsgl(1-3)`

Table 11-3 shows where local logfiles reside on AIX HTTPS-based managed nodes.

Table 11-3 **Local Logfiles on AIX HTTPS-based Managed Nodes**

Logfile	AIX
Default logfile path	`/var/opt/OV/log/`
HPOM errors/warnings	`System.txt`
HPOM messages	`System.txt`

Table 11-4 shows where local logfiles reside on other UNIX managed nodes.

Table 11-4 **Local Logfiles on Other UNIX HTTPS-based Managed Nodes**

Logfile	Linux and Solaris
Default logfile path	`/var/opt/OV/log/System.txt`
HPOM errors/warnings	`System.txt System.txt.(001-003)`
HPOM messages	`opcmsglg`, `opcmsg (1-3)`

HPOM Licenses

HP Operations Manager uses the HPOM licensing component to manage licenses and check them for licensed objects.

Licence Configuration

There are two prerequisites for the HPOM licensing component to function properly: `mailx` and configuration parameters.

mailx Utility

The UNIX utility program `mailx` must be correctly configured to ensure that the HPOM licensing component can send license status messages to the license administrator. The availability of `mailx` has no effect on the functionality of HP Operations Manager but enables it to send license notification messages.

Licence-Configuration Parameters

The HPOM licensing component uses configuration parameters which are stored under the file name `opr.el` in the `server` resource group. These parameters must be adapted to the requirements of the user.

`LicenseAdminEmailAddress`	E-mail address of the person responsible for HPOM license management or the person monitoring the HPOM license status. The initial setting is root@<local_long_hostname>.
`SwitchOffWarning`	Toggle warning messages on or off when the number of licenses for a licensed product component reaches the defined level. This can be set to `TRUE` or `FALSE`. `SwitchOffWarning` works in conjunction with the `Severity` configuration parameter. Critical

	license warning messages are always sent, regardless of the configuration settings.
Severity	Severity level that must be reached before an internal HPOM license warning message is sent. This parameter can be set to *Warning* or *Major*. The initial setting is *Warning*.
Content	Level of detail for license reports. The level can be set to *Summarized* or *Detailed*. The default setting is *Summarized*. License reports can be very lengthy when there is a large number of configured nodes. To avoid this, the detail level should be set to *Summarized*.

To Set License-Configuration Parameters

To set the configuration parameters, Use the following command:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opr.el \
   -set LicenseAdminEmailAddress license_admin@company.com \
   -set SwitchOffWarning FALSE \
   -set Severity Major \
   -set Content Summarized
```

License Reports

The `ovolicense` tool allows you to generate a license report which shows you which licenses are needed, how many are installed, how many are in use, how many are available and for how long they are valid.

`ovolicense` Tool

The `ovolicense` tool is the central tool for the management of the HPOM licenses and the generation of license reports. The `ovolicense` tool adds, enables, or disables license passwords, checks the license status and generates the license report.

Synopsis

```
ovolicense
   -h|-help
   -m|-mappings
   -i|-install -a|-category <category> [-f|-file <pwd_file>]
   -q|-request -a|-category <category>
   -s|-status -p|-product <product>
   -g|-gui -a|-category <category>
   -e|-email -p|-product <product> <report_options>
   -r|-report -p|-product <product> <report_options>
```

Report options

```
[-xml|-text] [-detailed] [-out <file>] [-quiet]
```

Unless otherwise specified, the report will be generated in summarized text form. Reporting options allow you to change the report format and content, as follows:

`-xml`

Creates a license report in XML format (instead of the default text format) intended for further processing.

Target Connector history data is part of the XML report.

`-detailed`

A detailed license report contains additional information on all configured nodes. This can make the report very lengthy, depending on the number of configured nodes.

Options

Note that some `ovolicense` functions use Java, and `JAVA_HOME` must be set to a valid runtime value. GUI features require Java and an X11 display. You can use the following options with the `ovolicense` command:

`ovolicense -help`

Displays a list of available options for the `ovolicense` command.

`ovolicense -mappings`

Shows which product components are registered for licensing and to which category they belong.

`ovolicense -install -category HPOM [-file <`*`password_file`*`>]`

Allows the installation of new license passwords. All license passwords in the specified file will be installed. If no file is specified, a GUI window asks you to specify the license password file and enables you to select a subset of passwords within the file.

`ovolicense -request -category HPOM`

Opens a GUI window allowing you to request and install license passwords belonging to an order number.

`ovolicense -gui -category HPOM`

Opens the GUI without any specific functionality selected.

`ovolicense -status -product HP Operations Manager`

Reports the license status of all registered license components for a product. For HP Operations Manager, the product is always `HP Operations Manager`.

`ovolicense -email -product HPOM [<`*`report_options`*`>]`

Generates a license report on the basis of the report options and sends it to the e-mail address specified in the `LicenseAdminEmailAddress` configuration parameter.

`ovolicense -report -product HPOM [<`*`report_options`*`>]`

Generates a license report on the basis of the report options and prints it in the terminal.

Example License Report

Figure 9-1 shows an HPOM license report, which displays details for all licensed HPOM components. The heading of the report displays information about the HP Operations Manager version and patch level. The body of the report shows the number of installed, used and available licenses for each installed HPOM component. The final part of the report shows an overview of the configuration parameters.

License reports comprise the following sections:

- ❏ Agent count:

  License type used to count and summarize the licenses. It is not part of the HPOM product and does not represent an installed license. The Agent Count in the example report displayed in Figure 11-1 on page 435 shows that there is an insufficient number of installed HPOM agent licenses.

- ❏ HP Operations management server:

  Status of the HP Operations management server license, for example: `OK`.

- ❏ HP Operations Manager tier agent:

  Status of the HP Operations agent license. The number of Used Licenses for Desktop Agent and Tier 0 Agent to Tier 4 Agent is always 0 (zero) because the agent tier cannot be detected and the agent license requirement cannot be assigned to the correct license type. Use Agent Count to count and summarize license status.

- ❏ Number of unpatched nodes:

  Number of nodes that are not using up-to-date HPOM agent software (HPOM 8.17 or higher). Licenses required for the node will only be reported by the HPOM agent software if it is up-to-date.

- ❏ Number of unreachable nodes:

  Number of nodes that sent license and node details but have not refreshed their data for 14 days.

Figure 11-1 License Report

```
HP Operations Manager License status report of Tue Jan 20 17:22:00 2009
=========================================================================

HP Operations Manager Server Information:
=========================================
Product Name         : HP Operations Manager for Unix
Version              : 09.00.000
Patch Level          : 09.00.000
Management server    : omuserver
Total of mgd nodes : 86

HP Operations Manager License Summary:
======================================

Agent Count
----------------------------------------------------------
  Installed Licenses       : 62
  Used Licenses            : 86
  Available Licenses       : -24

  ==========================================================
  CRITICAL: 24 'Agent Count' licenses are missing.
  Please acquire at least 24 'Agent Count' licenses.
  ==========================================================

HP Operations Manager Target Connector
----------------------------------------------------------
  Installed Licenses       : 1
  Used Licenses            : 0
  Available Licenses       : 1

HP Operations Manager Server
----------------------------------------------------------
  Installed Licenses       : 1
  Used Licenses            : 1
  Available Licenses       : 0

HP Operations Manager Tier 0 Agent
----------------------------------------------------------
  Installed Licenses       : 10
  Used Licenses            : 0
  Available Licenses       : 10

  Number of unpatched nodes    : 17
  Number of unreachable nodes : 1

Configuration Parameters:
=========================

  License Manager Mail Address : license_admin@company.com
  License Report Content       : Summarized
  License Warning Severity     : Major
  Disable License Warnings     : FALSE
```

Unregistered Components

A report can display a licensed object that is not registered for licensing, as shown in Figure 11-2 on page 436.

Figure 11-2 License Report - Unregistered Component

```
* Not Registered: 'noregspi'
-------------------------------------------------------------
  Installed Licenses      : 0
  Used Licenses           : 10
  Available Licenses      : -10

  ================================================================
  CRITICAL: 10 licenses with the plugin ID 'noregspi'
  are used by one or more nodes, but the according component
  is either not installed or is corrupt.
  Please install the missing component and make sure that
  a sufficient number of licenses is installed.
  ================================================================
```

Figure 11-3 on page 436 shows how the report displays node details, for example, when a configuration from one HP Operations management server is uploaded onto a different HPOM server which does not have the same components or SPIs installed. The report shows that the first management server has license requirements that are different to the requirements on the second management server.

Figure 11-3 License Report - Unregistered Component

```
Not Registered: noregspi: 4
```

To overcome this problem, the components or SPIs listed as unregistered must either be installed on all servers sharing a configuration or removed from the HPOM nodes whose configuration is shared by the servers.

Hostnames and IP Addresses

Hostnames work within IP networks to identify a managed node. While a node may have many IP addresses, the hostname is used to pinpoint a specific node. The system hostname is the string returned when you use the UNIX `hostname(1)` command.

It is not uncommon for a node to have more than one IP address. If a node becomes a member of another subnet, you may need to change its IP addresses. In this case, the IP address or fully qualified domain name may change.

NOTE For HTTPS-based nodes, you can also specify the IP address as dynamic. You can do this by using the `opcnode` command line tool.

In general, on HP-UX and Solaris systems, the IP address and the related hostname are configured in one of the following ways:

- ❏ An entry in the file `/etc/hosts`
- ❏ Domain Name Service (DNS)
- ❏ Network Information Service (NIS on HP-UX, NIS+ on Solaris)

HPOM also configures the hostname and IP address of the management server for the managed node in the management server database.

If you are moving from a non-name-server environment to a name-server environment (DNS or BIND), make sure the name server can access the new IP address.

To change the hostname or IP address of managed nodes, use the `opc_node_change.pl` command line tool on the management server. See "opc_node_change.pl" on page 438 for more information about this tool.

opc_node_change.pl

Use the tool `/opt/OV/bin/OpC/utils/opc_node_change.pl` on the HP Operations management server to change the hostname or IP address of managed nodes.

Synopsis

```
opc_node_change.pl [-h[elp]]
   -oldname <old_FQDN>
   -oldaddr <old_IP_addr>
   -newname <new_FQDN>
   -newaddr <new_IP_addr>[,<new_IP_addr>,...]
   [-nnmupdate -netmask <999.999.999.999>
   -macaddr <XX:XX:XX:XX:XX:XX> [-hook <cmdname>]
   [-nnmtopofix]]
```

Description

Before changing the IP address or hostname of one or more managed nodes in the HPOM database, `opc_node_change.pl` verifies that the new IP address and hostname can be resolved on the management server and that they are not already used by other managed nodes. The tool also verifies that all management server processes including the database processes are running. On the managed node, `opc_node_change.pl` ensures that the new IP address is configured with the HPOM agent software. If the hostname has changed, all currently assigned policies are redistributed. If required, HP Network Node Manager (NNM) is also updated.

Options

`opc_node_change.pl` has the following options:

`-oldname` <*new_FQDN*>

Current fully qualified domain name (*FQDN*) of the managed node.

`-oldaddr` <*old_IP_addr*>

Current IP address (*IP_addr*) of the managed node.

`-newname` <*new_FQDN*>

New fully qualified domain name of the managed node.

`-newaddr` <*new_IP_addr*>

New IP address of the managed node. If the node has multiple IP addresses, specify all of them separated by commas.

`-nnmupdate`

Update information for NNM specified with the `-netmask` option and the network adapter or MAC address of the managed node.

`-netmask` <*999.999.999.999*>

Specifies the network mask of the managed node.

`-macaddr` <*XX:XX:XX:XX:XX:XX*>

The network adapter or MAC address of the managed node in hexadecimal notation.

`-hook` <*cmdname*>

The network adapter or MAC address of the managed node as returned by a callback command-line tool. The command line tool will get the <*new_FQDN*> and <*new_IP_addr*> as parameters. It *must* exit with exit status 0 and pass the MAC address by printing the string `MAC=XX:XX:XX:XX:XX:XX` to standard output. One example of such a command line tool is `opcgetmacaddr.sh` which can be found in the `/opt/OV/contrib/OpC` directory on the management server.

`-nnmtopofix`

Troubleshooting information regarding problems with hostname and IP address changes. Note that this option can sometimes take a while to complete and consume system resources.

Changing the Hostname or IP Address of the Management Server

To change the hostname or IP address of the management server, follow these steps:

1. Request and install new licenses from the HP Password Delivery Service.

   For more information about HPOM licensing, refer to the *HPOM Concepts Guide*.

2. Stop *all* HPOM processes on your management server.

   Stop the manager, agent, and Java GUI processes running on the system:

   a. Stop *all* running Java GUIs.

   b. Stop the HPOM management-server processes with the following command:

      `# /opt/OV/bin/OpC/opcsv -stop`

   c. Stop the HPOM agents on your management server with the following command:

      `# /opt/OV/bin/ovc -kill`

   d. Verify that no HPOM processes are running by using the following command:

      `# ps -eaf | grep opc`

      `# ps -eaf | grep ovc`

   e. If an HPOM process is still running, kill it manually using the following command:

      `# kill <proc_id>`

      After you run this command, all HPOM intelligent agents on HPOM managed nodes start buffering their messages.

3. Make sure the database is running.

   a. Verify that the database is running using the following command:

      `# ps -ef | grep ora`

b. If the database is not running, start it using the following command:

```
# /sbin/init.d/ovoracle start
```

For more information about the Oracle database, refer to the *HPOM Installation Guide for the Management Server*.

4. Change the IP address or node name of the HP Operations management server in the HPOM database using the `opc_node_change.pl` command.

   The command `opc_node_change.pl` provides the following options:

```
# /opt/OV/bin/OpC/utils/opc_node_change.pl \
-oldname <old_FQDN> -oldaddr <old_IP_addr> \
-newname <new_FQDN> -newaddr <new_IP_addr>
```

`-oldname`	Current fully qualified domain name of the management server
`-oldaddr`	Current IP address of the management server
`-newname`	New fully qualified domain name of the management server
`-newaddr`	New IP address of the management server

   For information about other parameters you can use with the `opc_node_change.pl` command, see “opc_node_change.pl” on page 438.

5. Shut down the database with the following command:

```
# /sbin/init.d/ovoracle stop
```

6. Modify the HP Operations management server configuration.

   Update the HP Operations management server configuration using the following command:

```
# /opt/OV/bin/ovconfchg -ovrg server -ns opc \
-set OPC_MGMT_SERVER <new_FQDN>
```

NOTE The command also updates any other customized settings on the management server, such as `bbc.cb.ports:PORTS`.

7. Update the local agent configuration on the management server, as follows:

   a. Specify the new hostname of the management server in the security name space:

   ```
   # /opt/OV/bin/ovconfchg -ns sec.core.auth \
   -set MANAGER <new_FQDN>
   ```

   b. If the certificate server is located on the same system as the management server, update the `CERTIFICATE_SERVER` variable:

   ```
   # /opt/OV/bin/ovconfchg -ns sec.cm.client \
   -set CERTIFICATE_SERVER <new_FQDN>
   ```

8. Deploy the modified node configuration to the agent on the management server by running the `opcsw` command locally on the HPOM management server, as follows:

   ```
   # opcsw -get_nodeinfo
   ```

   The command writes a temporary file that is read by the distribution agent (for example, when the agent starts or restarts) and creates the appropriate `nodeinfo` file.

   For more information about the `opcsw` command, refer to the *opcsw(1m)* reference page.

9. Update the database files.

   a. Edit the following files and replace any occurrence of the old hostname with the new one:

   ```
   /opt/oracle/product/<version>/network/admin/listener.ora
   /opt/oracle/product/<version>/network/admin/sqlnet.ora
   /opt/oracle/product/<version>/network/admin/tnsnames.ora
   /opt/oracle/product/<version>/network/admin/tnsnav.ora
   ```

   b. If the directory `/var/opt/oracle/scls_scr/`*`<old_hostname>`* exists, rename it to `/var/opt/oracle/scls_scr/`*`<new_hostname>`*.

10. Reconfigure the HP Operations management server system with the new hostname or IP address and restart the system.

    a. Change the hostname or IP address:

       - HP-UX:

Run the special initialization script `/sbin/set_parms`. For more information about available parameters and options, refer to the *set_parms(1M)* reference page.

For details, refer to the *HP-UX System Manager's Guide*.

- Linux:

  Run the network configuration tool `system-config-network`. For more information, refer to the RHEL documentation.

- Sun Solaris:

  Run the `/usr/sbin/sys-unconfig` command. For more details, refer to the reference page *sys-unconfig(1M)*.

  If you are moving from an environment that does *not* provide a name resolution service to one that *does*, make sure the name server has the new hostname or IP address available.

b. Restart the system for your changes to take effect.

Reconfiguring the Management Server after a Hostname Change

To reconfigure the management server after changing its either its hostname or IP address, perform the following steps:

1. Stop the HPOM management server.

   To stop the HPOM management server, enter the following:

   `# ` **`/opt/OV/bin/OpC/opcsv -stop`**

2. Make sure the database is running.

   If the database is not running, start it with the following command:

   `# ` **`/sbin/init.d/ovoracle start`**

   For more information about the Oracle database, refer to the *HPOM Installation Guide for the Management Server*.

3. Start the HPOM processes:

   Start the server and agent processes on the HPOM management server, as follows:

a. To start the HPOM management-server processes, enter the following command on the management server:

```
# /opt/OV/bin/OpC/opcsv -start
```

b. To start the HPOM agent processes on the management server, enter the following command on the management server:

```
# /opt/OV/bin/ovc -start
```

NOTE When you restart the agent processes, the agent starts forwarding the messages it buffered while the processes were stopped.

4. Log in to the Java GUI.

   Enter the following:

   ```
   # /opt/OV/bin/OpC/ito_op
   ```

5. Verify policy assignments to the renamed node.

   Verify that all policies are still assigned to the new node.

6. Redistribute all event-correlation policies, if you have changed the hostname of the HPOM management server.

   To redistribute all event-correlation policies assigned to the management server, use the `opcragt` command with the `-dist(ribute)` parameter, as follows:

   ```
   # # opcragt -dist -force "$MGMTSV"
   ```

   The string `$MGMTSV` is the hostname of the management server.

7. Inform all managed nodes of the new hostname of the HPOM management server.

   To instruct managed nodes to use the new host name for the HPOM management server, perform the following steps on *all* HTTPS-based managed nodes that are configured in the node bank and which are running an HPOM agent:

   a. Stop all HPOM agent processes on the managed nodes, enter:

   ```
   # /opt/OV/bin/ovc -kill
   ```

b. Specify the new hostname of the management server in the security name space (`sec.core.auth`) by using the `ovconfchg` command as follows:

```
# /opt/OV/bin/ovconfchg -ns sec.core.auth \
-set MANAGER <new_FQDN>
```

c. If the certificate server is located on the same system as the management server (which now has a new host name), you must also update the `CERTIFICATE_SERVER` variable by using the `ovconfchg` command as follows:

```
# /opt/OV/bin/ovconfchg -ns sec.cm.client \
-set CERTIFICATE_SERVER \
<new_FullyQualifiedDomainName>
```

d. Restart all HPOM agent processes by using the following command:

```
# /opt/OV/bin/ovc -start
```

8. Change the primary management server.

   If the modified HP Operations management server is configured as a primary manager for some managed nodes, update those managed nodes by running the following command from the modified HP Operations management server:

```
# /opt/OV/bin/OpC/opcragt -primmgr [-all | \
[-nodegrp <group>…] <node>…]
```

9. Verify and redistribute the policies.

   Verify that the policies are still assigned to the managed nodes. Then redistribute the policies.

10. Update configuration in flexible-management environments, as follows:.

    - Hostname and IP address:

      Make sure that your hostname and IP address changes are reflected in all configurations and policies across the entire flexible-management environment.

      To find out how to set up, modify, or distribute the policies in a flexible-management environment, refer to the *opcmom(4)* reference page.

- Message forwarding:

  If you have set up message forwarding between HPOM management servers, modify the hostname and IP address manually on all management servers that have the changed system in their node bank.

  You must also check the message forwarding policy on the management servers for any occurrence of the old hostname or IP address.

  Modify all files in the following directory:

  `/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/`

  Modify the message-forwarding policy on the HPOM management servers, as needed.

Changing the Hostname or IP Address of an HTTPS Managed Node

Perform the following steps to change the hostname or IP address of an HTTPS-based managed node:

1. Before changing the hostname or IP address of a managed node, consider the following points:

   - Flexible-management environment:

     If you are running HPOM in a distributed management server (flexible-management) environment, make sure that you perform all steps described in this procedure on *all* management server systems that control or monitor the modified node.

   - DHCP:

     It is possible to set the IP address of the managed node to dynamic by using the `opcnode` command line interface. This allows you to perform your HPOM managed node IP address change in a safer and a more comfortable way.

- Service Navigator:

  If you are using Service Navigator, check the service configuration files. If the service configuration file contains hostnames and IP addresses, they may need to be changed before you run `opcservice` again. For more information, refer to the *Service Navigator Concepts and Configuration Guide*.

- Saved filter settings:

  Message browsers allow you to save the filter settings, such as `For the Following Symbols and Objects`. When you, for example, change the hostname of a managed node, remember to also change the saved filter to the new hostname so that the messages from the node continue to be displayed after the hostname change.

2. Reconfigure the HPOM managed node system with the new hostname or IP address and restart the system.

   On the managed node, change the hostname or IP address of the system as described in the documentation supplied with the operating system. Then restart the system for your changes to take effect.

3. Change the node name or IP address of the managed node in the HPOM database.

   To update the HPOM database with the new hostname for the managed node, run the `opc_node_change.pl` script on the management server, as follows:

   ```
   # opc_node_change.pl -oldname <old_FQDN> \
   -oldaddr <old_IP_addr> -newname <new_FQDN> \
   -newaddr <new_IP_addr> [,<new_IP_addr>,...]
   ```

`-oldname`	Current fully qualified domain name of the HPOM management server
`-oldaddr`	Current IP address of the management server
`-newname`	New fully qualified domain name of the management server
`-newaddr`	New IP address of the management server

   For more information about this command line tool, see “opc_node_change.pl” on page 438.

4. Deploy the modified node configuration to the agent on the management server by running the `opcsw` command locally on the HPOM management server, as follows:

   `# `**`opcsw -get_nodeinfo`** ***<node_name>***

   The command writes a temporary file that is read by the distribution agent (for example, when the agent restarts) and creates the appropriate `nodeinfo` file.

   For more information about the `opcsw` command, see the *opcsw(1m)* reference page.

Hostnames and IP Addresses in a Cluster Environment

Hostnames work within IP networks to identify a managed node. Although a node can have many IP addresses, the hostname is used to identify a specific node. The system hostname is the string returned when you use the UNIX `hostname(1)` command.

It is not uncommon for a node in a cluster environment to have more than one IP address. If a node becomes a member of another subnet, you may need to change its IP addresses. In this case, the IP address or fully qualified domain name may change.

NOTE For the HTTPS-based nodes, you can also specify the IP address as dynamic. You can do this by using the `opcnode` command line tool.

In general, on HP-UX and Solaris systems, the IP address and the related hostname are configured in one of the following ways:

- `/etc/hosts`
- Domain Name Service (DNS)
- Network Information Service (NIS on HP-UX, NIS+ on Solaris)

HPOM also configures the hostname and IP address of the management server for the managed node in the management server database.

If you are moving from a non-name-server environment to a name-server environment (DNS or BIND), make sure the name server knows about the new IP address.

Changing the Virtual Hostname or IP Address of the Management Server

To change the virtual hostname or IP address of the management server, perform these steps on the cluster node where the HP Operations management server is running:

1. Request and install new licenses from the HP Password Delivery Service.

   For more information about HPOM licensing, refer to the *HPOM Concepts Guide*.

2. Disable monitoring for the HP Operations management server.

   To disable monitoring, enter the following command:

   `# /opt/OV/lbin/ovharg -monitor <om_HARG> disable`

   <om_HARG> Name of the high-availability resource group that includes the HPOM management server for which you want to disable monitoring. The default name for the resource group is `ov-server`.

3. Stop *all* HPOM processes on your management server.

   Stop the manager, agent, and Java GUI processes running on the system:

   a. Stop *all* running Java GUIs.

   b. Stop the HPOM manager processes by entering:

      `# /opt/OV/bin/OpC/opcsv -stop`

   c. Stop the HPOM agents on your management server by entering:

      `# /opt/OV/bin/ovc -kill`

   d. Verify that no HPOM processes are running by entering:

      `# ps -eaf | grep opc`

      `# ps -eaf | grep ovc`

   e. If an HPOM process is still running, kill it manually by entering:

      `# kill <proc_id>`

      All HPOM agents on HPOM managed nodes start buffering their messages.

4. Make sure the database is running.

   If the database is not running, start it by entering:

   ```
   # /sbin/init.d/ovoracle start force
   ```

   For more information about the Oracle database, refer to the *HPOM Installation Guide for the Management Server*.

5. Change the IP address or node name of the HP Operations management server in the HPOM database.

   Use the following command to change the IP address or node name of the HP Operations management server:

   ```
   # /opt/OV/bin/OpC/utils/opc_node_change.pl \
   -oldname <old_FQDN> -oldaddr <old_IP_addr> \
   -newname <old_FQDN> -newaddr <new_IP_addr>
   ```

   See “opc_node_change.pl” on page 438 for more information about this tool.

6. Shut down the database.

   Enter the following:

   ```
   # /sbin/init.d/ovoracle stop force
   ```

7. Modify the HP Operations management server configuration.

   To change the hostname, perform the following steps:

   a. Specify the new hostname of the management server in the security name space:

      ```
      # ovconfchg -ns sec.core.auth -set MANAGER <new_FQDN>
      ```

   b. Update the HP Operations management-server configuration, enter the following:

      ```
      # ovconfchg -ovrg server -ns opc -set OPC_MGMT_SERVER\
      <new_FQDN>
      ```

      <new_FQDN> Fully qualified name of the system hosting the HPOM management server.

   c. If the certificate server is located on the same system as the management server, update the `CERTIFICATE_SERVER` variable by entering the following command:

      ```
      # ovconfchg -ovrg server -ns sec.cm.client -set \
      CERTIFICATE_SERVER <new_FQDN>
      ```

d. Specify the bind address for the server port, enter:

```
# ovconfchg -ovrg server -ns bbc.cb -set \
SERVER_BIND_ADDR <new_IP_addr>
```

8. Update the database files.

   On *each* cluster node replace the hostname with the new one:

```
/opt/oracle/product/<version>/network/admin/listener.ora
/opt/oracle/product/<version>/network/admin/sqlnet.ora
/opt/oracle/product/<version>/network/admin/tnsnames.ora
/opt/oracle/product/<version>/network/admin/tnsnav.ora
/etc/opt/OV/conf/ov.conf.ha
```

9. Start HPOM integrated services, using the following command:

```
# /opt/OV/bin/ovc -start
```

10. Set the new high-availability cluster configuration by performing the following steps:

   a. Stop the HPOM-server high-availability resource group by using the `ovharg_config` command with the `-stop` option, as follows:

```
# /opt/OV/bin/ovharg_config <om_HARG> -stop
<node_name>
```

   <om_HARG> Name of the high-availability resource group that includes the HPOM management server for which you want to disable monitoring. The default name for the resource group is `ov-server`.

   b. Change the cluster configuration to use the new IP address.

   For HP Serviceguard:

   Replace the entry `IP[0]=<old_IP_addr>` with `IP[0]=<new_IP_addr>` in the follow file on *all* cluster nodes.

```
/etc/cmcluster/ov-server/ov-server.cntl
```

   c. Start the HPOM-server high-availability resource group as follows:

```
# /opt/OV/bin/ovharg_config <om_HARG> -start \
<node_name>
```

Reconfiguring the Management Server after a Virtual Hostname Change

To reconfigure the management server after changing its virtual hostname or IP address in a cluster environment, perform the following steps:

1. Disable monitoring of the high-availability resource group (HARG).

   To disable HARG monitoring, enter the following command:

   `# /opt/OV/lbin/ovharg -monitor ov-server disable`

2. Stop the HPOM management-server processes.

   To stop the HPOM server processes, enter the following command:

   `# /opt/OV/bin/OpC/opcsv -stop`

3. Make sure the database is running.

   If the database is not running, start it with the following command:

   `# /sbin/init.d/ovoracle start`

   For information about managing the Oracle database, refer to the *HPOM Installation Guide for the Management Server*.

4. Start HP Software.

   To start HP Software including all integrated services (such as HPOM), use the `opcsv` command as follows:

   `# /opt/OV/bin/OpC/opcsv -start`

5. Enable monitoring of the high-availability resource group (HARG).

   To enable HARG monitoring, enter the following command:

   `# /opt/OV/lbin/ovharg -monitor ov-server enable`

NOTE When you re-enable monitoring for the high-availability resource group, the agent starts forwarding the messages it buffered while the HA resource group was offline.

6. Log in to the Java GUI.

To start the Java GUI and log in to HPOM, enter the following command:

```
# /opt/OV/bin/OpC/ito_op
```

7. Verify HPOM policy assignments.

   Verify that the policies are still assigned to the new node.

8. Reassign and redistribute all event-correlation policies.

   If you have changed the name of the virtual host on which the HPOM management server runs, reassign and redistribute all event-correlation policies assigned to the management server using the `opcragt` command as follows:

   ```
   # opcragt -dist -force "$MGMTSV"
   ```

   The string `$MGMTSV` specifies the name of the host where the HPOM management server is installed.

9. Inform managed nodes about the new (virtual) hostname of the management server.

   To inform managed nodes about a change to the virtual node name of the management server, perform the following steps on HTTPS-based managed nodes that are configured in the node bank and which are running an HPOM agent:

   a. Stop all HPOM agent processes on the managed nodes, enter:

      ```
      # /opt/OV/bin/ovc -kill
      ```

   b. Specify the new (virtual) hostname of the management server in the security name space:

      ```
      # /opt/OV/bin/ovconfchg -ns sec.core.auth \
      -set MANAGER <new_FQDN>
      ```

   c. If the certificate server is located on the same system as the management server, update the `CERTIFICATE_SERVER` variable using the `ovconfchg` command as follows:

      ```
      # /opt/OV/bin/ovconfchg -ns sec.cm.client \
      -set CERTIFICATE_SERVER <new_FQDN>
      ```

   d. Restart all HPOM agent processes by entering:

      ```
      # /opt/OV/bin/ovc -start
      ```

10. Change the primary management server.

If the modified HP Operations management server is configured as a primary manager for some managed nodes, update those managed nodes by running the following command from the modified HP Operations management server:

```
# /opt/OV/bin/OpC/opcragt -primmgr [-all | \
[-nodegrp <group>…] <node>…]
```

11. Verify and redistribute the policies.

    Verify that the policies are still assigned to the managed nodes. Then redistribute the policies.

12. Update the configuration files that define flexible-management environments, as follows:

    a. Make sure that your hostname and IP address changes are reflected in all configurations and policies across the entire flexible-management environment.

       Modify all files in the following directory:

       `/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs/`

       To find out how to setup, modify, or distribute the policies in a flexible-management environment, refer to the reference page *opcmom(4)*.

    b. If you have set up message forwarding between management servers, update any references to the old hostname and IP address on all management servers that include in their node bank the systems whose name or IP address you have changed.

    c. Check the message-forwarding policy on the management servers for occurrences of the old hostname or IP address, for example, in the following files:

       - `/etc/opc/OV/share/conf/OpC/mgmt_sv/respmgrs/msgforw`
       - `/etc/opc/OV/share/conf/OpC/mgmt_sv/respmgrs/escmgr`

       Modify the message-forwarding policy on the management servers, if necessary.

NOTE

Before setting up flexible-management environment, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide* for information about security certificates.

13. Change the hostname or IP address of a managed node.

    If you also want to change the hostname or IP address of a managed node, see “Changing the Hostname or IP Address of an HTTPS Managed Node” on page 446.

Improving HPOM Name Resolution

HPOM message processing may become slow due to slow name resolution. If the name resolution is slow, `opcmsgm` cannot process messages as fast as it normally does.

To improve HPOM name resolution and consequently message processing speed, do the following:

1. Make sure the reverse lookup works well.
2. Make sure unknown hosts and IP addresses resolve in a reasonable time.
3. If DNS works well, use DNS first and then fallback to `/etc/hosts` in `/etc/nsswitch.conf`:

```
hosts:        dns [NOTFOUND=continue] files
```

NOTE

`opcmsgm` processes messages immediately after the server restart even if the name service is slow. This is due to the fact that the IP mapping table is created in a separate thread.

It is also possible to disable the IP mapping table using the `ovconfchg` command as follows:

```
# ovconfchg -ovrg server -ns opc -set
OPC_DISABLE_IP_MAPPING_TABLE TRUE
```

4. Change the number of times HPOM tries to resolve hostnames to 1 (one) by entering the following command:

```
# ovconfchg -ovrg server -ns opc -set OPC_NAMESRV_RETRIES 1
```

5. Cache name service results either by setting up the caching DNS server on the management server or by increasing the size of the HPOM name service cache.

   If you want to increase the size of the HPOM name-server cache, make sure it is large enough to hold the names of all nodes in the node bank and some additional node names, too. For example:

   ```
   # ovconfchg -ovrg server -ns opc -set
   OPC_NAMESRV_CACHE_SIZE 10000
   ```

6. Measure the time it takes to resolve host names and generate a warning if the threshold is exceeded (for example, 200 milliseconds) by entering the following:

   ```
   # ovconfchg -ovrg server -ns opc -set
   OPC_NAMESRV_MAX_TIME 200
   ```

7. Within DNS, define time-outs for resolver functions to limit the time that a name service call takes, if it encounters problems with name-resolution services.

   Defining time-outs for resolver functions differs according to platform, as follows:

   - HP-UX:

     You can modify the following name-resolution settings on HP-UX:

     — `retrans`: retransmission time-out with the default value being 5000 milliseconds

     — `retry`: number of retries with the default value being 4

     On HP-UX systems, you can set the `retrans` and `retry` options in the following ways:

     — System wide: use the file `/etc/resolv.conf`

     To set the time-out to 1 second and retries to 2, add the following lines to `/etc/resolv.conf`:

     ```
     retrans 1000

     retry 2
     ```

— For specific processes: use the RES_RETRY and RES_RETRANS configuration variables

You can set the configuration variables for ovcd (and its children) in the ctrl.env name space, for example:

```
# ovconfchg -ns ctrl.env -set RES_RETRY 2 -set
RES_RETRANS 1000
```

You must restart the HPOM agent to implement the changes because the HPOM server processes are child processes of ovspmd, which is started by ovstart.

If you set RES_RETRAN and RES_RETRY for the management server, restart the management server processes with the new settings, as follows:

```
# ovstop
# export RES_RETRANS=1000
# export RES_RETRY=2
# ovstart
```

To make sure the variables are also set the next time the system is booted, set them before ovstart in the /sbin/init.d/ov500 script.

- Solaris:

  You can modify the following settings on Solaris in the same way as on HP-UX, namely system-wide or for specific processes:

  — retrans: retransmission time-out with the default value being 5 seconds

  — retry: number of retries with the default value being 4

  Syntax requirements meant that, on Solaris, you must set retrans and retry as options in the resolv.conf file. For example,

  ```
  options retrans:1

  options retry:2
  ```

- Linux:

  You can modify the following settings on Red Hat Linux:

— `timeout`: The amount of time (in seconds) the name resolver waits for a response from a remote name server before retrying. The default value is 5 seconds. `timeout` on Linux corresponds to `retrans` on HP-UX.

— `attempts` : the number of times the resolver will send a query to its name servers before giving up and returning an error to the calling application. The default value is 2. `attempts` on Linux corresponds to `retry` on HP-UX.

These settings can be modified system wide in `/etc/resolv.conf`. For example, to set the retransmission time-out to 1 second and retries to 2, add the following line to `/etc/resolv.conf`:

`options timeout:1 attempts:2`

The options keyword of a system `resolv.conf` file can be amended for specific individual processes by setting the environment variable `RES_OPTIONS` to a space-separated list of resolver options, for example:

`export RES_OPTIONS="timeout:1 attempts:2"`

12 HPOM Management Servers in a Cluster Environment

In this Chapter

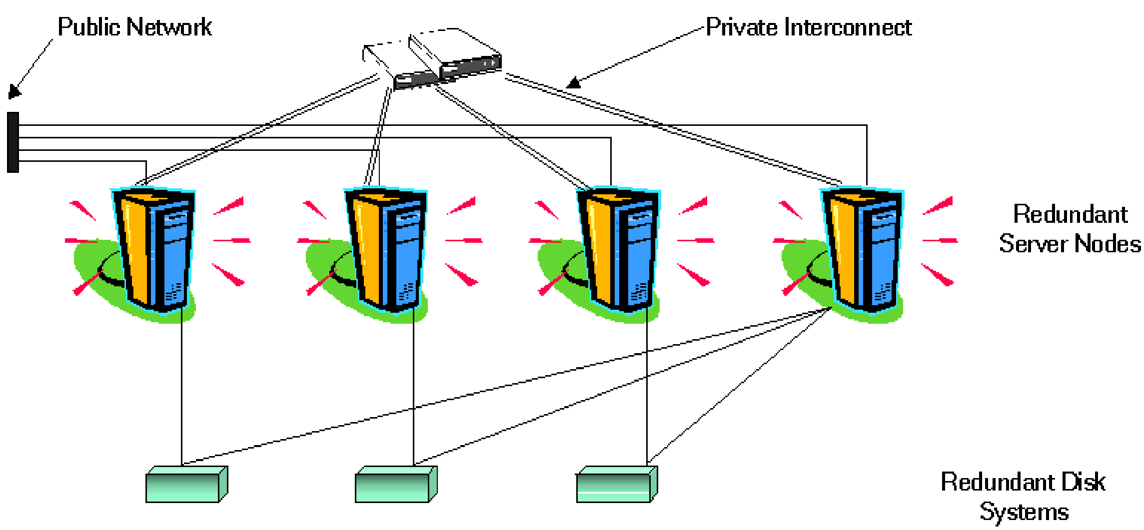
This chapter provides information for system administrators working with HP Operations Manager (HPOM) in a cluster environment. It assumes that you are familiar with the general concepts of HPOM and with high-availability (HA) concepts. The information in this chapter covers the following high-level topics:

For detailed information about installing and configuring the HPOM management server in a high-availability environment, refer to the *HPOM Installation Guide for the Management Server*.

High-Availability Cluster Environments

Cluster architecture provides a single, globally coherent process and resource management view for the multiple nodes of a cluster. Figure 12-1 shows an example of a cluster architecture.

Figure 12-1 Architecture of a High Availability Cluster



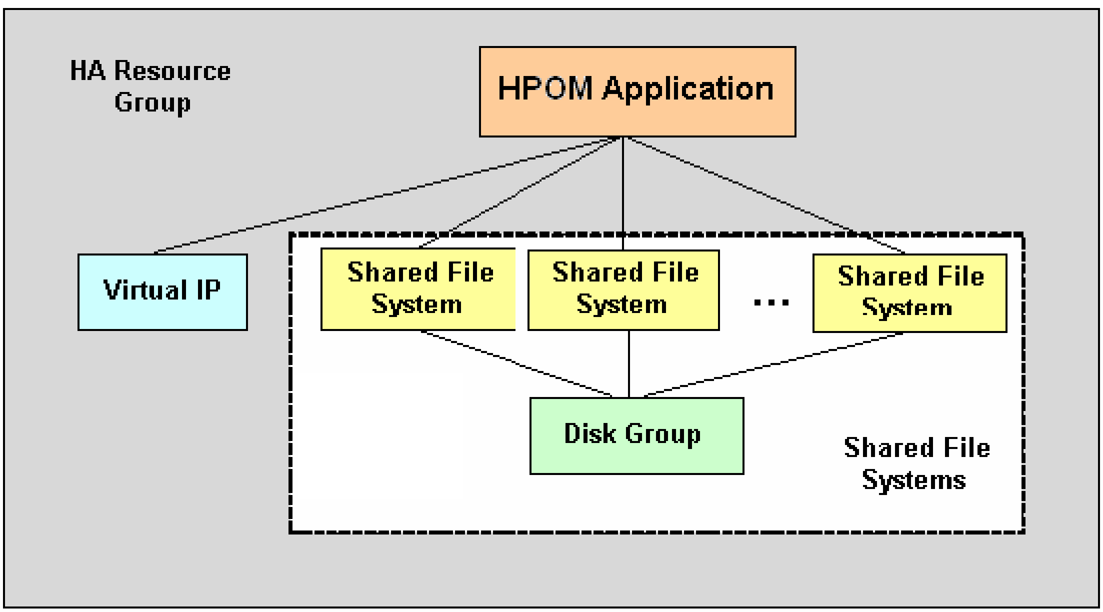
Each node in a cluster is connected to one or more public networks, and to a *private interconnect*, representing a communication channel used for transmitting data between cluster nodes.

Applications running in a cluster environment are configured as high-availability resource groups. A high-availability resource group (HARG) is a generic term for cluster objects representing highly available applications.

HPOM Management Servers in High-Availability Environments

In modern cluster environments such as HP Serviceguard, VERITAS Cluster, Sun Cluster, and so on, applications are represented as compounds of resources—simple operations enabling applications to run in a cluster environment. The resources comprise a **Resource Group**, which represents an application running in a cluster environment.

Figure 12-2 Typical HA Resources Group Layout



The concept of the high-availability resource group is represented differently according to the cluster environment you are talking about. Table 12-1, "Resource Group in High-Availability Cluster Environments," indicates how the resource group is referred to in the different high-availability environments.

Table 12-1 Resource Group in High-Availability Cluster Environments

HA Cluster Environment	Abbreviation	Resource Group Name
HP Serviceguard	HP SG	Package
VERITAS Cluster Server	VCS	Service Group
Sun Cluster	SC	Resource Group
Red Hat Cluster Suite	RH Cluster Suite	Service

Rather than refer to the different, product-specific cluster terms listed in Table 12-1, this document uses the generic term high-availability resource group (HARG) to designate a set of resources in a cluster environment.

High-Availability-Resource-Group Administration

HPOM provides the `ovharg_config` command to enable you to perform the common tasks required for the administration of HPOM management server running in a high-availability resource group. You can use the `ovharg_config` command to start and the HA resource group and switch the resource group between cluster nodes. The information in this section covers the following topics:

- "Checking the High-Availability-Resource-Group Status" on page 466
- "Starting the High-Availability Resource Group" on page 466
- "Stopping the High-Availability Resource Group" on page 467
- "Switching the High-Availability Resource Group" on page 467

Checking the High-Availability-Resource-Group Status

Before starting, stopping, or switching the high-availability resource group, you can check whether the target node is active:

`# /opt/OV/bin/OpC/opcsv -startable`

The `opcsv` command uses the following return codes with the `-startable` parameter:

`0`	Active cluster node is detected
`2`	Inactive cluster node is detected

To avoid starting optional processes whose initial configuration is not complete or requires some additional manual steps, use the `opcsv` command to check process availability, as follows:

`# /opt/OV/bin/OpC/opcsv -available [<process1> <process2> <...>]`

The `opcsv` command uses the following return codes with the `-available` parameter:

`0`	All specified processes are properly configured or no processes were specified
`1`	Not all specified processes are properly configured

Starting the High-Availability Resource Group

To start the high-availability resource group hosting the HPOM management server, use the `ovharg_config` command with the following parameters:

`# /opt/OV/bin/ovharg_config <om_HARG> -start <node_name>`

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to start. The default name for the resource group is `ov-server`.
<node name>	Name of the cluster node on which the high-availability resource group should start.

NOTE By default, the resource group name for the HPOM management server cluster is `ov-server`, but you can also choose an alternative name.

The `ovharg_config` command displays the following return codes:

`0`	HPOM application started successfully.
`1`	Start operation failed.

Stopping the High-Availability Resource Group

To stop the high-availability resource group hosting the HPOM management-server, use the `ovharg_config` command with the following parameters:

`# /opt/OV/bin/ovharg_config <om_HARG> -stop <node_name>`

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to stop. The default name for the resource group is `ov-server`.
<node name>	Name of the cluster node on which the high-availability resource group should stop.

The `ovharg_config` command displays the following return codes:

`0`	HPOM resource group stopped successfully.
`1`	Resource-group stop operation failed.

Switching the High-Availability Resource Group

To switch the high-availability resource group from one cluster node to another, enter:

`# /opt/OV/bin/ovharg_config <om_HARG> -switch <node_name>`

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to switch nodes. The default name for the resource group is `ov-server`.
<node name>	Name of the cluster node that the high-availability resource group should switch to and start.

The `ovharg_config` command displays the following return codes:

`0`	HPOM resource group switched successfully.
`1`	Resource-group switch operation failed.

Manual Management of the HPOM Management Server in Cluster Environments

The HP Operations management server in a cluster environment is represented as an application that is part of the high-availability resource group, containing resources which perform all necessary operations for starting, stopping and monitoring the application.

The `/opt/OV/lbin/ovharg` utility is used for starting, stopping, and monitoring the HP Operations management server running as an application in a cluster environment.

Starting the HPOM Management Server

To start the HP Operations management server manually in a high-availability cluster environment, use the `ovharg` command as follows:

`# ` **`/opt/OV/lbin/ovharg -start <`*`om_HARG`*`>`**

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to start. The default name for the resource group is `ov-server`.

The `ovharg` command displays the following return codes for the `-start` parameter:

`0`	HPOM management server was started successfully.
`1`	Start operation failed.

Stopping the HPOM Management Server

To stop the HP Operations management server manually in a high-availability cluster environment, use the `ovharg` command as follows:

`# ` **`/opt/OV/lbin/ovharg -stop <`*`om_HARG`*`>`**

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to stop. The default name for the resource group is `ov-server`.

The `ovharg` command displays the following return codes for the `-stop` parameter:

`0`	HPOM management server was stopped successfully.

`1`	Stop operation failed.

Monitoring the HPOM Management Server

To configure the cluster manager to monitor the HPOM management server in a high-availability cluster environment, use the `ovharg` command with the `-monitor` parameter, as follows:

`#` **`/opt/OV/lbin/ovharg -monitor <`*`om_HARG`*`>`**

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to monitor. The default name for the resource group is `ov-server`.

The `ovharg` command displays the following return codes for the `-monitor` parameter:

`0`	HPOM management server is running normally
`1`	HPOM management server is not running, which, if it has not already occurred, leads to a switch of the monitored resource group to another node in the high-availability cluster.

Disabling HPOM Management Server Monitoring

There are situations in which you need the HP Operations management server to be stopped, while all other parts of the high-availability resource group should continue to run. In such situations, you will need to disable monitoring manually.

To manually disable monitoring of the HP Operations management server in a high-availability cluster environment, use the `ovharg` command with the `-monitor` parameter and the `disable` option, as follows:

`#` **`/opt/OV/lbin/ovharg -monitor <`*`om_HARG`*`> disable`**

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server for which you want to disable monitoring manually. Note that the default name for the resource group is `ov-server`.

If the monitoring process is disabled, you can stop the HP Operations management server in the knowledge that this will *not* cause the resource group to be switched to another node in the high-availability cluster. If monitoring is disable, the cluster manager does *not* detect the event, because the code returned by the monitor command remains `0`.

NOTE After you have finished the manual HP Operations management server administration, you *must* restart the HP Operations management server.

To check whether the HP Operations management server is running normally, use the `opcsv` command as follows:

`# /opt/OV/bin/OpC/opcsv`

- ❏ If the management server is running, enable monitoring again by using the following command:

  `# /opt/OV/lbin/ovharg -monitor <om_HARG> enable`

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server for which you want to enable monitoring. The default name for the resource group is `ov-server`.

- ❏ If the HP Operations management server is *not* running properly, you have to perform additional manual steps in order to put it in a running state.

In a deployment where the HPOM management server runs in a separate resource group to the Oracle database server, you can temporarily disable monitoring of the Oracle high-availability resource group with the following command:

`# /opt/OV/lbin/ovharg -monitor <ORA_HARG> disable`

<ORA_HARG>	Name of the high-availability resource group hosting the Oracle database server for which you want to disable monitoring. The default name for the resource group is `ov-oracle`.

To enable monitoring of the Oracle high-availability resource group, use the `ovharg` command with the `-monitor` parameter and the `enable` option, as follows:

`# /opt/OV/lbin/ovharg -monitor <ORA_HARG> enable`

Script-Based Oracle-Database Monitor

If the HP Operations management server and the Oracle database server are configured as separate high-availability resource groups, the scripts that monitor the status of the high-availability resource group hosting the HPOM management server can also be used to monitor the status of the high-availability resource group hosting the Oracle database.

If you configure the scripts that monitor the status of the resource group hosting the HPOM management server to monitor the resource group hosting the Oracle database, too, note the information in the following list, which describes how the management-server monitor scripts react in the following ways to the current status of the Oracle high-availability resource group:

❏ Oracle high-availability resource group is not yet running:

  If the HP Operations high-availability resource group is started before the Oracle high-availability resource group is up and running, the HP Operations high-availability resource group scripts do not start the HPOM management server processes.

  As soon as the Oracle high-availability resource group is running, the HPOM management-server processes are started and the command returns `0`.

❏ Oracle high-availability resource group is stopped:

  If the Oracle high-availability resource group is stopped, switched, or experiences a fail over, the HP Operations management server processes are also stopped.

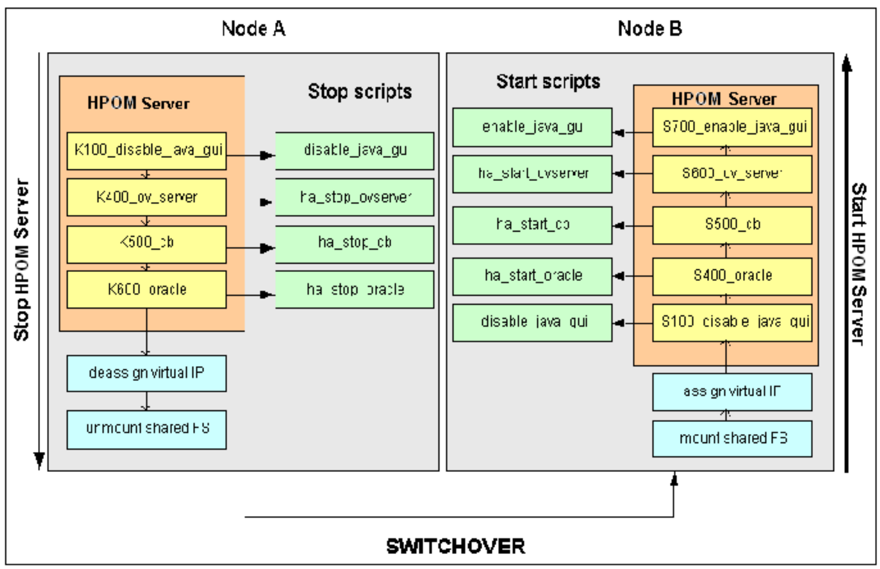
❏ Oracle high-availability resource group is restarted:

  As soon as the Oracle high-availability resource group is running, the HPOM management-server processes are started and the command returns `0`.

HPOM Switchover in High-Availability Clusters

The example illustrated in Figure 12-3 on page 472 shows the switchover procedure in a two node cluster in which the high-availability resource group `ov-server` is currently active on cluster system `Node A`. The cluster initiates switchover from `Node A` to the remaining `Node B`. The Resource Group `ov-server` is stopped on `Node A` and started on `Node B`. The switchower procedure is shown on Figure 12-3.

Figure 12-3 Switchover Procedure



Switchover Process

When a system failure occurs on `Node A`, the cluster initiates switchover of the Resource Group `ov-server` from `Node A`. The Resource Group is stopped on `Node A` and started on `Node B`. The switchover proceeds as follows:

1. On `Node A`, the cluster-management software performs the following actions:

   a. Cluster manager stops the HP Operations management server running as an application by performing the following action:

      `/opt/OV/lbin/ovharg -stop` *<om_HARG>*

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to stop. The default name for the resource group is `ov-server`.

      The `ovharg` script reads all stop links and executes stop scripts in the appropriate sequence.

   b. Cluster manager designs the virtual IP and unmounts shared file systems.

2. On `Node B`, the cluster-management software reforms the following actions:

   a. Cluster manager assigns the virtual IP and mounts shared file systems.

   b. Cluster manager starts the HP Operations management server running as an application by performing the following action:

      `/opt/OV/lbin/ovharg -start` *<om_HARG>*

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to start. The default name for the resource group is `ov-server`.

      The `ovharg` script reads all start links and executes start scripts in the appropriate sequence.

The resource group *<om_HARG>* (`ov-server`) is now active on `Node B`.

HPOM Troubleshooting in High-Availability Environments

The information in this section helps you to troubleshoot and resolve some of the problems that can occur when HPOM is running in a high-availability environment. In this section, you can find information covering the following topics:

❏ "High-Availability Resource Group Does Not Start" on page 474

❏ "Unplanned Switchover of the HPOM Management Server HA Resource Group" on page 478

❏ "Trap Interception in a High-Availability Environment" on page 479

High-Availability Resource Group Does Not Start

If the HPOM resource group cannot be started on any of the nodes in the high-availability cluster, enable tracing to find out why the resource group refuses to start. You can use the information logged in the trace file to help resolve the problem and restart the resource group. In this section you can find instructions to help you perform the following tasks:

❏ "Enabling Tracing for the HPOM Resource Group" on page 474

❏ "Starting a Resource Group Manually" on page 475

❏ "Starting Individual Resource-Group Components Manually" on page 476

Enabling Tracing for the HPOM Resource Group

To enable tracing in the HPOM high-availability resource group, perform the following steps:

1. Make sure that HPOM high-availability resource group is not running on any cluster node. If the HPOM high-availability resource group is running, stop it with the following command:

   ```
   # /opt/OV/lbin/ovharg_config <om_HARG> -stop <node_name>
   ```

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to stop. The default name for the resource group is `ov-server`.
<node_name>	Name of the high-availability cluster node on which the HPOM resource group that you want to stop is currently running.

2. Enable tracing for the HPOM resource group in the high-availability cluster by using the following command:

   `# /opt/OV/lbin/ovharg -tracing <om_HARG> enable`

3. Restart the HPOM resource group by entering the following command:

   `# /opt/OV/lbin/ovharg_config <om_HARG> -start <node_name>`

   The `ovharg_config` command displays the following return codes:

0	The resource group hosting the HPOM management server started successfully.
1	The resource group hosting the HPOM management server did not start.

If the resource group hosting the HPOM management server does not start, check the output of the trace file, which you can find in the following location on the shared disk on the management server:

`/var/opt/OV/hacluster/ov-server/trace.log`

If the HPOM management server failed to start, you can try to start it manually by performing the steps described in the section entitled “Starting a Resource Group Manually” on page 475.

Starting a Resource Group Manually

To start the high-availability resource group for the HPOM management server manually, perform the following steps:

1. Mount the shared file systems:

   - File system for the HP Operations server database
   - File system for `/etc/opt/OV/share`
   - File system for `/var/opt/OV/share`

- File system for `/var/opt/OV/shared/server`

2. Assign the virtual host to the network interface.
3. Start the HPOM resource group using the following command:

   `# /opt/OV/lbin/ovharg -start <om_HARG>`

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server you want to start manually. The default name for the resource group is `ov-server`.

   The `ovharg` command displays the following return codes:

`0`	The resource group hosting the HPOM management server started successfully.
`1`	The resource group hosting the HPOM management server did not start.

If the resource group hosting the HPOM management server did not start, check the output of the trace file, which you can find in the following location on the shared disk on management server:

`/var/opt/OV/hacluster/ov-server/trace.log`

If the HPOM management server does not respond to attempts to start it manually using the `ovharg` command, you can try to start individual components of the resource group using the steps described in the section entitled "Starting Individual Resource-Group Components Manually".

Starting Individual Resource-Group Components Manually

You can manually start individual HPOM management-server components by using the links placed in the following directory `/var/opt/OV/hacluster/ov-server`. When activated, the scripts perform start, stop, and monitor operations for the resource group hosting the HP Operations management server components. The links are given in the following format:

`[S|K|M]<index>_<operation>`

The following list describes in more detail the individual parts of the link:

`S`, `K`, or `M`	*Type* of action the link executes, for example: start (S), stop (K), or monitor (M).

<index>	Number that indicates the position in the sequence of execution.
<operation>	Name of the operation to start.

NOTE It is essential to execute links in the correct sequence.

Table 12-2 on page 477 lists the links that are available to *start up* individual components of the HPOM high-availability resource group

Table 12-2 Resource Group Component Startup

Link Name	Script Location (/opt/OV/bin/OpC/)	Action
`S100_disable_java_gui`	`utils/disable_java_gui`	Disables the Java GUI
`S400_oracle`	`utils/ha/ha_start_oracle`	Starts the Oracle HARG [a]
`S500_cb`	`utils/ha/ha_start_cb`	Starts the BBC communication broker
`S600_ov_server`	`utils/ha/ha_start_ovserver`	Starts the HPOM management-server HARG [a]
`S700_enable_java_gui`	`utils/enable_java_gui`	Enables the Java GUI

a. High-availability resource group

Table 12-3 on page 477 lists the links that are available to stop individual components of the HPOM high-availability resource group

Table 12-3 Resource Group Component Shutdown

Link Name	Script Location (/opt/OV/bin/OpC/)	Action
`K100_disable_java_gui`	`utils/disable_java_gui`	Disables the Java GUI
`K400_ov_server`	`utils/ha/ha_stop_ovserver`	Stops the HPOM management server HARG [a]
`K500_cb`	`utils/ha/ha_stop_cb`	Stops the BBC communication broker

Table 12-3 Resource Group Component Shutdown (Continued)

Link Name	Script Location (/opt/OV/bin/OpC/)	Action
K600_oracle	utils/ha/ha_stop_oracle	Stops the Oracle HARG [a]

a. High-availability resource group

Table 12-4 on page 478 lists the links that are available to enable monitoring for individual components of the HPOM high-availability resource group

Table 12-4 Resource Group Component Monitoring

Link Name	Script Location (/opt/OV/bin/OpC/utils/)	Action
M100_oracle	ha/ha_mon_oracle	Starts monitoring the Oracle HARG [a]
M200_cb	ha/ha_mon_cb	Monitors the BBC communication broker in a HA cluster
M300_ov_server	ha/ha_mon_ovserver	Starts monitoring the HPOM management-server HARG [a]

a. High-availability resource group

Unplanned Switchover of the HPOM Management Server HA Resource Group

If specific processes abort and cause an undesired switchover of the high-availability resource group hosting the HP Operations management server, you can temporarily remove the problematic processes from the list of monitored processes.

Disabling Monitoring for Individual Processes

To remove individual processes from the list of processes that you are monitoring in a high-availability environment, perform the following steps:

1. Open the ha_mon_ovserver file for editing.

   For more information about the location of the file, see Table 12-4, "Resource Group Component Monitoring," on page 478.

2. Disable monitoring for individual processes.

   In the list of monitored HPOM management server processes at the end of the file, comment out processes that are causing problems.

Trap Interception in a High-Availability Environment

On the active node in the high-availability cluster, the HPOM event interceptor (opctrapi) receives traps from the NNM Postmaster process (pmd). When the cluster switches, opctrapi on the now passive cluster node tries to connect to the pmd process until the high-availability resource group is switched again.

There is no need to manually stop the opctrapi process when the high-availability resource group switches. The process continues to attempt connecting to pmd because the configuration setting OPC_HA_TRAPI is automatically set to TRUE for the eaagt name space during the installation of HPOM in a cluster environment. If the setting is not enabled, opctrapi exits after several connection attempts fail and notifies HPOM of the problem when opctrapi starts again.

Error Handling and Logging in HA Clusters

The scripts that stop, start, and monitor high-availability resource groups (HARG) write information, warnings, and errors to the HA-specific `error.log` file, which you can find in the following location:

`/var/opt/OV/hacluster/<HARG>/error.log`

<HARG>	Name of the high-availability resource group log file you want to read. The default name of the resource group for the HPOM management server is `ov-server`.

The default size of the `trace.log` file for the high-availability resource group is limited. When the maximum file size is reached, `trace.log` is moved to `trace.log.old` and logging information is written into a new `trace.log` file

Setting the Size of the HARG Trace Log

To change the size limit of the `trace.log` file, edit the appropriate parameters in the `settings` file, as follows:

1. Edit the `settings` file for the high-availability resource group hosting the HPOM management server.

   On the HPOM management server, open the `settings` file for editing; you can find the `settings` file in the following location

   `/var/opt/OV/hacluster/<om_HARG>/settings`

<om_HARG>	Name of the high-availability resource group hosting the HPOM management server whose trace-file settings you want to change. The default name for the resource group is `ov-server`.

2. Set the maximum size of the `trace.log` file.

   Adding the following line to the `settings` file for the high-availability resource group hosting the HPOM management server whose operations you want to trace:

   `TRACING_FILE_MAX_SIZE=`*`<maximum size in kBytes>`*

   For example, to set a maximum size of 7MB, enter the following line:

   `TRACING_FILE_MAX_SIZE=7000`

HPOM Elements for High-Availability Resource Groups

This section lists and describes the HPOM elements included by default for a high-availability resource group hosting a HPOM management server. The information in this section covers the following areas:

❏ "HPOM Policies for High-Availability Resource Groups" on page 481

❏ "HPOM Files for High-Availability Resource Groups" on page 482

HPOM Policies for High-Availability Resource Groups

HPOM provides the following policies and policy groups for high-availability resource groups hosting an instance of the HPOM management server:

❏ `HA Virtual Management Server`

The `HA Virtual Management Server` policy group is assigned to the Virtual IP and contains the following policies for the virtual node hosting the HPOM management server:

- `SNMP 7.01 Traps`
- `SNMP ECS Traps`

Note that the trap policy is automatically distributed to all nodes in the high-availability cluster. Since the policy is assigned to the Virtual IP, it is only active on the cluster node where the high-availability resource group (for example, `ov-server`) is currently active.

❏ `HA Physical Management Server`

The `HA Physical Management Server` policy group contains the following policies for the physical instance of the HPOM management server:

- `distrib_mon`
- `opcmsg (1|3)`
- `Cron`

- `disk_util`
- `proc_util`
- `mondbfile`

HPOM Files for High-Availability Resource Groups

HPOM and the various cluster-management products it supports stored configuration files, commands, and so on in various directories. The information in this section explains which files are available and where they normally reside.

HP Operations Management-Server Files

A selection of files to manage the HPOM management server running in a high-availability environment are located in the following directory on the HP Operations management server:

`/opt/OV/bin/OpC/utils/ha`

The `ha` directory contains the following files

- `ha_mon_cb`
- `ha_mon_oracle`
- `ha_mon_ovserver`
- `ha_mon_ovserver_3tier`
- `ha_start_cb`
- `ha_start_oracle`
- `ha_start_ovserver`
- `ha_start_rg`
- `ha_stop_cb`
- `ha_stop_oracle`
- `ha_stop_ovserver`
- `ha_timeout`

For more information about what the individual commands do, see the various tables in “Starting Individual Resource-Group Components Manually” on page 476.

High-Availability Commands

HP Operations Manager provides the following commands to configure and manage an HPOM management server running in a cluster environment:

- ❏ `/opt/OV/lbin/ovharg`

  For more information, run the `ovharg` command with the `-help` option.

- ❏ `/opt/OV/bin/ovharg_config`

  For more information, run the `ovharg_config` command with the `-help` option.

Product-Specific High-Availability Files

HPOM provides configuration files that you can you use to set up, manage, and monitor HPOM in a cluster environment. The files available and their names differ according to platform and product, as follows:

- ❏ HP Serviceguard Files:

  HP Serviceguard specific files are located in the following directory :

  `/opt/OV/lbin/clusterconfig/mcsg`

  The `mcsg` directory contains the following files:

  — `ov_rg.cntl`

  — `ov_rg.conf`

  — `ov_rg.mon`

- ❏ Sun Cluster Files:

  You can find Sun Cluster files in the following directory:

  `/opt/OV/lbin/clusterconfig/sc3`

  The `sc3` directory contains the following files:

  — `monitor_start`

  — `monitor_stop`

  — `start`

  — `stop`

— `probe`

— `gettime`

— `HP.OVApplication`

Additional Sun Cluster files are located in the following directory:

`/opt/OV/lbin/clusterconfig/sc3/OVApplication`

The `OVApplication` directory contains the following files:

— `monitor`

— `online`

— `offline`

A HPOM Managed Node APIs and Libraries

In this Appendix

This chapter provides information about the application-programming interfaces (APIs) that HPOM provides. For example, HPOM allows applications to use the application-programming interface to automatically provide monitor values to HPOM or submit a message.

The information in this section covers the following topics:

- "HPOM APIs on Managed Nodes" on page 487
- "HPOM Managed-Node Libraries" on page 488

HPOM APIs on Managed Nodes

Table A-1 describes commands associated with application program interfaces (APIs) on HPOM managed nodes.

Table A-1 HPOM APIs on Managed Nodes

API	Command	Description
N/A	`opcmack(1)`	Acknowledges an HPOM message received from the message agent on the managed node and sent to the management server.
`opcmon(3)`	`opcmon(1)`	Sends the current value of a monitored object to the HPOM monitoring agent on the local managed node.
`opcmsg(3)`	`opcmsg(1)`	Submits a message to the HPOM message interceptor on the local managed node.

For more detailed information about the commands listed in Table A-1, including the parameters and options that are available, see the respective reference pages for the commands as described in "HPOM Reference Pages" on page 520.

An example of how the API functions are used is available in the following file on the management server:

`/opt/OV/OpC/examples/progs/opcapitest.c`

For the corresponding makefiles, see the *HPOM HTTPS Agent Concepts and Configuration Guide*.

HPOM Managed-Node Libraries

HPOM C functions are available in a shared library. The definitions and return values for the functions are defined in the HPOM include file, `opcapi.h`. For more information about the location of the include file, the required libraries and the makefile for a specific managed node platform, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

NOTE Customer applications must be linked to HPOM using the libraries provided, as well as the link and compile options, in the *HPOM HTTPS Agent Concepts and Configuration Guide*. Integration is only supported if applications are linked.

An example of how the API functions are used is available in the following file on the management server:

`/opt/OV/OpC/examples/progs/opcapitest.c`

This directory also contains the makefiles for building the examples. These makefiles use the compile and link options needed to correctly build an executable.

B HPOM Database Tables and Tablespaces

In this Appendix

This appendix describes the tables and tablespaces that HPOM uses in the in databases for example, to store messages, message annotations, managed node names, and so on. For detailed information about the function of the HPOM tables in the Relational Database Management System (RDBMS), refer to the *HPOM Reporting and Database Schema*.

The information in this section covers the following topics:

- Table B-1, "HPOM Tables and Tablespaces in an Oracle Database," on page 491
- Table B-2, "Non-HPOM Tablespaces," on page 496

HPOM Tables and Tablespaces in an Oracle Database

An Oracle database uses tablespaces to manage available disk space. You can assign datafiles of a fixed size to tablespaces. The size of the various datafiles assigned to a tablespace determines the size of the tablespace. Table B-1 on page 491 shows the default tablespace design and the assigned database tables for HPOM-related data.

To increase the size of a tablespace, you must add a datafile of a particular size to the tablespace. You can add datafiles interactively using the Oracle tool, Server Manager, or using the following `sql` command: `alter tablespace add datafile`.

Table B-1 HPOM Tables and Tablespaces in an Oracle Database

Tables	Tablespace	Size	Comments
opc_act_messages	OPC_1	SIZE 4M AUTOEXTEND ON NEXT 6M MAXSIZE 500M DEFAULT STORAGE (INITIAL 2M NEXT 2M PCTINCREASE 0)	Tables with a heavy load. Indexes are not on the same disk as the table, thus providing extra tablespace.
opc_anno_text opc_annotation opc_msg_text opc_orig_msg_text	OPC_2	SIZE 5M AUTOEXTEND ON NEXT 6M MAXSIZE 500M DEFAULT STORAGE (INITIAL 1M NEXT 1M PCTINCREASE 0)	Tables with a heavy load. Indexes are not on the same disk as the table, thus providing extra tablespace.

Table B-1 HPOM Tables and Tablespaces in an Oracle Database

Tables	Tablespace	Size	Comments
opc_node_names	OPC_3	SIZE 1M AUTOEXTEND ON NEXT 1M MAXSIZE 500M DEFAULT STORAGE (INITIAL 256K NEXT 256K PCTINCREASE 0)	Table with very frequent access.
All other tables	OPC_4	SIZE 26M AUTOEXTEND ON NEXT 2M MAXSIZE 340M DEFAULT STORAGE (INITIAL 64K NEXT 1M PCTINCREASE 0)	None.
Default tablespace of user opc_op	OPC_5	SIZE 1M AUTOEXTEND ON NEXT 1M MAXSIZE 500M DEFAULT STORAGE (INITIAL 32K NEXT 1M PCTINCREASE 0)	None.

Table B-1 HPOM Tables and Tablespaces in an Oracle Database

Tables	Tablespace	Size	Comments
opc_hist_messages	OPC_6	SIZE 4M AUTOEXTEND ON NEXT 2M MAXSIZE 500M DEFAULT STORAGE (INITIAL 2M NEXT 2M PCTINCREASE 0)	Tables with a heavy load. Indexes are not on the same disk as the table, thus providing extra tablespace.
opc_hist_msg_text	OPC_7	SIZE 4M AUTOEXTEND ON NEXT 2M MAXSIZE 500M DEFAULT STORAGE (INITIAL 2M NEXT 2M PCTINCREASE 0)	Tables with a heavy load. Indexes are not on the same disk as the table, thus providing extra tablespace.
opc_hist_orig_text	OPC_8	SIZE 4M AUTOEXTEND ON NEXT 2M MAXSIZE 500M DEFAULT STORAGE (INITIAL 2M NEXT 2M PCTINCREASE 0)	Tables with a heavy load. Indexes are not on the same disk as the table, thus providing extra tablespace.

Table B-1 HPOM Tables and Tablespaces in an Oracle Database

Tables	Tablespace	Size	Comments

`opc_hist_annotation`
`opc_hist_anno_text`
	`OPC_9`	`SIZE 6M`
		`AUTOEXTEND ON NEXT 2M`
		`MAXSIZE 500M`
		`DEFAULT STORAGE (`
		`INITIAL 2M`
		`NEXT 2M`
		`PCTINCREASE 0 )`
			Tables with a heavy load. Indexes are not on the same disk as the table, thus providing extra tablespace.

`opc_service_log`
`opc_service`
	`OPC_10`	`SIZE 6M`
		`AUTOEXTEND ON NEXT 6M`
		`MAXSIZE 500M`
		`DEFAULT STORAGE (`
		`INITIAL 2M`
		`NEXT 2M`
		`PCTINCREASE 0 )`
			Tables with a heavy load. Indexes are not on the same disk as the table, thus providing extra tablespace.

Temporary data (used for sorting)	`OPC_TEMP`	`SIZE 1M`
		`AUTOEXTEND ON NEXT 1M`
		`MAXSIZE 500M`
		`DEFAULT STORAGE (`
		`INITIAL 512K`
		`NEXT 512K`
		`PCTINCREASE 0 )`
			None.

Table B-1 HPOM Tables and Tablespaces in an Oracle Database

Tables	Tablespace	Size	Comments
Index tablespace for active messages	OPC_INDEX1	SIZE 13M AUTOEXTEND ON NEXT 1M MAXSIZE 500M DEFAULT STORAGE (INITIAL 1M NEXT 1M PCTINCREASE 0)	Disk other than than for the following tablespaces: opc_act_messages
Index tablespace for history messages	OPC_INDEX2	SIZE 10M AUTOEXTEND ON NEXT 1M MAXSIZE 500M DEFAULT STORAGE (INITIAL 1M NEXT 1M PCTINCREASE 0)	Disk other than that for the following tablespaces: opc_hist_messages
Index tablespace for service logging	OPC_INDEX3	SIZE 10M AUTOEXTEND ON NEXT 1M MAXSIZE 500M DEFAULT STORAGE (INITIAL 1M NEXT 1M PCTINCREASE 0)	Disk other than for the following tablespaces: opc_service_log

Non-HPOM Tables and Tablespaces

Table B-2 lists the non-HPOM tablespaces in an Oracle database.

Table B-2 Non-HPOM Tablespaces

Tables	Tablespace	Size	Comments

System tables	`SYSTEM`	`SIZE 50M`
		`DEFAULT STORAGE (`
		`INITIAL 16K`
		`NEXT 16K`
		`PCTINCREASE 50 )`
			None

Temporary data	`TEMP`	`SIZE 2M`
		`AUTOEXTEND ON NEXT 1M`
		`MAXSIZE 500M`
		`DEFAULT STORAGE (`
		`INITIAL 100K`
		`NEXT 100K`
		`PCTINCREASE 0 )`
			None

Rollback segments	`RBS1`	`SIZE 1M`
		`AUTOEXTEND ON NEXT 1M`
		`MAXSIZE 500M`
		`DEFAULT STORAGE (`
		`INITIAL 500K`
		`NEXT 500K`
		`MINEXTENTS 10`
		`PCTINCREASE 0 )`
			Tablespace with a heavy load

Table B-2 Non-HPOM Tablespaces (Continued)

Tables	Tablespace	Size	Comments

Tablespace for Oracle Tool Tables (for example, Report Writer)	`TOOLS`	`SIZE 1M`
		`AUTOEXTEND ON NEXT 1M`
		`MAXSIZE 100M`
		`DEFAULT STORAGE (`
		`INITIAL 100K`
		`NEXT 100K`
		`PCTINCREASE 0 )`
			None

C HPOM Audits

In this Appendix

The information in this appendix lists the areas of HP Operations Manager that you can target for audit, describes the actions and operations that produce an entry in the audit log files, and indicates the default level of information logged when the action occurs. For example, you can find out how to monitor changes made to user configurations or any HPOM objects. You can also learn how to use the audit facility to monitor when the scripts and binaries that HPOM uses are started and stopped and if any changes occur to the HPOM processes used by the management server and managed nodes.

In the area of user configuration, you can monitor the names of users who log in and out, when the logins occur, what profiles are assigned to user, and what, if any, changes occur to the user or user profile.

You can also enable auditing for individual HPOM objects such as: managed nodes, node groups, policies, or messages. Any attempts to upload or download configuration data can be logged, too.

You can monitor the use of HPOM scripts, and binaries, for example, when the command-line interface to HPOM is used, or a license check fails.

Finally, you can audit the HPOM processes that control the management server and managed nodes, for example, when the processes are started or stopped.

HPOM Audit Areas

The information in this section explains how to set up an HPOM audit and how to use it to monitor the HPOM environment. The information covers the following areas:

- HPOM user security:

  For more information about the various aspects of user security and authorization that you can target for auditing in HPOM, see "HPOM User Audits" on page 501.

- HPOM objects:

  For more information about the HPOM objects that you can target for auditing, see "HPOM Object Audit Areas" on page 506.

- HPOM scripts and binaries:

  For more information about the HPOM scripts and binaries that you can target for auditing, see "HPOM Scripts and Binaries" on page 515.

- HPOM processes:

  For more information about HPOM processes that you can target for auditing, see "HPOM Processes" on page 516.

Note that the default audit *level* signifies the importance that HPOM attaches by default to a particular audit area. You can use this level to control the amount of information that HPOM writes in audit log files. For example, if you set the audit level to "MAJOR", all actions tagged with the audit level "MAJOR" and anything that is less important (MINOR) are logged in the audit trace files.

HPOM User Audits

This section describes the aspects of HPOM users that you can target for auditing and indicates the audit level that is set by default. The information included in this section covers the following areas:

- Table C-1, "HPOM User-Logins Audit," on page 502
- Table C-2, "HPOM User-Configuration Audit," on page 503
- Table C-3, "HPOM User-Profile Audit," on page 504

- ❏ Table C-4, “HPOM Security-Certificate Audit,” on page 505

Table C-1 on page 502 lists the HPOM objects that you can target for auditing in the area of user logins and logouts. Note that, for auditing purposes, the tracing of successful user logins and logouts is disabled by default. If you want HPOM to write entries in the audit log files for successful user logins and logouts, change the audit level, for example, to “MINOR” or “MAJOR”.

Table C-1 HPOM User-Logins Audit

User Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
Login	User logon succeeds	Disabled	LOGIN_SUCCESS
Login	User logon fails	MAJOR	LOGIN_FAILURE
Login	User logon succeeds from the Java GUI - Client process	SERIOUS	LOGIN_SUCCESS
Login	User logon succeeds from the Java GUI	SERIOUS	LOGIN_SUCCESS
Login	User logon fails from the Java GUI	MAJOR	LOGIN_FAILURE
Logout	User connection closes	Disabled	LOGOUT
Logout	User logs out from the Java GUI - Client process	MAJOR	LOGOUT
Logout	User logs out from the Java GUI	MAJOR	LOGOUT

a. Minor, Major, Serious, or Internal

Table C-2 on page 503 lists the actions and operations that you can target for auditing in the area of user configuration.

Table C-2 HPOM User-Configuration Audit

User Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
User	Administrator modifies user	SERIOUS	OM_CFG_CHG_USER
User	Administrator deletes user	MAJOR	OM_CFG_DEL_USER
User	Administrator assigns user responsibility	SERIOUS	OM_CFG_USER_RESP
User	Administrator deassigns user responsibility	SERIOUS	OM_CFG_USER_RESP
User	Administrator changes a user password	SERIOUS	OM_CFG_USER_PWD_CHANGE
User	Administrator creates a user with administrator privileges	SERIOUS	OM_CFG_ADD_USER
User	Administrator creates a new user	MAJOR	OM_CFG_ADD_USER
User	Administrator assigns a user profile to a user or a user profile	SERIOUS	OM_CFG_CHG_USER
User	Administrator deassigns a user profile from a user or user profile	SERIOUS	OM_CFG_CHG_USER
User	Administrator assigns an application to a user	MINOR	OM_CFG_CHG_USER
User	Administrator deassigns an application from a user	MINOR	OM_CFG_CHG_USER

Table C-2 HPOM User-Configuration Audit (Continued)

User Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
User	Administrator assigns an application group to a user	MINOR	OM_CFG_CHG_USER
User	Administrator deassigns an application group from a user	MINOR	OM_CFG_CHG_USER

a. Minor, Major, Serious, or Internal

Table C-3 on page 504 lists the HPOM actions that you can target for auditing in the area of user profiles.

Table C-3 HPOM User-Profile Audit

User Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
User Profile	Administrator creates a user profile	MINOR	OM_CFG_ADD_USER_PROFILE
User Profile	Administrator copies a user profile	MINOR	none
User Profile	Administrator modifies a user profile	MINOR	OM_CFG_CHG_USER_PROFILE
User Profile	Administrator deletes a user profile	MAJOR	OM_CFG_DEL_USER_PROFILE
User Profile	Administrator assigns an application to a user profile	MINOR	OM_CFG_CHG_PROFILE
User Profile	Administrator deassigns an application from a user profile	MINOR	OM_CFG_CHG_PROFILE

Table C-3 HPOM User-Profile Audit (Continued)

User Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
User Profile	Administrator assigns an application group to a user profile	MINOR	OM_CFG_CHG_PROFILE
User Profile	Administrator deassigns an application group from a user profile	MINOR	OM_CFG_CHG_PROFILE

a. Minor, Major, Serious, or Internal

Table C-4 on page 505 lists the HPOM objects that you can target for auditing in the area of security certificates.

Table C-4 HPOM Security-Certificate Audit

User Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
Certificate	New certificate request created	MAJOR	OM_SV_REQUEST_CERTIFICATE
Certificate	Certificate request granted	SERIOUS	OM_SV_GRANT_CERT_REQUEST
Certificate	Certificate request denied	MAJOR	OM_SV_DENY_CERT_REQUEST
Certificate	Certificate request deleted	MAJOR	OM_SV_DEL_CERT_REQUEST
Certificate	Generic certificate event occurs	MINOR	none

a. Minor, Major, Serious, or Internal

HPOM Object Audit Areas

Table C-5 on page 506 lists the actions and operations that you can target for auditing in the area of HPOM objects.

Table C-5 HPOM-Object Audit Areas

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Message	User owns a message	MINOR	OM_MESSAGE_OWN
HPOM Message	User disowns a message	MINOR	OM_MESSAGE_OWN
HPOM Message	User forwards a message to the Trouble Ticket interface	MINOR	OM_MSG_FWD_NS_IF
HPOM Message	User forwards a message to the Notification Service interface	MINOR	OM_MSG_FWD_TT_IF
HPOM Message	User deletes one or more HPOM messages	MINOR	OM_MSG_DEL
HPOM Message	User acknowledges one or more HPOM messages	MINOR	OM_MSG_MULTI_ACK
HPOM Node	User creates a node	MINOR	OM_CFG_ADD_NODE
HPOM Node	User modifies a node	MINOR	OM_CFG_CHG_NODE
HPOM Node	User deletes a node	MAJOR	OM_CFG_DEL_NODE
HPOM Node	User assigns a policy to a node	MINOR	OM_CFG_CHG_NODE
HPOM Node	User deassigns a policy from a node	MINOR	OM_CFG_CHG_NODE
HPOM Node	User assigns a policy to a node group	MINOR	OM_CFG_CHG_NODE_GRP

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Node	User deassigns a policy from a node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM Node	User assigns a policy group to a node	MINOR	OM_CFG_CHG_NODE
HPOM Node	User deassigns a policy group from a node	MINOR	OM_CFG_CHG_NODE
HPOM Node	User assigns a policy group to a node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM Node	User deassigns a policy group from a node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM Node	User assigns a category to a node	MINOR	OM_CFG_CHG_NODE
HPOM Node	User deassigns a category a the node	MINOR	OM_CFG_CHG_NODE
HPOM Node	User installs a subagent	SERIOUS	OM_SUBAGT_INSTALL
HPOM Node	User removes a subagent	SERIOUS	OM_SUBAGT_DEINSTALL
HPOM Node	User reinstalls a subagent	SERIOUS	OM_SUBAGT_INSTALL
HPOM Node	User activates a subagent	SERIOUS	OM_SUBAGT_INSTALL
HPOM Node	User deploys agent software to a node	SERIOUS	OM_AGT_SW_INSTALL
HPOM Node	User removes agent software from a node	SERIOUS	OM_AGT_SW_DEINSTALL
HPOM Node	User updates the flexible-management policy deployment	SERIOUS	OM_AGT_MGRCONF_DEPLOY

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Node	User deploys HPOM instrumentation to a managed node	SERIOUS	`OM_AGT_INSTR_DEPLOY`
HPOM Application	User starts a terminal application	MAJOR	`OM_TERMINAL_APP_LAUNCH`
HPOM Application	User starts an application	MAJOR	none
HPOM Application	User creates an HPOM application	MINOR	`OM_CFG_ADD_APPL`
HPOM Application	User modifies an HPOM application	MINOR	`OM_CFG_CHG_APPL`
HPOM Application	User deletes an HPOM application	MAJOR	`OM_CFG_DEL_APPL`
HPOM External Application	User registers an external application with the message-stream interface (MSI)	MINOR	`OM_SV_REGISTER_MSI`
HPOM External Application	User unregisters an external application from the MSI	MINOR	`OM_SV_REGISTER_MSI`
HPOM Config	User downloads messages from the history browser	MINOR	`OM_SV_HIST_MSG_DOWNLOAD`
HPOM Config	User uploads messages to the history browser	SERIOUS	`OM_SV_HIST_MSG_UPLOAD`
HPOM Config	User performs a configuration upload	SERIOUS	`OM_CFG_UPLOAD`

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Config	User modifies the database-maintenance configuration	SERIOUS	OM_CFG_DB_MAINTENANCE
HPOM Config	User modifies the management-server configuration	SERIOUS	OM_CFG_DB
HPOM Config	User performs a configuration download	MINOR	OM_CFG_DOWNLOAD
HPOM Config	Administrator activates heartbeat monitoring for a managed node	SERIOUS	OM_CFG_CHG_NODE_HEARTBEAT
HPOM Config	Administrator deactivates heartbeat monitoring for a node	SERIOUS	OM_CFG_CHG_NODE_HEARTBEAT
HPOM Config	Administrator changes the heartbeat monitoring interval for a node	SERIOUS	OM_CFG_CHG_NODE_HEARTBEAT
HPOM Config	User uploads generic policies from a directory	MAJOR	OM_CFG_UPLOAD_POLICY_TYPE
HPOM Config	User uploads generic policies from a file	MINOR	OM_CFG_UPLOAD_POLICY_TYPE
HPOM Config	User enables duplicate message suppression	SERIOUS	OM_CFG_DUP_MSG_SUPPRESS
HPOM Config	User disables duplicate message suppression	SERIOUS	OM_CFG_DUP_MSG_SUPPRESS
HPOM Config	User changes global options for the HPOM management server: parallel distribution	SERIOUS	OM_CFG_MISC

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Config	HPOM reads Service Navigator configuration	MAJOR	OM_CFG_READ_SERVNAV
HPOM Config	HPOM notices a change to the Service Navigator configuration	SERIOUS	OM_CFG_WRITE_SERVNAV
HPOM Config	User performs a backup	MINOR	OM_SV_BACKUP
HPOM Config	User enables customized startup message	MINOR	OM_STARTUPMSG
HPOM Config	User disables customized startup message	MINOR	OM_STARTUPMSG
HPOM Config	User modifies customized startup message	MINOR	OM_STARTUPMSG
HPOM Config	User deletes customized startup message	MINOR	OM_STARTUPMSG
HPOM Other	User creates a new category	MINOR	OM_CFG_ADD_CATEGORY
HPOM Other	User modifies a category	MINOR	OM_CFG_CHG_CATEGORY
HPOM Other	User deletes a category	MAJOR	OM_CFG_DEL_CATEGORY
HPOM Other	User registers a generic policy type	MINOR	OM_CFG_ADD_POLICY_TYPE
HPOM Other	User modifies a generic policy type	MINOR	OM_CFG_CHG_POLICY_TYPE
HPOM Other	User deletes a generic policy type	MAJOR	OM_CFG_DEL_POLICY_TYPE
HPOM Other	User creates an application group	MINOR	OM_CFG_ADD_APPL_GRP

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Other	User modifies an application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM Other	User deletes an application group	MAJOR	OM_CFG_DEL_APPL_GRP
HPOM Other	User assigns an application to an application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM Other	User deassigns an application from an application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM Other	User assigns an application group to another application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM Other	User deassigns an application group from another application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM Other	User creates a condition	MINOR	OM_CFG_CHG_POLICY
HPOM Other	User deletes a condition	MINOR	OM_CFG_CHG_POLICY
HPOM Other	User adds/sets an instruction interface	MINOR	OM_CFG_DEL_INSTR_IF
HPOM Other	User copies an instruction interface	MINOR	OM_CFG_CPY_INSTR_IF
HPOM Other	User modifies an instruction interface	MINOR	OM_CFG_CHG_INSTR_IF
HPOM Other	User deletes an instruction interface	MAJOR	OM_CFG_DEL_INSTR_IF

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Other	User creates a new message group	MINOR	OM_CFG_ADD_MSG_GRP
HPOM Other	User modifies a message group	MINOR	OM_CFG_CHG_MSG_GRP
HPOM Other	User modifies a message-group name	SERIOUS	OM_CFG_CHG_MSG_GRP
HPOM Other	User deletes a message group	MAJOR	OM_CFG_DEL_MSG_GRP
HPOM Other	User creates a node-layout hierarchy	MINOR	OM_CFG_NODE_LAYOUT
HPOM Other	User modifies a node-layout hierarchy	MINOR	OM_CFG_NODE_LAYOUT
HPOM Other	User deletes a node-layout hierarchy	MAJOR	OM_CFG_NODE_LAYOUT
HPOM Other	User creates a layout group	MINOR	OM_CFG_LAYOUT_GRP
HPOM Other	User modifies a layout group	MINOR	OM_CFG_LAYOUT_GRP
HPOM Other	User deletes a layout group	MAJOR	OM_CFG_LAYOUT_GRP
HPOM Other	User creates a notification schedule	MINOR	OM_CFG_CHG_NOTIFY_SCHEDULE
HPOM Other	User modifies a notification schedule	MINOR	OM_CFG_CHG_NOTIFY_SCHEDULE
HPOM Other	User deletes a notification schedule	MINOR	OM_CFG_CHG_NOTIFY_SCHEDULE

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Other	User creates a notification service	MINOR	OM_CFG_CHG_NOTIFY_SERVICE
HPOM Other	User modifies a notification service	MINOR	OM_CFG_CHG_NOTIFY_SERVICE
HPOM Other	User deletes a notification service	MINOR	OM_CFG_CHG_NOTIFY_SERVICE
HPOM Other	User creates a node group	MINOR	OM_CFG_ADD_NODE_GRP
HPOM Other	User modifies a node group	MINOR	OM_CFG_ADD_NODE_GRP
HPOM Other	User deletes a node group	MAJOR	OM_CFG_ADD_NODE_GRP
HPOM Other	User changes the MSI setting - Enable	SERIOUS	OM_CFG_CHG_MSI
HPOM Other	User changes the MSI setting - Disable	SERIOUS	OM_CFG_CHG_MSI
HPOM Other	User changes the MSI setting - Allowing for externally defined actions	SERIOUS	OM_CFG_CHG_MSI
HPOM Other	User assigns a category to a policy	MINOR	OM_CFG_CHG_POLICY
HPOM Other	User deassigns a category from a policy	MINOR	OM_CFG_CHG_POLICY
HPOM Other	User assigns a category to a policy group	MINOR	OM_CFG_CHG_POLICY_GRP

Table C-5 HPOM-Object Audit Areas (Continued)

Object Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Other	User deassigns a category from a policy group	MINOR	`OM_CFG_CHG_POLICY_GRP`
HPOM Other	User creates a category directory under the instrumentation directory	MINOR	`OM_CFG_ADD_CATEGORY`
HPOM Other	User removes a category directory under the instrumentation directory	MINOR	`OM_CFG_DEL_CATEGORY`
HPOM Other	User creates a policy group	MINOR	`OM_CFG_ADD_POLICY_GRP`
HPOM Other	User assigns a node to a node group	MINOR	`OM_CFG_CHG_NODE_GRP`
HPOM Other	User deassigns a node from a node group	MINOR	`OM_CFG_CHG_NODE_GRP`
HPOM Other	User creates a new policy	MINOR	`OM_CFG_ADD_POLICY`
HPOM Other	User modifies a policy	MINOR	`OM_CFG_CHG_POLICY`
HPOM Other	User deletes a policy	MAJOR	`OM_CFG_DEL_POLICY`
HPOM Other	User edits a policy using the `poledit` application	MINOR	`OM_CFG_CHG_POLICY`

a. Minor, Major, Serious, or Internal

HPOM Scripts and Binaries

Table C-6 on page 515 lists the HPOM processes that you can select for auditing

Table C-6 HPOM Scripts and Binaries Audit Areas

Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM script/binaries access - Execute	Command-line interface (CLI) starts	MINOR	none
HPOM script/binaries access - Execute	Scheduled action runs	MAJOR	OM_AGT_RUN_SCHED_ACT
HPOM script/binaries access - Execute	License check fails when adding a new node	MAJOR	OM_LICENSE_CHECK_FAILURE
HPOM script/binaries access - Execute	License check fails when adding a new agent-less node	MAJOR	OM_LICENSE_CHECK_FAILURE
HPOM script/binaries access - Execute	Nightly license check fails	MAJOR	OM_LICENSE_CHECK_FAILURE

a. Minor, Major, Serious, or Internal

HPOM Processes

Table C-7 on page 516 lists the HPOM processes that you can select for auditing

Table C-7 HPOM Process Audit Areas

Audit Area	Use Case	Default Audit Level [a]	ovoconf Variable in Audit Name Space
HPOM Startup	Administrator starts the HP Operations agent software locally	MINOR	OM_AGT_START
HPOM Startup	Administrator starts the HP Operations agent software remotely	MINOR	OM_AGT_START
HPOM Startup	Administrator starts the HP Operations management-server software	MAJOR	OM_SV_START
HPOM Shutdown	Administrator shuts down the HP Operations management-server software	SERIOUS	OM_SV_STOP
HPOM Shutdown	Administrator shuts down the HP Operations agent software locally	SERIOUS	OM_AGT_STOP_ON_SV
HPOM Shutdown	Administrator shuts down the HP Operations agent software remotely	MAJOR	OM_AGT_STOP
HPOM Service Engine	Administrator performs one of the following actions: add, remove, replace, assign, or deassign.	None	opcsvcm

a. Minor, Major, Serious, or Internal

D Reference Pages

In this Appendix

This appendix describes how to access the reference pages that are available for HP Operations Manager (HPOM) and HP Service Navigator (Service Navigator) and lists all the reference pages that are available for the different areas. The information in this appendix covers the following areas:

- "HPOM Reference Pages" on page 519
- "HPOM Reference Pages" on page 520
- "Reference Pages for the HPOM API" on page 525
- "Reference Pages for Service Navigator" on page 526

HPOM Reference Pages

You can access the HPOM reference pages from the command line, from online help, or in HTML format on your management server.

Accessing Reference Pages from the Command Line

To access an HPOM reference page from the command line, enter the following command:

```
# man <reference-page_name>
```

Printing Reference Pages from the Command Line

To print an HPOM reference page from the command line, enter the following command:

```
# man <reference-page_name> | col -lb | lp -d printer_name
```

Accessing Reference Pages in HTML Format

To access the HPOM reference pages in HTML format, for example, from an Internet browser, enter the following URL in the browser:

```
http://<management_server>:3443/ITO_MAN
```

Substitute the variable in the URL as follows:

<management_server>	Fully qualified host name of your HPOM management server.

HPOM Reference Pages

This section describes the reference pages that are available in HPOM.

Table D-1 **HPOM Reference Pages**

Reference Page	Description
call_sqlplus.sh(1)	Calls SQL*Plus.
inst.sh(1M)	Installs HPOM software on managed nodes.
inst_debug(5)	Debugs an installation of the HPOM agent software.
ito_op(1M)	Launches the HPOM JavaGUI or Service Navigator GUI.
ito_op_api_cli(1M)	Enables calls to the Java GUI Remote APIs.
opcbackup_offline(1M)	Interactively backs up the HPOM environment for Oracle.
opcbackup_offline(5)	Backs up the HPOM configuration.
opc_chg_ec(1M)	Changes circuit names in event correlation (EC) policies in the HPOM database.
opcdelmsg(1M)	Removes messages from the message-manager queue even while management-server processes are running. Only messages matching all specified criteria are deleted.
opcrecover_offline(1M)	Interactively restores the HPOM environment for Oracle.
opcrecover_offline(5)	Restores the HPOM configuration.
opcack(1M)	Externally acknowledges active messages.

Table D-1 HPOM Reference Pages (Continued)

Reference Page	Description
opcackmsg(1M)	Externally acknowledges active messages using message IDs.
opcackmsgs(1M)	Externally acknowledges active messages using specific message attributes.
opcactivate(1M)	Activates a pre-installed HPOM agent.
opcadddbf(1M)	Adds a new datafile to an Oracle tablespace.
opcagt(1M)	Manages agent processes on a managed node.
opcagtutil(1M)	Parses the agent-platform file and performs operations with extracted data.
opccfgdwn(1M)	Downloads configuration data from the database to flat files.
opccfgout(1M)	Configures condition status variables for scheduled outages in HPOM.
opccfgupld(1M)	Uploads configuration data from flat files to the database.
opccfguser(1M)	Configures HPOM for UNIX operators and is used for assigning user profiles, unassigning user profiles, and configuring the user-responsibility matrix.
opccltconfig(1M)	Configures HPOM client file sets.
opcconfig(1M)	Configures an HPOM management server.
opccsa(1M)	Provides the functionality for listing, mapping, granting, denying, and deleting specified certificate requests.

Table D-1 HPOM Reference Pages (Continued)

Reference Page	Description
opccsacm(1M)	Performs `ovcm` functionality, for example, manually issuing new node certificate or using the installation key.
opcdbidx(1M)	Upgrades the structure of the HPOM database.
opcdbinit(1M)	Initializes the database with the default configuration.
opcdbinst(1M)	Creates or removes the HPOM database schema.
opcdbpwd(1M)	Changes the password of the HPOM database user `opc_op`.
opcdbsetup(1M)	Creates tables in the HPOM database.
opcdcode(1M)	Views HPOM encrypted policy files.
opcerr(1M)	Displays instruction text for HPOM error messages.
opcgetmsgids(1m)	Lists the IDs associated with an original message ID (provided as the argument with the command), for example: the ID of correlated messages, messages modified by an external MSI, and so on.
opchbp(1M)	Switches heartbeat polling of managed nodes on or off.
opchistdwn(1M)	Downloads HPOM history messages to a file.
opchistupl(1M)	Uploads history messages to the HPOM database.
opcinstrumcfg(1M)	Manages category information in the file system and database level simultaneously.

Table D-1 HPOM Reference Pages (Continued)

Reference Page	Description
opcinstrumdwn(1M)	Downloads all instrumentation files to a single flat file that can then be manually deployed to an HPOM agent.
opcmack(1)	Acknowledges an HPOM message by specifying the message ID.
opcmom(4)	Provides an overview of HPOM flexible-management functionality.
opcmomchk(1)	Checks the syntax of HPOM flexible-management policies.
opcmon(1)	Forwards the value of a monitored object to the HPOM monitoring agent on the local managed node.
opcmsg(1)	Submits a message to HPOM.
opcownmsg(1M)	Sets, unsets, and changes HPOM message ownership.
opcpat(1)	Tests a program for HPOM pattern matching.
opcragt(1M)	Remotely manages agent services for HPOM on a managed node.
opcskm(3)	Manages secret keys.
opcsqlnetconf(1M)	Configures the HPOM database to use an Net8 connection.
opcsv(1M)	Manages HPOM management-server processes.
opcsw(1M)	Sets the software status flag in the HPOM database.
opcswitchuser(1M)	Switches ownership of the HPOM agents.
opcpolicy(1M)	Maintains policies in files.

Table D-1 HPOM Reference Pages (Continued)

Reference Page	Description
opcpolicy(1M)	Enables and disables policies.
opctmpldwn(1M)	Downloads and encrypts HPOM message-source policies.
opcwall(1)	Sends a message to all HPOM users who are currently logged in.
ovocomposer(1M)	Performs tasks related to OV Composer.
ovocomposer(5)	Describes the Correlation Composer, an HPOM event-correlation feature.
ovtrap2opc(1M)	Converts the `trapd.conf` file and the HPOM policy file.

Reference Pages for the HPOM API

This section describes reference pages that are available for HPOM application program interfaces (APIs).

Table D-2 HPOM API Reference Pages

Reference Page	Description
opcmon(3)	Forwards the value of a monitored object to the HPOM monitoring agent on the local managed node.
opcmsg(3)	Submits a message to HPOM.

Reference Pages for Service Navigator

This section describes reference pages for the Service Navigator.

Table D-3 **Service Navigator Reference Pages**

Reference Page	Description
opcservice(1M)	Configures Service Navigator.
opcsvcattr (1M)	Adds, changes, or removes service attributes.
opcsvcconv(1M)	Converts service-configuration files of Service Navigator from the previous syntax to the Extensible Markup Language (XML).
opcsvcdwn(1M)	Downloads status logs of Service Navigator to a file.
opcsvcterm(1M)	Emulates an interface to Service Navigator. The interface inputs Extensible Markup Language (XML) markup into `stdin` and outputs Extensible Markup Language (XML) markup to `stdout`.
opcsvcupl(1M)	Uploads the Service Navigator service-status logs to the HPOM database.

Index

C

G

I

O

T

X

Z