HP Operations Manager for UNIX

Administrator's Reference

Software Version: 9.00

Manufacturing Part Number: None

Date: June, 2009

© Copyright 1996-2009 Hewlett-Packard Development Company, L.P.

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.

©Copyright 2005-2009 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

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

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of the Open Group.

1. Installing HPOM Agents on the Managed Nodes

2. Configuring HPOM

6. Integrating Applications into HPOM

7. About Notification Services and Trouble Ticket Systems

8. About HPOM Language Support

9. About the HPOM Java-Based Operator GUI

10. About HPOM Processes

11. About HPOM Security

12. Maintaining HPOM

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.

First Edition:	May 2009

Preface

This guide explains HP Operations Manager (HPOM) for UNIX to the HPOM administrator who installs, administers, and troubleshoots HPOM systems.

The product name has been recently changed from HP OpenView Operations to the HP Operations Manager. Consider that the short product name is HPOM. Due to a recent product name change, you will find in this document as well as in most other HPOM related materials still the old names referenced: HP OpenView Operations for UNIX, or in short OVO/UNIX or just OVO.

What this Guide Does

This guide explains agent installation, first-time configuration, agent de-installation, tuning, and troubleshooting to HPOM administrators.

Who Should Read this Guide

This guide is for the HPOM administrator who installs HPOM on the managed nodes, and is responsible for administering and troubleshooting the HPOM system. The guide assumes you have a sound knowledge of HP-UX or Sun Solaris system, as well as network administration and troubleshooting.

Authority Required to Use this Guide

To use this guide, you should have authority to do the following:

- ❏ Update the system with new software
- ❏ Perform remote logins to other systems
- ❏ Search, locate, and edit plain text files

Knowledge Required to Use this Guide

To use this guide, you should be thoroughly familiar with the following:

- ❏ File system organization
- ❏ X applications
- ❏ HP NNM platform user interface and services
- ❏ Database administration
- ❏ HPOM concepts

About Related Documents

For information about how to install HPOM on the management server or upgrade an earlier version of HPOM, see the *HPOM Installation Guide for the Management Server*. For information about HPOM concepts, see the *HPOM Concepts Guide*.

Conventions

The following typographical conventions are used in this manual.

Table 1 Typographical Conventions

Font	Meaning	Example
Italic	Book or manual titles, and man page names	Refer to the *HPOM Administrator's Reference* and the *opc(1M)* manpage 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** observes...
`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/dialog-box 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]`.

HPOM 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 gets updated every 2-3 months with the latest news such as additionally supported OS versions, latest patches and so on.

HPOM Manuals

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

Table 2 HPOM Manuals

Manual	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: • Software and hardware requirements • Software installation and de-installation 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 Entity Relationship Diagrams	Provides you with an overview of the relationships between the tables and the HPOM database.	PDF only

Table 2 HPOM Manuals (Continued)

Manual	Description	Media
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
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
Managing Your Network with HP Network Node Manager	Designed for administrators and operators. This manual describes the basic functionality of the HP Network Node Manager, which is an embedded part of HPOM.	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 for UNIX Developer's Toolkit If you purchase the HP Operations Manager for UNIX 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
HP Event Correlation Designer for HPOM If you purchase HP Event Correlation Designer for HPOM, you receive the following additional documentation. Note that HP Event Correlation Composer is an integral part of HPOM. HP Composer usage in the HPOM context is described in the OS-SPI documentation.		
HP ECS Configuring Circuits for HPOM	Explains how to use the ECS Designer product in the HPOM environment.	PDF

HPOM Online Information

The following information is available online.

Table 4 HPOM Online Information

Online Information	Description
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 Man Pages	Manual pages available online for HPOM. These manual pages are also available in HTML format. To access these pages, go to the following location (URL) with 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 man pages for the HP Operations HTTPS agents are installed on each managed node.

About HPOM Online Help

This preface describes online documentation for the HP Operations Manager (HPOM) Java operator graphical user interface (GUI).

Online Help for the Java GUI and Service Navigator

The online help for the HP Operations Manager (HPOM) Java graphical user interface (GUI), including Service Navigator, helps operators to become familiar with and use the HPOM product.

Types of Online Help

The online help for the HPOM Java GUI includes the following information:

- **Tasks**

  Step-by-step instructions.

- **Concepts**

  Introduction to the key concepts and features.

- **References**

  Detailed information about the product.

- **Troubleshooting**

  Solutions to common problems you might encounter while using the product.

- **Index**

  Alphabetized list of topics to help you find the information you need, quickly and easily.

Viewing a Topic

To view any topic, open a folder in the left frame of the online documentation window, then click the topic title. Hyperlinks provide access to related help topics.

Accessing the Online Help

To access the help system, select `Help: Contents` from the menu bar of the Java GUI. A web browser opens and displays the help contents.

NOTE To access online help for the Java GUI, you must first configure HPOM to use your preferred browser.

1 Installing HPOM Agents on the 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 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 UNIX systems, 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
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 logfiles 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.

Tips for Installing on Managed Nodes

When installing on the managed nodes, follow these guidelines:

- **Install on All Managed Nodes**

  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.

- **Do Not Use Internal HPOM Names**

  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.

- **Do Not Use Host Aliases**

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

- **Specify One 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.

- **Reserve Extra 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.

- **Use Long Host Names for Actions Only**

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

❑ **Use Operating System Versions Supported by HPOM**

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
```

❑ **Synchronize System Times**

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.

❑ **Learn All Root Passwords**

Before you install the HPOM agent software, make sure you know all the root passwords of all the managed nodes.

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).

❑ **Work Around Disk Space Limitations**

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.

❑ **Network Path to Management Server**

There must be an existing route (network path) to and from the management server from and to the managed nodes.

❑ **De-install Software Before Moving Management Server**

If you want to move the management server to some other system, you must first de-install the HPOM managed node software from all managed nodes. See also “Changing Hostnames and IP Addresses” on page 446 for more information.

❑ **Purge the Functionality of the HPOM Default Operator**

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. This information will be recreated when you re-install the HPOM agent software.

UNIX:

- 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 may not remove the HPOM default operator from Windows managed nodes because the agents run under the operator’s account.

❑ **Stop All Programs and Applications Using “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*.

Tips for Installing on the Management Server

When installing on the management server, follow these guidelines:

- **Clean the "distrib" 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`

  You should clean this directory only in an emergency, and only after the HP Operations management server processes have been stopped.

- **Do Not Interrupt Installation or De-Installation**

  Avoid interrupting the software installation or de-installation 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 de-installation 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`

- **Do Not De-Install Bits**

  If any managed node is still configured and has the HPOM bits, do not de-install any of the management server bits (for example `OVOPC-ORA` or `OVOPC`).

- **Do Not De-Install the Tape Image**

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

Tips for 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.

❑ **Same Log Directory**

During de-installation of HPOM, the non-default log directory on UNIX systems is erased.

The following rules apply to this directory:

- *Directories for Managed Nodes*

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

- *Directories for Other Applications*

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

- *Subdirectories for Other Applications or Managed Nodes*

  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**

  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.

Installing or Updating HPOM Software Automatically

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.

About the Installation Script

When you install, update, or de-install HPOM software, you use the `inst.sh(1M)` script.

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 of this script, you can set a shell variable for the user `root`:

Bourne/Korn `OPC_SILENT=1; export OPC_SILENT`

C `setenv OPC_SILENT`

About 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.

About Managed Nodes

Before installing or de-installing HPOM software on the managed nodes, read the section “Installation Tips” on page 38.

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* manpage.

To Install or Update HPOM Software Automatically

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 a password is missing, you are asked to supply one before installation is done.)

Watch the script execution carefully. Your interaction might be required if any errors or warnings occur. Then, when the script is finished, verify the overall result of the script run.

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

If necessary (for example, 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 Method

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*

    Software requirements as described in the *HPOM Installation Guide for the Management Server*.
  - *Managed Nodes*

    Software requirements for the HPOM managed node as described in *HPOM Software Release Notes*.
- ❏ Installed and fully configured SSH client and server (daemon) on both the management server and the managed nodes.
- ❏ Login without a password for the user `root` from the management server must be enabled on both the management server and the managed nodes. See “To Install HPOM Agent Software Using SSH Installation Method” on page 49.

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

To Install HPOM Agent Software Using SSH Installation Method

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 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. Run the `ssh-keygen`.

   ```
   [username@local ~]$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:

   - **`scp .ssh/identity.pub user@managednode:.ssh/authorized_keys`**
   - **`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 at 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)`.

To Install HPOM Agent Software Using SSH Agent Installation Method

This section describes how to use the Secure Shell (SSH) agent for installing the HPOM agent software on managed nodes with the difference from the "To Install HPOM Agent Software Using SSH Installation Method" section in that you must provide a password before the installation. This prevents passwordless root logins from the HPOM management server to the managed nodes.

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 "To Install HPOM Agent Software Using SSH Installation Method" 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 "To Install HPOM Agent Software Using SSH Installation Method" 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 “To Install HPOM Agent Software Using SSH Installation Method” section.
5. Remove the key from the database, or stop the SSH agent by running the following command:

   ssh-add -d *<identity_file_name>*

De-Installing HPOM Software from the Managed Node

To de-install the HPOM agent software, follow these steps:

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

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

NOTE

After de-installing the HPOM software from a managed node, you must enter the following command on the management server:

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

Managing HPOM Agent Software

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.

Managing Different Versions of Agent Software

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 56 for information about how to query the version of the installed agent software.

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

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

Where:

<platform_selector>	One of the selectors for your platform.
<ovo_version>	Version of HPOM that supports this agent platform (for example, A.08.10).
<package_type>	Type of RPC communication used by that platform.

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

Administering Managed Nodes Depending on Subagent id Values

`opcragt` in HPOM for UNIX can accept subagent id values as numbers or names. The communication type being used is HTTPS.

When the `subagent id` argument is a name, the selected node is administrated directly. When the `subagent id` is a number, a mapping to `subagent id name` must exist in the `subagt_aliases` file.

By default three mappings are defined in `subagent_aliases` file:

- (0 -> AGENT)
- (1 -> EA)
- (12 -> CODA)

The location of the `subagt_aliases` file is:

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

When mapping between number and name is required but does not exist, the following error message is displayed:

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

USAGE EXAMPLES

❑ Query Subagent Status

```
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.
```

❑ Start/Stop Subagent on Nodes

```
opcragt -start -id CODA <node_name>
Node <node_name>:
Starting OpC services...Done.
```

Removing an Older Agent Package

If you no longer need an older HPOM agent package, and that package is not installed on any managed node, you can remove it by running:

/opt/OV/bin/OpC/install/rm_opc.sh <*platform_selector*> \ <*vpo_version*>

Where:

<*platform_selector*>.	One of the selectors for your platform.
<*hpom_version*>.	Version of HPOM that supports this agent platform (for example, 9.00).

NOTE

Do not use `swremove` to de-install an HPOM agent package that you no longer need. Running `swremove` is useful only if you want to de-install *all* HPOM agent packages of a particular architecture. In addition, remove the managed nodes by using the `opcnode` tool *before* performing a complete de-installation of all managed nodes of a given architecture. Otherwise, the managed nodes cannot be removed easily using the `rm_opc.sh` script.

Managing of Subagents in HPOM

Subagents are components that are not a part of the default HPOM distribution, but are partially manageable from HPOM. Some of them are controlled by the OV Control Daemon.

Administering of subagents in HPOM include operating with the tasks outlined in the “Administering the Subagents in HPOM” on page 60.

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*.

Administering the Subagents 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. These tasks are outlined in the following topics:

1. Assigning Subagents to Managed Nodes
2. Installing Subagents on Managed Nodes

To avoid problems with subagents distribution to managed nodes, consider also the tasks presented in the following topics:

- ❏ Activating Subagents
- ❏ Resolving Migration Impacts

Assigning Subagents 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.

Installing Subagents 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.

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

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

Where the *<node_name>* is the name of the node where the subagent is installed.

Likewise, use the `-uninstall` option of the `opcragt` to deinstall the subagent:

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

To install all assigned subagents simultaneously, enter the following:

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

To redistribute the subagent software, use the following command:

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

NOTE Use of `opcragt -force` does not trigger the redistribution process. This is to prevent the unnecessary deployment of subagent packages upon the the agent configuration distribution using the `-force` option of the command `opcragt`.

See the *opcragt (1M)* man page for usage details.

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

Activating Subagents

Activating a subagent means setting the active flag for this subagent in the HPOM database. To activate a subagent for a particular node, enter the following command:

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

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 Impacts

When the configuration is migrated 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 upon subsequent distribution, you can activate the subagents for managed nodes on the target HPOM server. For more information, see “Activating Subagents” on page 62.

To avoid problems with subagent distribution on nodes, perform **one** of the following tasks:

- Install all subagent packages on the HPOM 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 an inventory information about particular subagents on managed nodes.

Debugging Software Installation and De-Installation on Managed Nodes

HPOM provides facilities for debugging the installation and de-installation 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.

Facilities for Debugging Installation and De-Installation

The following facilities are available:

- **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 de-installation 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.

To Enable Debugging

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

To enable installation and de-installation debugging, 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 man page *inst_debug(5)*.

To Disable Debugging

To disable debugging, remove the following file:

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

2 Configuring HPOM

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*.

About 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.

About 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.

Node Group for the Management Server

The management server belongs to the `hp_ux` node group.

Managing Node Groups

As an HPOM administrator, you can add, modify, delete, and list node groups using the `opcnode` command line tool HPOM. For more information, see the *opcnode(1m)* man page.

About Default Message Groups

HPOM provides default message groups. As an administrator, 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
SNMP	Messages generated by SNMP traps.
Network	Messages about network or connectivity problems.
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.
Performance	Messages about hardware malfunctions (that is, CPU, disk, or process malfunctions) and software malfunctions (for example, HP Performance malfunctions).
Output	Messages about print spooling and hardcopy functionality (for example, `lp(1)`, `lpr(1)`.
Job	Messages about job streaming.
OS	Messages about malfunctions in the operating system, I/O, and so on.
Security	Messages about security violations or attempts to break into a system.
Database	Messages about database problems
OpC	Messages generated by HPOM itself. This message group should not be used by `opcmsg(1|3)`. The HPOM message group cannot be deleted.
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.

Table 2-1 HPOM Default Message Groups (Continued)

Message Group	Description
Hardware	Messages about hardware problems
SSP	Messages generated by SSP policies.
HA	Messages about high-availability problems.

About Message Ownership

HPOM message ownership enables users to mark or own messages.

Marking or Owning a Message

By marking or owning a message, you restrict access to the message, as follows:

- **Marking a Message**

  Operator or administrator has taken 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.

Types of Ownership Display Modes

HPOM provides different ways to configure the way message ownership is displayed and enforced.

HPOM provides two **ownership-display modes**:

- **No Status Propagation** (default)

  Uses the option `OPC_OWN_DISPLAY NO_STATUS_PROPAGATE`.

- **Status Propagation**

  Uses the option `OPC_OWN_DISPLAY STATUS_PROPAGATE`.

About the “No Status Propagation” Display Mode

If the display mode is set to `No Status Propagation`, 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.

About the "Status Propagation" Display Mode

If the ownership-display mode is set to status propagation, then the status of all messages whether they are owned or not is used in reflecting status propagation in 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 72 and *"Configuring Message Ownership Display Mode" on page 73* respectively.

Changing Ownership Display Modes

To change to an alternative ownership display mode, follow these steps:

1. To use the required display mode, use the command line tool `ovconfchg` on the HP Operations management server. For example, to change to the status propagation display mode, use the option `OPC_OWN_DISPLAY STATUS_PROPAGATE`. See "Types of Ownership Display Modes" on page 70 for the available options.
2. Reload the configuration of any connected Java GUI. (See the *HPOM Java GUI Operator's Guide*.)

Types of Default Ownership Modes

The administrator sets 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`.

Enforced User *must* take ownership of messages. Use the option `OPC_OWN_MODE ENFORCED`.

Informational Concept of ownership is replaced with that of marking and unmarking. A marked message indicates that an operator has taken note of a message. Use the option `OPC_OWN_MODE INFORM`.

About the "Optional" Ownership Mode

In **optional** 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 mode, only the owner of a message may do the following:

- **Actions**

  Perform operator-initiated actions related to the message.

- **Acknowledgement**

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

About the “Enforced” Ownership Mode

In enforced ownership mode, either an operator chooses explicitly to take ownership of a message, or the operator 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 attempts to do the following with the message:

- **Actions**

  Perform operator-initiated actions relating to the message.

- **Unacknowledgement**

  Unacknowledge the message (that is, move the message from the history database to the active database).

About the “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, informational mode does not restrict or alter operations on the message. Operator may unmark only those messages they themselves have marked.

Configuring Message Ownership Mode

The HPOM administrator can choose a message ownership mode to determine the message ownership policy.

To specify a message ownership mode, enter the following:

```
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.

Configuring Message Ownership Display Mode

The HPOM administrator can choose the ownership display mode to determine the way in which message ownership is displayed.

To change the message ownership display mode:

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

Where *<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 OPC_OWN_DISPLAY NO_STATUS_PROPAGATE.

About Policy Groups

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

Default Policy Groups

Default policy groups are provided with the HP Operations management server. To get a list of policy groups, run the following command:

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

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

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

About Default Users

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

Types of Default Users

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.

HPOM Default User Names and Passwords

For a list of default user names and passwords for all preconfigured users, see Table 2-2 on page 75.

Table 2-2 HPOM User Names and Passwords

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

About the HPOM Administrator

HPOM supports only one HPOM administrator, whose responsibility is to set up and maintain the HPOM software. The HPOM administrator's login name, `opc_adm`, cannot be modified.

For detailed information, refer to the *opccfguser* man page.

Types of Default Operators

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*.

Types of Default Node Groups

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	✓		✓
Solaris	✓		✓
Net Devices		✓	✓

Types of Default Message Groups

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	✓	✓	✓
SSP	✓		✓

The messages each operator receives and the nodes those messages come from are not necessarily the same. The responsibility matrix chosen by the administrator 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 the administrator makes in a given operator's responsibility matrix.

Types of Default Application Groups

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		✓	✓

Types of Default Applications

The applications and application groups assigned by default to the HPOM users reflect the responsibility given to them by the administrator.

Table 2-6 on page 78 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. The administrator can use the default settings as a base for configuring users and responsibilities that match the needs of individual environments. For more information on managing applications, see the *opcappl(1m)* man page.

Table 2-6 Default Applications for Operators

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

About 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		✓
SSP Tools		✓
UN*X Tools		✓
X-OVw		✓
Broadcast	✓	
HPOM Status	✓	

About the "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 is required because the application is started through the HPOM action agent.

- **Windows**

  Default User: **opc_op**

  Default Password: None is required because the application is started through the HPOM action agent.

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

About the "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.

About the "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 NNM cannot be installed on the same system as the HPOM management server.

Correlating Events

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:

     ```
     # 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, see *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.

Encapsulating Logfiles

For detailed information about logfile encapsulator, refer to 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.

For details about which logfiles are monitored by default, see logfile policies. Use the following command:

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

You can edit the existing and configure the new logfile policies by editing 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*.

Intercepting SNMP Traps and Events

For details about which traps are intercepted by default, see the SNMP trap policies. Use the following command:

```
# 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.

Types of Traps that Can Be Intercepted

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

Resolving Localhost IP Addresses

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.

If you want intercepted traps of this type to be forwarded 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:

Use the `ovconfchg` command-line tool as follows:

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

Intercepting Distributed Events

HPOM Distributed Event Interception 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.

Configuring HPOM Distributed Event Interception

HPOM Distributed Event Interception has two configurations:

- **Basic Configuration**

  To set up the basic configuration, follow these 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, perform the following on HTTPS-based managed nodes:

Use the ovconfchg command-line tool as follows:

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

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

❑ **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 Events with Event Correlation Services

By default, opctrapi connects to the correlated event flow of pmd.

You can change this behavior by using the ovconfchg command-line tool on managed nodes as follows:

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

where:

CORR	Correlated event flow (the default).
RAW	Uncorrelated event flow. This flow does not contain events created by correlations.
ALL	CORR plus RAW minus any duplicates.

The correlated event flow (CORR) is further divided into streams.

opctrapi connects to the default Event Correlation Services (ECS) stream of pmd (default). If necessary, you can configure opctrapi to connect to a specific ECS stream of pmd by performing the following on managed nodes:

Use the ovconfchg command-line tool as follows:

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

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

Intercepting HPOM Messages

By default, any message submitted through the `opcmsg(1)` command or through the `opcmsg(3)` API is intercepted. For message attribute defaults, logging options and so forth, see the `opcmsg(1|3)`.

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

Monitoring Objects

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`	Monitors the software distribution process. Generates a message for each pending distribution.	1	10m
`mondbfile`	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

Monitoring MIB Objects from Other Communities

You can monitor MIB objects from communities other than `public`. To monitor these communities, perform the following on HTTPS-based managed nodes:

Use the `ovconfchg` command-line tool as follows:

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

In this instance, `<community>` is the community for which the `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, see the *opcnotiservice* and *opctt* man pages.

About 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 9.00 management server, and are organized in a tree-like structure. See “Policy Versioning” on page 96 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 to Managed Nodes” on page 187.

Policy Files Naming Schema

Policy files must adhere to the following rules:

- *Policy header*

  `<uuid>_header.xml`

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

- *Policy bodies*

  `<uuid>_dataX`

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

  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 *opcpolicy (1M)* and *opccfgupld (1M)* man pages for usage details. 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.

See *opcpoltype (1M)* man page for usage details. 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.

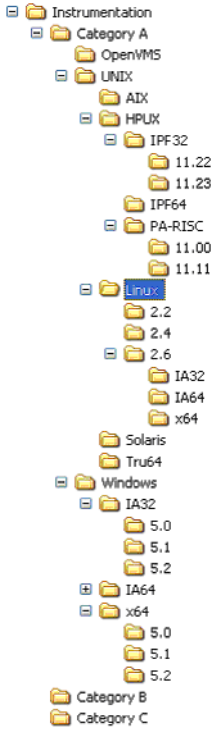
The following is an example of the XML registration file:

```
<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 92 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>

Policy types can be listed using the `opcpoltype -list` command. Deassigning policies is performed using options `-del_from_group` (for `opcpolicy`) and `-deassign_pol` (for `opcnode`).

To list the contents of a policy group, enter the following:

opcpolicy -list_group pol_group=<policy_group_name>

Retrieving list of policies assigned to a managed node is performed 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
```

See *opcpolicy (1M)* and *opcnode (1M)* man pages for usage details.

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.

See the *opcragt (1M)* man page for usage details.

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 a policy group ”Test group” use the following command:

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

For detailed information, refer to the *opcpolicy(1M)* man 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
```

See *opcpolicy (1M)* man page for usage details.

Modifying Policies

Editing Policies

While default policy types delivered with HPOM 9.0 have their editors defined, a different editor can be defined for custom policy types during registrations.

You can define a generic editor for policies of each policy type.

The editor can be specified during the policy type registration with the **`opcpoltype -reg -editor`** command, see “Registering Policy Types” on page 90.

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 see the *opcpoltype(1M)* man page.

As an administrator, you 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. See *opcpolicy (1M)* man page for usage details. 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 *opcpolicy (1M)* man page.

Changing Policy Syntax Versions

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

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

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 have to do that before the next deployment, otherwise, the policy will be deployed with an old syntax version.

See the *opcpolicy (1M)* man page for usage details.

Policy Versioning

With HPOM 9.00, it is possible to have multiple versions of policies stored on the management server. Having multiple versions of policies on the HPOM 9.00 management server enhances the flexibility in operating with policies and policy groups, and allows simplified interoperability between HPOM for Unix and Windows platforms.

For conceptual information about policy versioning and the policy group hierarchy organization, refer to the *HPOM Concepts Guide*.

Changing the Policy Version

All policies have version numbers. The policy version can be replaced according to your preferences by using the `opcpolicy` command line utility. 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)* man page for usage details. 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 9.00 Policies

The migration of templates to policies, which also includes the conversion of template groups to policy groups, is performed by using the `opccfgupld` utility. Consider the changes in the directory structure used for the upload and the download:

- *HPOM 8.xx*

  <upload_path>`/TEMPLATES/*`

  (also includes *<upload_path>*`/TEMPLATES/TEMPLGROUPS`)

- *HPOM 9.00*

  <upload_path>`/POLICIES`

  and

  <upload_path>`/POLICYGROUPS`

Refer to the *opccfgupld (1M)* man page for usage details.

During the standard HPOM policy checksum comparison it may happen that these 1.0 policies are identical, and the upload is skipped. In case the policies of the same version are different, the uploaded policy replaces the policy in the database if the `-replace [-`*<subentity>*`]` option of `opccfgupld` is used.

Updating Policy Assignments

Policies can be assigned to nodes, node groups, and policy groups. A basic difference between HPOM 8.xx and HPOM 9.00 is that the modification of the policy leads to a new policy version in HPOM 9.00, 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 9.00 inroduces 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* man pages for usage details.

Policy Assignment Tasks in HPOM

Table 2-9 lists policy-related tasks and operations provided with HPOM version 8.xx for Windows and HPOM for Unix versions 8.xx and 9.00. 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 for Windows and Unix

		HPOM 8.xx for Windows Policies		HPOM 8.xx for Unix Templates		HPOM 9.00 for Unix Policies	
		New	Existing	New	Existing	New	Existing
Create		✔		✔		✔	
Deploy		✔	✔	✔	✔	✔	✔
Assign				✔		✔	
Update assignments							✔
Modify	Create new version		✔				✔
	Overwrite				✔		✔

About 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 Timeouts 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*.

Create and Integrate a New Report

Although HPOM provides a comprehensive set of default reports, you may want to customize one of them, or create and integrate new reports.

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 configuration file.

The configuration of a new report is done by either creating a new script or 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 for the administrator and which are for the operator.

1. Access 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. New reports must have the ending `.sql` and must be contained in this directory.

3. Test the new or modified report from the command line:

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

   where <*name*> is the name of the report file without the `.sql` ending, and <*parameter*> is an optional parameter passed to the report.

4. Choose the configuration file (`oper.rpts` or `admin.rpts`) to enter details about your new report. The `.rpts` file contains a definition for each report. The syntax of this definition is defined as follows:

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

   A PGM report (SQL*Plus or program) may look like this:

   ```
   REPORTNAME      Active Message
   REPORTTYPE      PGM
   DESCRIPTION     Report about one selected active message
   ```

```
REPORTFILE      /opt/OV/bin/OpC/call_sqlplus.sh sel_actmsg
PARM            $message_active

REPORTNAME      History Message
REPORTTYPE      PGM
DESCRIPTION     Report about one selected history message
REPORTFILE    /opt/OV/bin/OpC/call_sqlplus.sh sel_histmsg
PARM            $message_history

REPORTNAME      System.txt Logfile Report
REPORTTYPE      PGM
DESCRIPTION     Review of System.txt logfile
REPORTFILE      /bin/cat
PARM            /var/opt/OV/log/System.txt
```

HPOM supports 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
```

5. Save the appended `.rpts` file with the same name in the same directory.

Types of Preconfigured Administrator Reports

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.
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).

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

Report Name	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.
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 polocies. 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.

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

Report Name	Description
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 $OPC_HOME, if set, $HOME, or `/tmp` in that order. All files that are created when the administrator saves report output are owned by the administrator’s UNIX user, which may be but does not need to be the root.

Types of Preconfigured Operator Reports

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.

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

Report Name	Description
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.
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 $OPC_HOME (if set), $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.

About 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.

Configuring Flexible Management Policies

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:

CONDSTATUSVARS

Conditions status variables. For details, see “About Status Variables for Conditions” on page 124.

RESPMGRCONFIG

Responsible manager configuration.

DESCRIPTION

Short description of the manager.

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.

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.

MSGTARGETRULES

Message target rules.

MSGTARGETRULE	Rule to configure the message target conditions and the message target manager.
DESCRIPTION	Description of the message target rule.

MSGTARGETMANAGERS

Message target managers. 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`

Message target rule conditions.

`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. Can be Unknown, Normal, Warning, Minor, Major, 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"`
`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.
`SERVICE_NAME`	A string containing the unique identifier of the service. Pattern-matching may be used.
`MSGOPERATION`	Message operation: • Suppress • Log-only • Inservice For details, see Table 2-13.

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.

More Information about Syntax Examples

For more information about the policy syntax for flexible management policies, see the man 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 in Flexible Management Policies

The syntax examples below use the following special characters:

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

Example: `e`

`#` — Comment. If you want to include a comment in a policy, include a pound sign (`#`) before 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 <string>[1] |
                   <mtrcond> SERVICE_NAME  <string> [1]|
                   <mtrcond> MSGCONDTYPE  <msgcondtype> | e
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>
```

1. Pattern-matching is only available with TEXT and SERVICE_NAME.

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>/*
```

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 Management Responsibility Switching Policies

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

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

Syntax for Message Target Rules Policies

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 Policies

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 Policies

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
timetmplconds[1] ::= <timetmplconds> TIMETMPLCOND <timetmplcond>
timetmplcond   ::= [TIMECONDTYPE <timecondtype>] [TIME FROM
```

1. Outages only.

```
                    <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>/*
```

Syntax for service hours and scheduled outages:

```
respmgrconfigs  ::=  <respmgrconfigs> RESPMGRCONFIG[1]
                     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 <string>[2]  |
                      <mtrcond> SERVICE_NAME <string> [1]  |
                      <mtrcond> MSGCONDTYPE
                      <msgcondtype>  |  e
bool            ::=  True  | False
severity        ::=  Unknown  |  Normal  |  Warning
                     |  Critical | Minor  |  Major
msgcondtype     ::=  Match  |  Unmatch
nodelist        ::=  <node>  |  <nodelist>  <node>
node            ::=  IP  <ipaddress>  |  IP  <ipaddress>
```

1. Only one RESPMGRCONFIG (responsible manager configuration) is supported in scheduled outage configuration files.
2. Pattern-matching is only available with TEXT and SERVICE_NAME.

```
                        <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.

About Scheduling Policies

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

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

- It is NOT forwarded to troubleticket.
- No automatic actions are triggered by the HP Operations management server.
- The messages are used for message correlation. 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 118 and “Syntax for Service Hours and Scheduled Outages Policies” on page 119.

Location of Service Hours and Scheduled Outages Policies

The policy for service hours and scheduled outages is located in the following directory:

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

Before making any changes, copy the file to the working directory:

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

After the policy file is ready for use, move it to the following directory:

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

Then start a new HPOM session so the new configuration can be read and implemented.

NOTE You may not change policy names. HPOM looks for specific policy file names. To find out more about how to set up policies for service hours and scheduled outages, see the “Syntax for Service Hours and Scheduled Outages Policies” on page 119

Parameters for Service Hours and Scheduled Outages Policies

Table 2-13 on page 122 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	If the message condition matches, and the time policy condition does *not* match, HPOM sends messages to the Pending Messages Browser, where they remain until the **unbuffer** time condition is matched or until the message is unbuffered manually.
LOGONLY	Send a matching messages to the history browser.
SUPPRESS	*Deletes* messages. Message-related actions triggered by the HP Operations 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 trouble ticket
- ❏ Forward to 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 Policies” on page 119.

About 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.

About the Time Zone String

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.

Syntax for the Time Zone String

The following example illustrates the syntax 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.

About the 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:

```
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
```

About the Policy for Message Forwarding

HPOM enables you to generate notification messages to be sent to remote management servers. And it enables you to assign control of the messages to the source management server with one policy. You can check the policy using the tool `opcmomchk`.

Location of the Message Forwarding Policy

HPOM stores the message forwarding policy in:

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

NOTE For all MoM 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:

- **Targets**

  You can assign a message to multiple target servers.

- **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.

- **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.

- **Acknowledgement**

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

Attributes of the Message Forwarding Policy

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, see the man page *opcmom(4)*.

Setting Parameters for the Message Forwarding Policy

As an HPOM administrator, 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.

Table 2-14 Message Forwarding Parameters (Continued)

Parameter Name	Default Value	Description
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.
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.

Table 2-14 Message Forwarding Parameters (Continued)

Parameter Name	Default Value	Description
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.

These example policies are located in the following directory:

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

To define message-target rules:

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`
   `Suppress`

4. Define the message attributes in the subsection, `MSGTARGETRULES`. You can define the following attributes:

   Severity, Message group, Application, Object, Node, Message type, Message text, Service name.

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 ensure that your changes are correct:

   ```
   /opt/OV/bin/OpC/opcmomchk file_name
   ```

   See the man page *opcmomchk(1)* for more information.
8. As user root, copy the validated file to the configuration directory:

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

About HTTPS-Based Event Forwarding Between Multiple Management Servers

HPOM uses HTTPS-based communication for forwarding 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, establish a trust relationship between the HP Operations management servers that will be communicating directly.

For setting up trust relationships between HP Operations management servers, refer to the section titled *Certificate Handling for a Second HPOM Management Server* in the *HPOM HTTPS Agent Concepts and Configuration Guide*.

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

NOTE

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 timeouts 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 133 let you configure different aspects of event forwarding. See “Descriptions of Forwarding Configuration Parameters” on page 133 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 timeouts and will not be delivered to remote servers (seconds)

Descriptions of 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 133 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

If, for some reason, removal of all buffered messages is required, perform the following steps:

1. Stop the HP Operations management server processes:

   ```
   ovc -stop OPC
   ```

2. Remove the directory in which the forward manager stores buffer files:

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

3. Start the HP Operations management server processes:

   ```
   ovc -start OPC
   ```

About 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 continually at one minute intervals. Wildcard characters are not recognized.

Examples of Time Policies

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

- **No 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.

- **Specific Days or Dates**

  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 Dates*

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

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

- *Time Periods*

  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 like `DATE FROM 05/07/08 TO 10/10/*`.

For further examples of time policies, see the following:

❏ “Syntax for Time Policies” on page 118

❏ man page `opcmom(4)`

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

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 for Time Policies

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

`TIMETEMPLATE <string>`

Policy name is contained in `<string>`.

`DESCRIPTION` Short description of the time policy.

`TIMETMPLCONDS` `TIMETMPLCOND`

`TIMECONDTYPE` Condition defining 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.

At least one of the following parts must be used for the definition:

- *Match*
- *Suppress*

If the current time is within the defined time period, *match is true* and *suppress is false*.

HPOM does not interpret either of these parts as “always.”

`TIME FROM <time> TO <time>`

Specifies a time period. Set the variable `<time>` using the format:

`<HH>:<MM>`

The `FROM <time>` variable must be before the `TO <time>` variable (for example, `FROM 18:00 TO 24:00` or `FROM 0:00 TO 6:00`).

WEEKDAY	You can specify every day of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday: • ON <*day*> Day of the week (for example, ON Sunday). • FROM <*day*> TO <*day*> Time period (for example, FROM Monday TO Wednesday).
DATE	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*>

Examples of Flexible Management Policies

This section provides a number of example policies that illustrate a simple implementation of selected flexible management features.

Example of Management Responsibility Switch Policy

The following example policy defines management responsibility switching.

```
#
# 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"
```

Example of Follow-the-Sun Responsibility Switch Policy

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"
```

Example of 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 does the following:

- **Forward Messages to Expert Center**

  Forward messages with 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.

- **Inform Treasury Server**

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

- **Inform 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 Hours

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
```

Example of Scheduled Outage Policy

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
```

About 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 surround the variable with quotes, especially if it may 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. HPOM variables are reserved words. That is to say, they must not be used for any other purpose (such as creating user-defined variables).

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

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>
```

To Set Personal Environment Variables

Personal environment variables can be set in the script file `HomeDirectory/.dtprofile`.

1. Edit `HomeDirectory/.dtprofile`
2. Add lines to the file to set the environment variable

The desktop will accept either sh or ksh syntax for the commands in this file. The commands should only be those that set environment variables, not any that perform terminal I/O, ex. **`tset`** or **`stty`**.

NOTE

By default, the files `HomeDirectory/.profile` and `HomeDirectory/.login` are NOT read by the desktop, as they may contain terminal I/O based command inappropriate for a graphical interface. These files ARE read if the last line of `.dtprofile` is uncommented; the line 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 (from `/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 (from /etc/passwd)
TERM	Set to dtterm
TZ	Set to the system's zone or to the value of the Dtlogin ``timeZone`` resource

About 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

$OPC_HOME

Returns the working directory of the user who starts a HPOM GUI session. If $OPC_HOME is not set, the working directory is /tmp. If the UNIX user that started the HPOM GUI has no write permission in /tmp, an error message is displayed but the GUI still starts. Example: export OPC_HOME=$HOME/opc

About 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. This means, that most configuration variables that are 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

About Variables in All 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, the *opcmsg* or *opcmon* man page.

NOTE

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

Resolving Variable Values 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 they are matching. The order in which the variable values are determined is as follows:

1. Value set by the external source (API/executable, event, and so on). For example, if the following `opcmsg` command is called:

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

   The variable `<$MSG_APPL>` is assigned the value APP.

2. Values for some variables can not be set by external sources and are internally generated by HPOM, for example, message ID.

3. If none of the above is valid for a variable, that variable uses the value set in the policy body for which the variable is evaluated. If there is no default value set, the value of that variable is empty or 0, depending on its type.

The above order is strictly adhered to when resolving variable values. For example, if a value for `<$MSG_OBJECT>` is set in step 1, a default value set in the 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 MS WINS (Windows Internet Name Service). 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 (Jan 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 pmd's machine 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 to Be Used in 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 details, refer to the *opcinstrif(1m)* man 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 170

❏ "Examples of Message-Related Variables" on page 179

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. Note, 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 or not 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.com
```

`$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.

- **Accessing 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]
  ```

- **Finding Duplicate Messages**

  If you need information about the number of message duplicates for an application, you would use the following:

  ```
  $OPC_MSG.DUPLICATES
  ```

- **Extracting Creation Time and Severity**

  If want to do some statistical calculations, you would specify the message creation time and the severity, as follows:

  ```
  $OPC_MSG.CREATED
  ```

  ```
  $OPC_MSG.SEVERITY
  ```

- **Extracting 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]`.

- **Evaluating 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.

- **Accessing Annotations**

  To access the second annotation of a selected message in an application, you would use the following:

  `$OPC_MSG.ANNOTATIONS[2]`

3 Installing and Updating the HPOM Configuration on the Managed Nodes

In this Chapter

This chapter describes how to install and update the HP Operations Manager (HPOM) configuration on the managed nodes.

Distributing the HPOM Agent Configuration to the Managed Nodes

After customizing the configuration and assigning policies to managed nodes, distribute the managed node configuration by using the `opcragt` command line tool. 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, refer to the *opcragt (1M)* man page.

Before Distributing Instrumentation to the Managed Nodes

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 logfile 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:

- **Not Already Installed**

  Instrumentation files are available on the management server, but are not already installed on the managed node.

- **Newer Versions Available**

  Newer versions of instrumentation files are available on the management server than on 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 186.

❑ **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 191 for more information). For description of categories and the distribution method based on them, see “Category-Based Distribution of Instrumentation to Managed Nodes” on page 187.

❑ **Distribution Process opcbbcdist**

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. For 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 to Managed Nodes” on page 187 for more information about categories. For details on Selective Distribution Feature, see “Selective Distribution of User-selected Files to Managed Nodes” on page 198.

Distribution Methods

Depending on the scope of contents you want to be distributed, and on the selection of managed nodes where you want the data to be distributed, there are few distribution methods. If you decided to:

- Distribute entire instrumentation to each specified managed node, choose one of the following (*the first is recommended*):
  - **“Category-Based Distribution of Instrumentation to Managed Nodes” on page 187**.
    To complete your task, see “Before You Distribute Instrumentation Data” on page 191.
  - **“Distribution of Instrumentation from Monitor, Actions and Commands to Managed Nodes” on page 195**.
- Distribute only specified user-selected files to a particular managed node, choose one of the following (*the first is recommended*):
  - **“Category-Based Distribution of Instrumentation to Managed Nodes” on page 187**.
    To complete your task, see “Before You Distribute Instrumentation Data” on page 191.
  - **“Selective Distribution of User-selected Files to Managed Nodes” on page 198**.

Category-Based Distribution of Instrumentation to Managed Nodes

This section describes the distribution of instrumentation to managed nodes based on **categories**. Category is a concept upon which the related instrumentation files are configured into a logical unit.

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 due to the multilevel 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 filesystem and on the database level by means of the `opcinstrumcfg` command-line utility. See *opcinstrumcfg(1M)* man page for usage 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 as follows:

- *On the HPOM management server:*

  The directory for executables on the HP Operations management server is located in:

  `/var/opt/OV/share/databases/OpC/mgd_node/`

If no categories are created, the instrumentation data from the directories actions, commands, and monitors is anyway deployed, as described in the “Distribution of Instrumentation from Monitor, Actions and Commands to Managed Nodes” on page 195.

When the categories for the instrumentation files are created, the `instrumentation` directory is also created automatically, along with 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/` is deployed, including the contents of the `monitor|actions|cmds` directories. However, if there are files with the same filenames in both `monitor|actions|cmds` and within the created categories, the files organized in categories are distributed.

The subdirectory structure under the `instrumentation` directory is defined as follows:

`$InstrumDir/<category>/<OS_family>/<OS_type>/\`
`<cpu_type>/<OS_version>`

Or,

`$InstrumDir/<category>/<OS_family>/<OS_type>/\`
`<OS_version>/<cpu_type>`

Where the values for the above stated selectors are the following:

`$InstrumDir` is `/var/opt/OV/share/databases/OpC/mgd_node/instrumentation` directory.

<OS_family>

Unix, Windows

<OS_type>

Windows, Linux, HP-UX, Solaris, AIX, Tru64, and OpenVMS

NOTE

Windows and OpenVMS have only one directory level for OS family and OS type, since they are identical. 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>

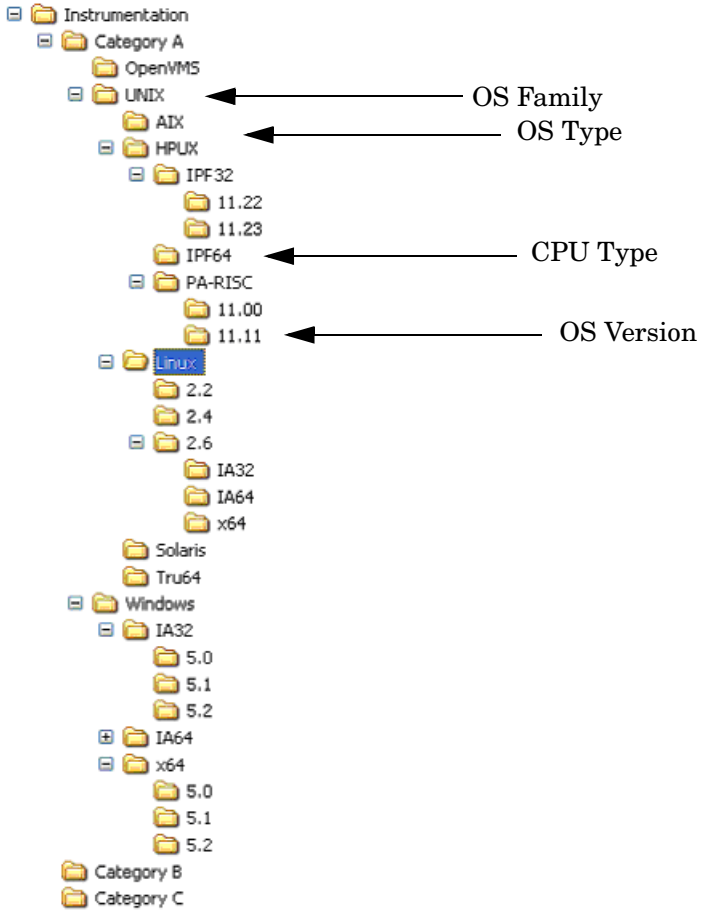
All agent OS versions supported by HPOM 9.00. Refer to *HPOM Software Release Notes* for more information.

NOTE

The OS version directory can be either 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 filesystem.

Figure 3-1 on page 190 shows the instrumentation directory structure on the HPOM management server.

Figure 3-1 Instrumentation Directory Structure on the HPOM Server



❑ *On the HPOM managed nodes*

On HPOM managed nodes, all deployed instrumentation data (category-based instrumentation, as well as the `monitor|actions|cmds` files) is located in the following directory:

`/var/opt/OV/bin/instrumentation`

Before You Distribute Instrumentation Data

Consider the following before you start the distribution process:

- 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 at an appropriate location under the category you have created for this purpose. For example, if you want to be deployed only the instrumentation related to IPF32 11.23 under a category `Custom`, perform the following procedure:

NOTE

For more information on how to perform each individual step, see the section “Preparing Instrumentation for Distribution using Categories” on page 192.

1. Create the `Custom` category.
2. Place the instrumentation files at the following location:

   `$InstrumDir/Custom/Unix/HP-UX/IPF32/11.23/`

3. Assign the category `Custom` to the appropriate managed nodes, and/or to the appropriate policies.
4. Start the distribution process using the `opcragt` command-line utility with the `-instrum` option. See “Distributing Instrumentation Data” on page 194 for more information about the distribution process.

Preparing Instrumentation for Distribution using Categories

To prepare instrumentation data for the distribution using categories, perform the following:

1. Create categories for the instrumentation you want to distribute. This can be done in several ways:

   - By using the `opcinstrumcfg` utility, enter:

     `opcinstrumcfg -add <categoryA>,<categoryB>`

     Note that comma-separation is used between categories, since the category names can contain blank characters.

     The `opcinstrumcfg` utility enables you to manage categories both on a filesystem and on a database level. Refer to the *opcinstrumcfg (1M)* man page for more information.

   - By using the `opcpolicy` utility, enter:

     `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 filesystem.

`opcpolicy` is the symbolic link and therefore equivalent to the `opctempl` command line utility, and is used for managing policies. Refer to the *opcpolicy (1M)* man page for usage parameters. For additional information about policies, refer to the *HPOM Concepts Guide*.

   - By using the `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)* man pages.

2. Place the instrumentation data at an appropriate location within the instrumentation subdirectory structure.

To complete this task, see the sections "Before You Distribute Instrumentation Data" on page 191 and "Instrumentation Data Directory Structure" on page 187.

3. Assign the created categories. Categories can be assigned to the target managed nodes, and/or to the appropriate policies, as follows:

   - *Assign the categories to the managed nodes* by using the `opcnode` command line utility:

     ```
     opcnode -assign_cat node_list=<node_list>\
     cat_list=<category_list>
     ```

     Refer to the *opcnode (1M)* man page for the usage details.

   - *Assign the categories to the policies* by using the `opcpolicy` command line utility.

IMPORTANT

To assign a category this way, make sure the following prerequisites are fulfilled:

— A category is assigned to a policy, for example `policyX`.

— This policy (`policyX`) is assigned to the target managed nodes.

Refer to the *HPOM Concepts Guide* and the section "About HPOM Policies" on page 89 to learn about the policy management.

Enter the following:

```
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 preferred policy version, otherwise it is assigned to all versions of this policy.

4. Start the distribution, as described in the "Distributing Instrumentation Data" on page 196.

Distributing Instrumentation Data

To distribute instrumentation data to managed nodes using the category-based distribution method, enter the following on the HPOM management server:

```
/opt/OV/bin/OpC/opcragt -distrib -instrum <node_name>
```

Where *<node_name>* is a name of the node to which you want to distribute the data.

NOTE

The `opcragt` command with the `-instrum` option deploys all instrumentation data, including the contents of the `monitor|actions|cmds` directories. However, if there are files with the same filenames in `monitor|actions|cmds` and in the `instrumentation` directory, the files from the `instrumentation` directory are used.

If the policies are updated with the required category assignments you can also start the distribution process as follows:

```
/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)* man page for distribution details.

Distribution of Instrumentation from Monitor, Actions and Commands to Managed Nodes

This section contains the recommendations and 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.

Distribution Tips for All Systems

- **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:

  ```
  /name/opc_op/scripts/my_ps
  ```

  ```
  my_ps
  ```

  You can call this script as an application from the Java GUI or as a broadcast command.

  In this example, the *$PATH* variable of the executing user on the managed node must contain the following:

  `/name/opc_op/scripts`.

Distribution Tips for UNIX Systems

When distributing scripts to managed nodes on UNIX systems, follow these guidelines:

- **Mixed Clusters**

  With mixed clusters, you must install the `monitor|actions|cmds` scripts and programs only once for each architecture type. For each architectural type, select one cluster node.

- **File Names**

  The file names of the `monitor|actions|cmds` binaries may 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.

Distributing Instrumentation Data

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 causing an increase in network load.

For information about the directories on the management server and the managed node, see “Directory Structure for Commands, Actions and Monitor Instrumentation Data” on page 197.

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.

Directory Structure for Commands, Actions and Monitor Instrumentation Data

The instrumentation data is organized as follows:

- *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
  ```

  Where `<arch>[/<comm>]` is the directory specific to the operating system and optionally the communication type of the node to which you want to distribute files.

  The files contained within the vendor tree:`/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 needed only if policies are assigned and distributed.

NOTE

Use the `customer` file if identical files for `actions|cmds|monitor` are found in the `customer` and `vendor` directories.

- *On the HPOM managed nodes*

  On HPOM managed nodes, all instrumentation data (category-based instrumentation, and the `monitor|actions|cmds` files) is located in the following directory:

  ```
  /var/opt/OV/bin/instrumentation
  ```

Selective Distribution of User-selected Files to Managed Nodes

This section describes the Selective Distribution feature of `opcbbcdist` using 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 “Directory Structure for Commands, Actions and Monitor Instrumentation Data” on page 197.

Normally, files are distributed which are not needed on a specific node. This problem 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|monitor` to specific nodes that do not belong to the node group associated with the SPI.

A configuration file `seldist` is provided in which node group names together with file name prefixes and files are listed. For details about `seldist` configuration file, see “The seldist Configuration File” on page 200.

The advantages of this distribution include the reduction of the following:

- ❏ disk space utilization on managed nodes
- ❏ network traffic during configuration file distribution

If selective distribution is *not* enabled, the standard distribution from monitors, actions and commands is performed. If you want to avoid distributing the entire instrumentation data, the category-based distribution method may be of avail to you, since it also allows you to distribute only specified user-selected files to a particular managed node.

See “Category-Based Distribution of Instrumentation to Managed Nodes” on page 187 for more information. See also “Distribution Methods” on page 186 to learn about the available distribution methods.

How Does Selective Distribution Work?

On starting configuration file distribution from the command line, `opcbbcdist` checks the selective distribution configuration and 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, every file from the customer `actions|cmds|monitor` 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 MoM environment, you *must* manually ensure synchronization of the `seldist` files on all of your HP Operations management servers.

Most Database SPI files have a `dbspi` prefix, SAP SPI files have an `r3` prefix, so an example of a SAP SPI binary would be named `r3perfmon`.

In addition to the preconfigured SPI-related files, you may 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 206.

The 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 read by `opcbbcdist` either on startup, or triggered by the `opcseldist` utility. For more information on the `opcseldist` utility, usage and command line options, see "The opcseldist Utility" on page 203 or refer to the *opcseldist(1m)* man page.

Selective Distribution is automatically enabled if the `seldist` file exists in the directory:
`/etc/opt/OV/share/conf/OpC/mgmt_sv/`

When the distribution of actions, commands or monitors is started, Selective Distribution in accordance with the requirements of the `seldist` file is started.

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 node group plus a list of files and file prefixes that belong to this SPI. You must add all managed nodes that need these files to this node group.

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|commands|monitor` as only certain "known" files are blocked from distribution to nodes that do not belong to a specific group of nodes.

Example of a policy configuration file

A policy configuration file, `seldist.tmpl`, contains all currently known SPIs with proposed node group names. To use this Selective Distribution policy, you *must* copy the file to `seldist`. For more information, see the section "Enabling Selective Distribution Using the Supplied SPI Configuration File" on page 204.

Here is an example extracted from the `seldist.tmpl` 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 is as follows:

- Text after a hash (`#`) is treated as a comment and is *not* evaluated.
- In all uncommented lines, only the first two words are evaluated:

  `DBSPI dbspi`

  `sap r3`

The first word represents the node group name, for example `DBSPI` and `sap`, and 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 stand for `ntwdblib.dll.old`.

- The same node group can be specified several times and thus it is possible to specify multiple prefixes, file names, or both for the same node group.
- The same prefix can be specified for several node groups. This is the case where several SPIs may share a common subset of files. An example is the PeopleSoft SPI which ships certain DBSPI files that are used on a PeopleSoft database server.

  The relevant lines of the `seldist` file are:

  ```
  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 even possible specify prefixes that are subsets of each other.

NOTE

Any files that do not display in the `seldist` file or do not match any of the listed prefixes, will always be distributed to all nodes, in the same way as they would be distributed to all nodes if the `seldist` functionality is not enabled.

- To use node groups with spaces, put them in double quotes in `/etc/opt/OV/share/conf/OpC/mgmt_sv/seldlist` file.
  If a node group does not contain spaces, quoting is not necessary.

  For example:
  `"node group 1" prefix1`
- Node group names may be localized.

The opcseldist Utility

The `opcseldist` utility is a syntax check tool for `seldist` configuration files. It can also be used to send a re-configuration request to `opcbbcdist`.

The `opcseldist` utility has the following command line options:

- `-check <filename>`, which checks the syntax of the specified file
- `-reconfig`, which sends the re-configuration request to `opcbbcdist`

If the syntax of the configuration file is not correct, `opcseldist` will display a list of corresponding errors. If there are errors in a `seldist` file, for example, a node group is specified without a file name prefix, and the file is used to manage distribution, the distribution manager evaluates the `seldist` file up to the error. The rest of the file is ignored. This can result in distribution of more files than intended.

A re-configuration request to `opcbbcdist` is accompanied by a request status message.

Enabling Selective Distribution Using the Supplied SPI Configuration File

To enable Selective Distribution using the supplied SPI configuration file, perform the following procedure:

1. Create node groups for the nodes to which you want to distribute your actions, commands and monitors. Most SPIs already come with default node groups for their specific configurations but you may use a different node group and change the `seldist` file accordingly.

NOTE

The `Node Group Name` that has to be used in the `seldist` file. The `Node Group Label` can be freely used, for example, localized.

2. Add all nodes that should have the SPI files distributed to the node group.
3. Change directory to the location of the configuration policy:

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

4. Make a copy of the `seldist.tmpl` file where you are to make your changes:

   `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.

NOTE

To avoid confusion, check the configuration sections for all SPIs that you do not have installed. Make sure that you do not have a node group with the same name as one listed in the `seldist` file but has nothing to do with the `seldist` feature. If necessary, disable the configuration section for SPIs you do not have installed by preceding with a `#` comment sign.

6. Save the configuration file and check the syntax:

   `/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`:

   `/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 -reconfig` utility.

For more information on the `opcseldist` utility, usage and command line options, see “The opcseldist Utility” on page 203 or refer to the *opcseldist(1m)* man page.

8. Distribute the `actions|cmds|monitor` binaries by using the `opcragt` command line interface.

NOTE

If you have previously distributed all SPI `actions|cmds|monitor` to all nodes, and you now want to remove unnecessary binaries from these nodes, you can perform the following:

- On HTTPS-based managed nodes, run a distribution using the `opcragt` command with `-purge` option. However, note that if you are distributing the instrumentation from several HP Operations servers, the `-purge` option removes the whole instrumentation from the nodes (even if the instrumentation has been distributed from another HP Operations server).

Disabling Selective Distribution

If you do not want Selective Distribution of `actions|cmds|monitor`, you can disable Selective Distribution by performing the following steps:

1. Change directory to the location of the configuration file:

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

2. Rename the `seldist` file, for example

   `mv seldist seldist.old`

3. If the server processes are currently running, run:

   `/opt/OV/bin/OpC/utils/opcseldist -reconfig`

Configuring Custom Selective Distribution

The default `seldist` file currently contains all known SPIs with proposed node group names 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|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, complete the following steps:

1. Edit the `seldist` file and create a new configuration section including:

   - The node group you assign all the nodes that should receive the files below.
   - File names, prefixes, or both of the files you want to distribute.

   See “The seldist Configuration File” on page 200 for syntax rules that must be observed.

2. Run the `opcseldist -check` command to check the syntax rules and correct any syntax errors if reported:

   `/opt/OV/bin/OpC/utils/opcseldist -check seldist`

3. Add the nodes to which you want to distribute files to the node group.

4. Run the `opcseldist` utility to re-configure `opcbbcdist` as follows:

   `/opt/OV/bin/OpC/utils/opcseldist -reconfig`

4 HP Performance Agent

In this Chapter

This chapter describes HP Performance Agent.

About Other Platforms

HP Performance Agent is provided on separate installation package and is *not* deployable from HPOM.

Each platform has its own installation and configuration guide.

NOTE For list of managed node platforms and operating system versions that are supported by HP Performance Agent, see the *HPOM Software Release Notes*.

About HP Performance Agent

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.

Integrating Data 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.

Analyzing Data 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.

Logging Data with HP Performance Agent

The comprehensive data logged by HP Performance Agent enables you to do the following:

- ❏ Characterize the workloads in the environment.
- ❏ Analyze resource usage for load balancing.
- ❏ Perform service-level management based on transaction response time.
- ❏ Perform capacity planning.
- ❏ Respond to alarm conditions.
- ❏ Solve system management problems before they arise.

Customizing HP Performance Agent

HP Performance Agent gathers comprehensive and continuous information on system activity without imposing significant overhead on the system. Its design offers considerable opportunity for customizing. You can accept default configurations or set parameters to collect data for specific conditions.

Installation Requirements

This section describes the system requirements for installing HP Performance Agent on a managed node.

- **Hardware and software requirements**

  See “Hardware and Software Requirements” on page 213 for more information.

- **Supported managed node platforms**

  For list of managed node platforms that are supported by HP Performance Agent, as well as the requirements for installing HPOM on the management server, see the *HP Operations Manager Software Release Notes*.

- **HP Performance Agent in other languages**

  HP Performance Agent is language-independent and can run on any supported system. Manuals are provided in both English and Japanese editions. See “HP Performance Agent Documentation” on page 226 for a list of manual titles.

- **Embedded performance component**

  HP Performance Agent and the embedded performance component can co-exist on the same system. However, if you do not require the embedded performance component, you can disable it.

Hardware and Software Requirements

Before installing HP Performance Agent, make sure your managed node platform meets the hardware requirements detailed in the *HP Performance Agent Installation and Concepts Guide*.

DCOM and IIS Setup for HTTPS Managed Nodes on Windows

Before installing HTTPS agents on Windows managed nodes, make sure that the following permissions are set for the Distributed Component Object Model (DCOM) and Internet Information Services (IIS):

- **DCOM**

  Local administrators must have both launch and access permissions.

  To configure launch and access permissions to DCOM, run `dcomcnfg`, and check the default permissions in the security settings.

  Refer to the `Readme.txt` file that is available with the HP Performance Agent installation packages for more information about DCOM setup.

- **IIS**

  Make sure that FTP access is available and you have write access as anonymous FTP or administrator user.

  To configure FTP write access to IIS, enable write access to the FTP site directory in the Computer Management module.

See the Microsoft Windows documentation for more information about configuring DCOM and IIS.

Installing and De-Installing HP Performance Agent

This section describes how to install and de-install HP Performance Agent on HPOM managed nodes.

Installing HP Performance Agent

You can install HP Performance Agent on supported managed nodes using the manual installation.

TIP For additional installation and configuration information, see the *HP Performance Agent Installation and Concepts Guide*.

HP Performance Agent installs into the following directories:

Table 4-1 HP Performance Agent Installation Directories

Managed Node Platform	Installation Directory	Data Directory
AIX	`/usr/lpp/perf`	`/var/opt/perf`
HP-UX 11.00, 11.11, 11.23	`/opt/perf`	`/var/opt/perf`
Linux	`/opt/perf`	`/var/opt/perf/`
Solaris	`/opt/perf`	`/var/opt/perf`
Tru64	`/usr/opt/perf`	`/var/opt/perf`
Windows	`<ProgramFilesDir>\HP\HP BTO Software`	`<ProgramFilesDir>\HP\HP BTO Software\data`

Manual Installation of HP Performance Agent

To install HP Performance Agent on a managed node or management server, follow these steps:

1. Make sure the selected temporary directory on the managed node contains the required disk space specified in the *HP Performance Agent Installation and Concepts Guide*.

   Install the depot `HPOvPADep-08.70.000-HPUX11.0-release.depot` on a HP-UX machine. Run the following command:

   ```
   # swinstall -x enforce_scripts=false -x
   enforce_dependencies=false  \
   -x   autoselect_dependencies=false -x
   allow_incompatible=false -x \ match_target=false \
   -s /tmp/HPOvPADep-08.70.000-HPUX11.0-release.depot  \*
   ```

   Ignore the following errors in the `swagent.log` file:

   ```
   * Installing fileset "HPOvPADep.HPOVPADAX,r=8.70.000" (1 of 6).
   ERROR:   opcsareg failed with exit code 127
   * Installing fileset "HPOvPADep.HPOVPADHP,r=8.70.000" (2 of 6).
   ERROR:   opcsareg failed with exit code 127
   * Installing fileset "HPOvPADep.HPOVPADLX,r=8.70.000" (3 of 6).
   ERROR:   opcsareg failed with exit code 127
   * Installing fileset "HPOvPADep.HPOVPADSN,r=8.70.000" (4 of 6).
   ERROR:   opcsareg failed with exit code 127
   * Installing fileset "HPOvPADep.HPOVPADWN,r=8.70.000" (5 of 6).
   ERROR:   opcsareg failed with exit code 127
   * Installing fileset "HPOvPADep.HPOVPAINT,r=8.70.000" (6 of 6).
   ```

NOTE The command `opcsareg` is not available anymore for subagent registration.

2. Install the subagent using the following command:

   ```
   # swinstall -s
   /var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/ipf3
   2/hpux1122/./C.04.70/ovpa_pkg.Z.B.11.31 \*
   ```

   To install the PA agent on a remote machine, first send the depot to the remote node using `ftp`. Make sure you take the depot out of the right OS directory:

   ```
   /var/opt/OV/share/databases/subagent/VP_Perf_Agt/ms/intel/nt/\
   C.04.70/ovpa_inst.exe
   /var/opt/OV/share/databases/subagent/VP_Perf_Agt/ms/x64/winxp/\
   C.04.70/ovpa_inst.exe
   /var/opt/OV/share/databases/subagent/VP_Perf_Agt/ms/x86/winnt/\
   ```

```
C.04.70/ovpa_inst.exe
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/ibm/rs6000/\
aix/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/ibm/rs6000/\
aix5/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/ia64/\
hp-ux11_32/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/ia64/\
hp-ux11_32/C.04.70/ovpa_pkg.Z.B.11.31
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/ipf32/
hpux1122/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/ipf32/\
hpux1122/C.04.70/ovpa_pkg.Z.B.11.31
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/pa-risc/\
hp-ux11/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/pa-risc/\
hp-ux11/C.04.70/ovpa_pkg.Z.B.11.23
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/pa-risc/\
hp-ux11/C.04.70/ovpa_pkg.Z.B.11.31
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/pa-risc/\
hpux1100/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/pa-risc/\
hpux1100/C.04.70/ovpa_pkg.Z.B.11.23
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/pa-risc/\
hpux1100/C.04.70/ovpa_pkg.Z.B.11.31
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/linux/intel/\
linux24/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/linux/intel/\
linux26/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/linux/ipf64/\
linux26/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/linux/x64/\
linux26/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/linux/x86/\
linux24/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/linux/x86/\
linux26/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/sun/sparc/\
solaris/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/sun/sparc/\
solaris7/C.04.70/ovpa_pkg.Z
/var/opt/OV/share/databases/subagent/VP_Perf_Agt/sun/x86/\
solaris10/C.04.70/ovpa_pkg.Z
```

After the installation is finished, you can check if the fileset installed correctly. For example, run the following command on HP-UX:

```
# swlist -l fileset MeasureWare
```

```
# MeasureWare            C.04.70.000    MeasureWare Software/UX
MeasureWare.MWA          C.04.70.000 MeasureWare Software files (IA)
MasureWare.MWALIC-SERVER C.04.70.000 Perf Agent License files (IA)
MeasureWare.PERFDSI      C.04.70.000 HP PCS Data Source Integration(IA)
```

HP Performance Agent Package and Installation Files

Copy the HP Performance Agent package and installation files to the `install/ovpa_inst` subdirectories before starting the installation. Package and installation files are available for the HTTPS-based managed nodes. For detailed information, see “HTTP Managed Nodes” on page 217.

HTTP Managed Nodes

- **HP-UX 11.0**

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/hp/pa-risc/hpux1100/C.03.72/ovpa_pkg.Z`

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/hp/pa-risc/hpux1100/C.03.72/install/ovpa_inst`

- **HP-UX 11.11**

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/hp/pa-risc/hpux1100/C.03.72/ovpa_pkg.Z.B.11`

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/hp/pa-risc/hpux1100/C.03.72/install/ovpa_inst`

- **HP-UX 11.23**

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/hp/ipf32/hpux1122/C.03.71.23/ovpa_pkg.Z`

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/hp/ipf32/hpux1122/C.03.71.23/install/ovpa_inst`

- **Sun Solaris**

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/sun/sparc/solaris7/C.03.82/ovpa_pkg.Z`

  `/<OVDataDir>/share/databases/subagent/VP_Perf_Agt\`
  `/sun/sparc/solaris7/C.03.82/install/ovpa_inst`

- **Microsoft Windows**

  - *unzip utility*

The unzip utility must be available on the node:

```
/<OVDataDir>/share/databases/subagent/VP_Perf_Agt/\
ms/x86/winnt/C.03.65/unzip.exe
```

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/ms/\
intel/nt/A.07.10/RPC_DCE_TCP/unzip.txt
```

- *HP Performance Agent*

  ```
  /<OVDataDir>/share/databases/subagent/VP_Perf_Agt\
  /ms/x86/winnt/C.03.65/ovpa_pkg.zip
  ```

  ```
  /<OVDataDir>/share/databases/subagent/VP_Perf_Agt\
  /ms/x86/winnt/C.03.65/install/ovpa_inst.exe
  ```

De-Installing HP Performance Agent

You can de-install HP Performance Agent from HPOM managed nodes using the standard or manual de-installation methods.

Standard De-Installation of HP Performance Agent

To de-install OVPA from a managed node using the standard installation method, run the following from the `/opt/OV/bin/OpC/agtinstall` directory:

```
product_inst.sh -r
```

The OVPA executable files are removed from the managed node. Configuration files and data files are *not* removed.

Manual De-Installation of HP Performance Agent

To de-install HP Performance Agent from a managed node using the manual installation method, follow these steps:

1. Copy the appropriate `ovpa_inst` file from the directories listed in "HP Performance Agent Package and Installation Files" on page 217 to a temporary directory of the managed node.
2. To remove the files, enter the following command on the managed node:
   a. Go to the directory containing the package and installation files copied from the HP Operations management server.
   b. Start the HP Performance Agent de-installation with the command:

      ```
      ovpa_inst REMOVE
      ```

See "To De-Install HP GlancePlus" on page 219 for more information about removing GlancePlus from the system.

To De-Install HP GlancePlus

The `ovpa_inst` script does *not* remove HP GlancePlus from the system. To remove GlancePlus, run the one of the following scripts, depending on your preferred mode:

- **Motif Mode Interface**

  UNIX ***<install_dir>*/bin/gpm.remove**

Windows `<install_dir>\bin\gpm.remove`

- **Character Mode Interface**

  UNIX `<install_dir>/bin/glance.remove`

  Windows `<install_dir>\bin\glance.remove`

Preconfigured Elements

This section describes preconfigured policies, policy groups, and applications used by HP Performance Agent on HP-UX and Sun Solaris managed nodes.

NOTE HP Performance Application bank functions are not available for Windows managed nodes. For Windows, only deploy and remove are available.

Types of Applications

There is one application group named `OV Performance`. You can select the following applications from the `Application Group: OV Performance` window.

Table 4-2 Applications in Group: OV Performance

Application	Description
`Check alarmdef`	Check the syntax of the HP Performance Agent `alarmdef` file (`utility -xc`).
`Check parm`	Check the syntax of the HP Performance Agent `parm` file (`utility -xp`).
`Config alarmdef`	Edit the HP Performance Agent `alarmdef` file and check the syntax (`utility -xc`).
`Config parm`	Edit the HP Performance Agent `parm` file and check the syntax (`utility -up`).
`Config Datasources`	For HP Performance Agent 3.x, edit the `/var/opt/perf/perflbd.rc` file. For HP Performance Agent 4.x, edit the `/var/opt/OV/conf/perf/datasources` file.
`Config ttd.conf`	Edit the `/var/opt/perf/ttd.conf` file.
`List Processes`	List the active performance tool processes (`perfstat -p`).
`List Versions`	List the version numbers for key performance tool files (`perfstat -v`).
`Reactivate alarmdef`	Reinitialize HP Performance Agent `alarmgen` process (`mwa restart alarm`).
`Restart PA Servers`	Reinitialize HP Performance Agent server processes (`mwa restart server`).

Table 4-2 Applications in Group: OV Performance (Continued)

Application	Description
`Restart Perf Agt`	Reinitialize all HP Performance Agent processes (`mwa restart`).
`Start extract`	Start the HP Performance Agent `extract` program.
`Start Perf Agt`	Start all HP Performance Agent processes (`mwa start`).
`Start pv`	Start the HP Performance Manager monitoring tool.
`Start pvalarmd`	Start the HP Performance Manager `pvalarmd` process (`pvalarmd.start`).
`Start utility`	Start the HP Performance Agent `utility` program.
`Stop Perf Agt`	Stop all HP Performance Agent processes except for `ttd` (`mwa stop`).
`Stop pvalarmd`	Stop the HP Performance Manager `pvalarmd` process (`pvalarmd.stop`).
`Tail Status Files`	Display last few lines of performance tool status files (`perfstat -t`)
`Start OVPM`	Start theHP Performance Manager processes.
`Stop OVPM`	Stop the HP Performance Manager processes.
`Restart OVPM`	Restart theHP Performance Manager processes.
`Status OVPM`	Status of HP Performance Manager is displayed.

Types of Policies

HP Performance Agent installs the `OpenView Performance` policy group, which contains the `OV Performance Agent` and the `OV Performance Manager` policy groups.

OV Performance Agent Template Group

The `OV Performance Agent` policy group contains policies of the following types:

- **Message policies**

  See Table 4-3, “OV Performance Agent: Message Templates,” on page 223.

- **Logfile policies**

  See Table 4-4, “OV Performance Agent: Logfile Templates,” on page 224.

- **Monitor policies**

  See Table 4-5, “OV Performance Agent: Monitor Templates,” on page 224.

Table 4-3 shows the message policies in the `OV Performance Agent` policy group.

Table 4-3 OV Performance Agent: Message Templates

Template	Description
`opcmsg for OV Performance`	Interception of messages from HP Performance Agent.

Table 4-4 shows the logfile policies in the `OV Performance Agent` policy group.

Table 4-4 OV Performance Agent: Logfile Templates

Template	Description
`status.alarmgen`	Retrieves messages from the `alarmgen`/`agdbserver` status file.
`status.mi`	Retrieves messages from the `midaemon` status file.
`status.perflbd`	Retrieves messages from the `perflbd` status file.
`status.rep_server`	Retrieves messages from the `rep_server` status file.
`status.scope`	Retrieves messages from the `scopeux` status file.
`status.ttd`	Retrieves messages from the `ttd` status file.

Table 4-5 shows the monitor policies in the `OV Performance Agent` policy group.

Table 4-5 OV Performance Agent: Monitor Templates

Template	Description
`agdbserver`	Sends a message if the `agdbserver` process is not running.
`alarmgen`	Sends a message if the `alarmgen` process is not running.
`midaemon`	Sends a message if the `midaemon` process is not running.
`perflbd`	Sends a message if the `perflbd` process is not running.
`rep_server`	Sends a message if the number of `rep_server` processes running does not match the number configured in the `perflbd.rc` file.
`scopeux`	Sends a message if the `scopeux` process is not running.
`ttd`	Sends a message if the `ttd` process is not running.

OV Performance Manager Template Group

You can select the following `OV Performance Manager` policies:

- **Logfile policies**

  See Table 4-6, “OV Performance Manager: Logfile Templates,” on page 225.

- **Monitor policies**

  See Table 4-7, “OV Performance Manager: Monitor Templates,” on page 225.

Table 4-6 shows the logfile policies in the `OV Performance Manager` policy group.

Table 4-6 OV Performance Manager: Logfile Templates

Template	Description
`status.pv`	Retrieves messages from the `pv` status file.
`status.pvalarmd`	Retrieves messages from the `pvalarmd`/`pvmapd` status file.

Table 4-7 shows the monitor policies in the `OV Performance Manager` policy group.

Table 4-7 OV Performance Manager: Monitor Templates

Template	Description
`pvalarmd`	Sends a message if the `pvalarmd` process is not running.

HP Performance Agent Documentation

HP Performance Agent documentation is available in the following languages from the web, or from an HPOM managed node where HP Performance Agent is installed:

- ❏ English
- ❏ Japanese

NOTE HP Performance Agent for Sun Solaris systems is *not* localized. The documentation is available in the English language only.

The documentation on an HPOM managed node can be found at the following location:

/<install directory>/paperdocs/*<product>*/*<language>*/*<manual>*

For example:

`/opt/perf/paperdocs/mwa/C/mwauser.pdf`

All HP Software product manuals can be downloaded from the web site:

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

To download the HP Performance Agent documentation:

1. Select `performance agent` in the product list box, select the product version, and the operating system. Click `[Search]`.
2. Select the document you require and click `[Open]` to view the document online, or click `[Download]` to save the file on your computer.

Downloading and Viewing Documentation

All documentation files are in Adobe Acrobat 4.0 Portable Document Format (PDF). You can view these file on the web with Adobe Acrobat Reader 3.0 or higher. If the Acrobat Reader is not already installed in your Web browser, you can download it at no charge from the Adobe web site:

`http://www.adobe.com`

While viewing a document in the Acrobat Reader, you can print a single page, a group of pages, or the entire document.

5 About HPOM Interoperability

In this Chapter

This chapter describes interoperability between HPOM for UNIX and HP Operations Manager for Windows (HPOM for Windows).

See “Interoperability Between HPOM for UNIX and HPOM for Windows” on page 232.

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, but 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.

Note that 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 for UNIX and HPOM for Windows

The HPOM management server is available in two versions: a UNIX version and a Windows version. Both versions of management servers can work together to manage the same nodes in your environment.

HPOM for UNIX and HPOM for Windows provide several possibilities for exchanging messages and configuration. Figure 5-1 on page 233 shows the various communication paths between HPOM for UNIX and HPOM for Windows:

- **Message forwarding**

  HPOM for Windows management servers can forward messages to HPOM for UNIX management servers. See “Forwarding HPOM for Windows Messages to HPOM for UNIX” on page 234 for more information.

- **Messages**

  HPOM agents can send messages in the following directions:

  - HPOM for UNIX agents to HPOM for Windows servers
  - HPOM for Windows agents to HPOM for UNIX servers

  See “Configuring HPOM Agents to Send Messages to Different Management Servers” on page 234 for more information.

- **Configuration**

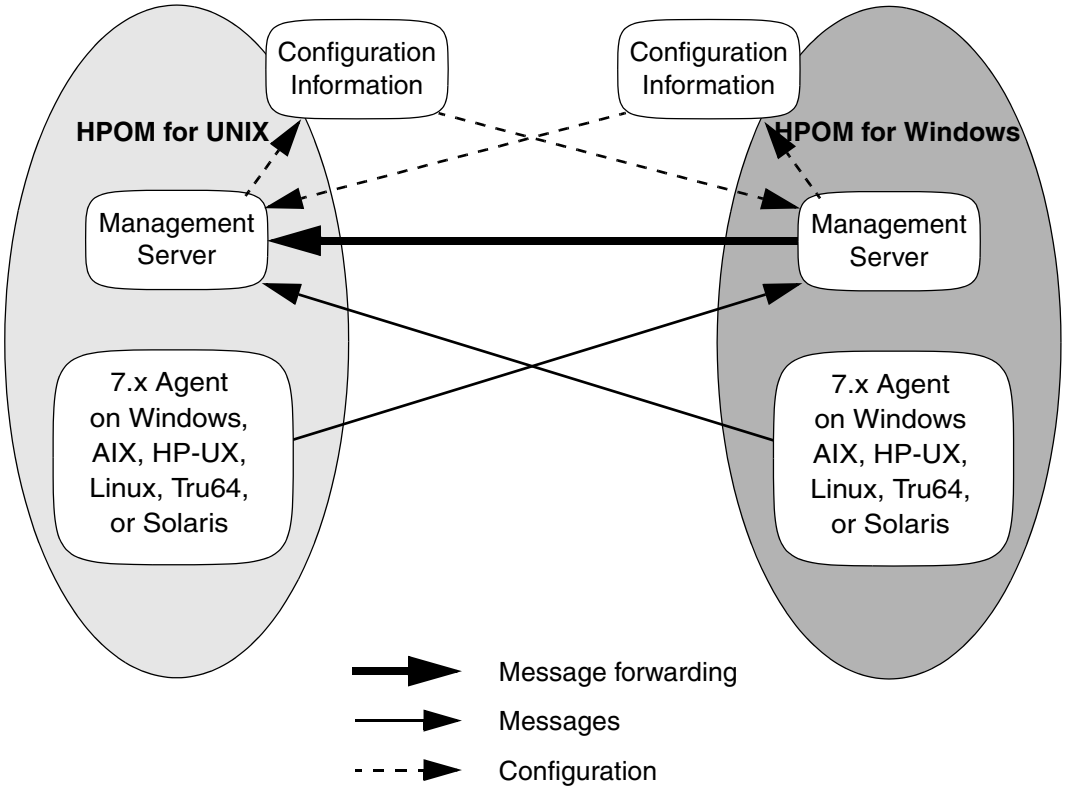
  You can synchronize HPOM configuration information such as policies and nodes between HPOM for UNIX and HPOM for Windows using the upload and download tools provided with each version of the management server. See “Synchronize Configuration Between Servers” on page 241 for more information.

NOTE HPOM for Windows policies are synonymous with policies.

The key features of interoperability as well as the configuration tasks are described in this chapter and in the HPOM for Windows online help at:

HP Operations Manager for Windows
Administering Your Environment
Scalable Architecture for Multiple Management Servers

Figure 5-1 HPOM for UNIX and HPOM for Windows Interoperability



Configuring HPOM Agents to Send Messages to Different Management Servers

Agent-based flexible management allows 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 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:

HP Operations Manager for Windows
Administering Your Environment
Scalable Architecture for Multiple Management Servers
Agent-based flexible Management
Working with HP Operations Manager for UNIX

Forwarding HPOM for Windows Messages to HPOM for UNIX

HPOM for Windows offers two methods for forwarding messages to HPOM for UNIX:

- **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 in HPOM for Windows” on page 235 for more information.

- **Server-based message forwarding**

  Server-based flexible management is the recommended message forwarding solution for HPOM for Windows 8.xx. It uses the same message forwarding and synchronizing techniques used in HPOM for UNIX. It allows forwarding messages directly from one management server to other management servers, including HPOM for UNIX management servers.

  See the HPOM for Windows online help for more information about server-based message forwarding:

  HP Operations Manager for Windows
  Administering Your Environment
  Scalable Architecture for Multiple Management Servers
  Server-based Flexible Management

Configuring Agent-Based Message Forwarding in HPOM for Windows

To configure an HPOM for Windows management server to forward messages to HPOM for UNIX, perform these procedures:

1. Configure HPOM for UNIX to accept messages forwarded from a HPOM for Windows management server.

   For detailed instructions, see “To Configure HPOM for UNIX to Accept Messages Forwarded from an HPOM for Windows Management Server” on page 236.

2. Configure the HPOM for Windows agent.

   For detailed instructions, see “To Configure the HPOM for Windows Agent” on page 239.

3. Optional: Configure the Windows registry

   For detailed instructions, see “Optional: To Change the Default Name of the WMI Policy” on page 239.

About 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:

- **Management 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 for UNIX management server. The installed agent is an HPOM for Windows agent.

- **OV_Messages**

  All OV_Messages with property `Type` equal to `ForwardToVP` are sent to the HPOM for UNIX management server. All other messages go to the HPOM for Windows management server. This configuration is established through the HPOM for UNIX management server with a policy for flexible-management configuration.

- **WMI Interceptor**

  To mark messages that should be forwarded to HPOM for UNIX, 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 for UNIX server.

To Configure HPOM for UNIX to Accept Messages Forwarded from an HPOM for Windows Management Server

1. **Prepare the HPOM for UNIX management server.**

   To prepare the management server:

   a. Add the Windows node on which the HPOM for Windows server is running as an HPOM-controlled node by using the `opcnode` command line interface. For more information, see the *opcnode(1m)* man page.

   b. Update the HPOM for UNIX configuration and start heartbeat polling for the HPOM for Windows node manually.

      Use the following commands:

      `/opt/OV/bin/OpC/opcsw -installed <node>`

      Sample output: `f887b88`

/opt/OV/bin/OpC/opchbp -start <*node*>

The opcsw command returns the hexadecimal value of the node's IP address. Write this value down. You will need it to set up the flexible-management configuration policy.

For more information about opcsw, see the man page *opcsw*(1M).

2. **Create the message forwarding file.**

   a. Create a file and name it with the hexadecimal value returned by the command opcsw.

   b. Copy the policy below and paste it into the file.

   File: <*hex-value*>

```
#
# 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. In the policy, change the server names `bigunix` (HPOM for UNIX server) and `bignt` (HPOM for Windows server) to the server names used in your environment.

d. To ensure that your changes are correct, run the HPOM for UNIX policy validation tool `opcmomchk(1)` on the finished configuration file:

   `/opt/OV/bin/OpC/opcmomchk <filename>`

   For more information about opcmomchk, see the man page *opcmomchk(1)*.

e. Copy the file you created to the following directory on the HPOM for UNIX server:

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

3. Run the tool `Switch management server for Windows nodes`, located in the HPOM for Windows management server console under `Tools/OpenView Tools`.

IMPORTANT

Be aware that the status of the tool will stay on “starting” if the switch was successful.

When prompted by the script, enter the name of the HPOM for UNIX management server.

4. To distribute the created flexible-management policy to the Windows node of the HPOM for Windows server, use the following command line:

```
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.

To Configure the HPOM for Windows Agent

To configure the HPOM for Windows agent, deploy the policy `Policy management\Samples\Forward to VP` on the HPOM for Windows management server.

Optional: To Change the Default Name of the WMI Policy

The WMI policy used to define the messages to be forwarded to HPOM for UNIX 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>"
```

Optional: To Change the Default Property Type of All Messages Forwarded to HPOM

The WMI interceptor sets the property **message type** of all messages to be forwarded to HPOM for UNIX. 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 for UNIX, you must adjust the flexible management policy accordingly. As you can see in the sample policy in “To Configure HPOM for UNIX to Accept Messages Forwarded from an HPOM for Windows Management Server” on page 236, the default value `ForwardToVP` is used in `MSGTYPE ForwardToVP` to match the forwarded messages.

Synchronize Configuration Between Servers

HP Operations management servers allow exchanging configuration information between management servers. This is useful if you want to centrally develop policy and other configuration information and then deploy this configuration to multiple management servers.

Configuration synchronization is very helpful for forwarding and synchronizing messages between management servers. You can easily synchronize node configuration and instruction text configuration between the forwarding management servers, to set up a working message forwarding environment.

Refer to the following sections in the HPOM for Windows online help for details:

HP Operations Manager for Windows
Administering Your Environment
Scalable Architecture for Multiple Management Servers
Synchronize Configuration Between Servers
Heterogeneous Synchronization

6 Integrating Applications into HPOM

In this Chapter

This chapter explains how to integrate applications into HPOM.

For more detailed information on the elements and the windows you can use to carry out the integration, see the *HPOM Concepts Guide*. See also the *HPOM Application Integration Guide* available within the HP Operations Manager Developer's Toolkit.

About Application Integration

HP Operations Manager (HPOM) enables operators to invoke applications.

Assigning Applications to Operators

You can assign a different set of applications to each operator, as needed.

Integrating HP Applications into HPOM

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 `opccfgupld(1M)`.

Integrating Applications into HPOM Components

You can integrate applications into the following HPOM components:

- ❏ Java GUI
- ❏ Broadcasts
- ❏ Automatic actions, operator-initiated actions, and scheduled actions
- ❏ Monitoring
- ❏ Logfile encapsulation
- ❏ SNMP trap and message interception

Integrating Applications into 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`.

Integrating HPOM Applications

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 detailed information on this tool, refer to the *opcappl(1m)* man page. HPOM provides a selection of default applications and application groups..

Integrating 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.

Requirements for Integrating Applications as Broadcast Commands

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 either case, the application must be available on the managed node.

Distributing Application to Managed Nodes

You can distribute simple and widely used applications to managed nodes through HPOM. For details, see “Distributing the HPOM Agent Configuration to the Managed Nodes” on page 183.

Integrating 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.

About the 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 “Distributing the HPOM Agent Configuration to the Managed Nodes” on page 183.

Integrating Monitoring 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 either case, the application 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 “Distributing the HPOM Agent Configuration to the Managed Nodes” on page 183.

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 set-up procedure. For more information, see 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.

About the 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.

Starting 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 s, `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**

  If a delay of more than two seconds occurs during output or input activity, HPOM assumes that an error has occurred and stops 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.

Guidelines for Setting Up User Profiles

When setting up user profiles, follow these guidelines:

- **User Input**

  Do not ask for specific user input in the profile. Instead, provide a default value that users confirm with by pressing **Return**.

  For example, 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
```

  The correct way to specify the default value is shown in the following script. 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.

Integrating NNM 7.xx into 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 the HPOM. For a list and description of the default NNM application groups and applications, see “About Default Applications and Application Groups” on page 79.

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 Incident Web Service (IWS). See “Integrating NNMi into HPOM” on page 259.

Installing the NNM 7.xx Integration Software

Note that NNM cannot be installed on the same system as the HP Operations management server. This section refers to the NNM installation on the HP Operations agent.

The integration with NNM 7.xx is supported on the following HP Operations agent platforms:

- HP-UX 11i v3
- Solaris 10 for SPARC

To make use of the remote HPOM integration with Network Node Manager (NNM), follow this procedure:

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 NNM system.

   For the prerequisites and installation instructions for the HP Operations agent, see the Chapter 1, “Installing HPOM Agents on the Managed Nodes,” on page 33.

3. Assign the subagent policy HPOvOUOvwMgr to the node where NNM is installed. Use the following command:

   opcnode -assign_pol pol_name=HPOvOUOvwMgr pol_type=Subagent version=1.0 node_name=<*node_name*> net_type=NETWORK_IP

   where <*node_name*> is the name of the node where NNM is installed.

4. Install the HPOM subagent package on the one or more NNM systems.

   The HPOVOUOVWMGR package responsible for the integration of the HPOM with NNM 7.xx is supplied with HPOM subagent and is installed during the subagent installation on the managed node. For the subagent installation procedure, see the “Installing Subagents on Managed Nodes” on page 61.

To Enable Operators to Control 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.

To enable operators to control HPOM agents, follow these steps:

1. Create a copy of the HPOM Status application:

   # opcappl -copy_app app_name=”HPOM Status” new_name=”HPOM Agent Start”

2. Modify the application to enable an operator to start HPOM agents:

   # 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. In the HPOM application bank, create a copy of the HPOM Status application:

   # opcappl -copy_app app_name=”HPOM Status” new_name=”HPOM Agent Stop”

4. Modify the application to enable an operator to stop HPOM agents:

   ```
   # 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>
   ```

   For more options, refer to the *opcappl(1m)* man page.

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 options, refer to the *opccfguser(1m)* man page.

Integrating NNMi into HPOM

This section describes how to configure and use the HP Network Node Manager i-series Software (NNMi) integration on HPOM management servers.

The NNMi–HPOM integration is installed automatically with the HPOM installation. HP Operations Manager Incident Web Service (IWS), necessary for the integration, is also an integral part of the HPOM installation.

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.

Before you can use the features of the NNMi–HPOM integration, you need to perform some configuration tasks. These tasks are described in the section “Configuration Tasks” on page 265.

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*.

Overview

The NNMi–HPOM integration uses a web services-based integration module to forward incidents automatically from NNMi into the active messages browser in HPOM server installations. 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.

Supported Versions

For up-to-date information on 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, but this not a requirement. For example, an NNMi management server may have an HP-UX platform, while the HPOM management server has a Windows operating system.

Integration Features

- **Automatic Incident Forwarding**

  NNMi detects a network problem, processes and correlates it, and displays it in one or more of the NNMi incident views. You can configure NNMi to forward incidents automatically to one or more HPOM management servers. You can also configure filters that limit the criteria under which NNMi forwards incidents to HPOM.

  The forwarded incidents appear in the HPOM active messages browser. These messages in the HPOM browser are associated with the original incidents reported in NNMi.

- **Launch the NNMi Console**

  From within HPOM, you can launch the NNMi console showing the original incident. You can do this in the context of an incident forwarded from NNMi and in the context of an NNMi node that is set up as a managed node in HPOM.

NOTE

For the HP NNM 7.x integration, it was a requirement to deploy an agent from the HPOM management server to the NNM management server. For the new NNMi integration, it is no longer essential to do so.

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.

- **Launch NNMi Forms, Views and Tools**

  Tools for accessing NNMi forms, views, and tools are integrated into HPOM. You need to configure the tools before you can use them (see "Configuration Tasks" on page 265). You can launch the tools for accessing NNMi forms, views, and tools from the HPOM user interface to assess the network status. The tools provided by the integration are listed in Table 6-1.

Tools Provided by the Integration

There are a number of NNMi forms, views and tools that are integrated into HPOM. These appear as tools in the HPOM console, and are divided into four tools groups, as shown in Table 6-1:

Table 6-1 NNMi s by Group

Group Name	Comment
NNMi/By Incident	Tools in this group require an incident (or message) context to run them. All the information required (incident identifier, source NNMi server name, and port number) is contained in the message forwarded to the HPOM message browser.
NNMi/By Node (*<short host name>*)	Tools in this group require a node context to run them.
NNMi/General (*<short host name>*)	Tools in this 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.

Table 6-1 NNMi s by Group (Continued)

Group Name	Comment
NNMi Int-Admin	This group contains a tool, `Create Server Apps`, to create 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 by specifying the NNMi host name and port number.

For installation instructions, see “Installing Additional NNMi Tools” on page 267.

Tools in the By Incident Group

NNMi tools in the `By Incident` group are listed in Table 6-2.

Table 6-2 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 6-2 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.

Tools in the By Node Group

NNMi tools in the `By Node` group are listed in Table 6-3.

Table 6-3 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, giving details about the selected node for troubleshooting purposes.

Table 6-3 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.

Tools in the General Group

NNMi tools in the `General` group are listed in Table 6-4.

Table 6-4 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 on and log out activity for each user account).

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 6-5:

Table 6-5 Synchronization of Incident Lifecycle State Changes

Trigger	Result
In HPOM, the message is acknowledged.	In NNMi, the corresponding incident's lifecycle state is set to Closed.
In HPOM, the message is unacknowledged.	In NNMi, the corresponding incident's lifecycle state is set to Registered.
In NNMi, the incident's lifecycle state is set to Closed.	In HPOM, the corresponding message is acknowledged.
In NNMi, the incident's lifecycle state is changed from Closed to any other state.	In HPOM, the corresponding message is unacknowledged.

Configuration Tasks

Before you can use the features of the HP NNMi–HPOM integration, you first need to perform the following configuration tasks:

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 on creating external nodes, see the *opcnode(1m)* man 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:

   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`

   - 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 267.

Installing Additional NNMi Tools

You can also install additional tools in the main NNMi tools group. The additional tools groups are:

- `General` (see "Tools in the General Group" on page 264).
- `By Node` (see "Tools in the By Node Group" on page 263).

You can install the additional tools for a specific NNMi management server using one of the following methods:

- Running the NNMi application installation script.
- Using the `Create Server Apps` tool from your HPOM console.

During installation, you need to specify the NNMi host name and port number of the desired server node.

NNMi Application Installation Script

HPOM provides an NNMi Application Installation script that lets you install the additional tools. You can execute the script with or without specifying the server parameters.

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.

Running the Script With the Server Parameters To run the NNMi Application Installation script by specifying the server parameters, enter the following:

```
/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).

Running the Script Without the Server Parameters To run the NNMi Application Installation script without specifying the server parameters, do the following:

1. Run the script:

   /opt/OV/contrib/OpC/NNMi-Appls/create_nnm_appls.sh

2. Enter all the necessary information for the specific NNMi server system as prompted (fully qualified host name, a short host name, and the port name).

   You are free to choose your own short name.

   An example run of the script is shown below:

```
>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 tools group is created in the main NNMi group, and is identified by the short host name. An administrator 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 in open operator user interfaces (`File -> Reload Configuration`).

Create Additional Tools from the HPOM Console

If you want, you can install the additional tools from the HPOM console by using the `Create Server Apps` tool.

To install the additional tools, do the following:

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 where you want to run the tool. Then 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`.

5. Select `File –> Reload Configuration`.

   The Configuration Status window opens. Click `OK` when the reload is done.

   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).

Configuring Web Browser Settings

You should configure the web browser settings for the console as follows:

- **Windows platforms**

  Configure the console to always use either an external web browser or the Internet Explorer ActiveX control.

- **Other platforms**

  Configure the console to always use an external web browser.

NOTE Use a web browser that is supported for use with HP NNMi 8.xx.

To check or change the web browser settings for the console:

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`.

Launching NNMi Tools from the HPOM Console

The tools listed in the section “Tools Provided by the Integration” on page 261 can be run after installation (see “Installing Additional NNMi Tools” on page 267).

Examples of how to use the tools follow.

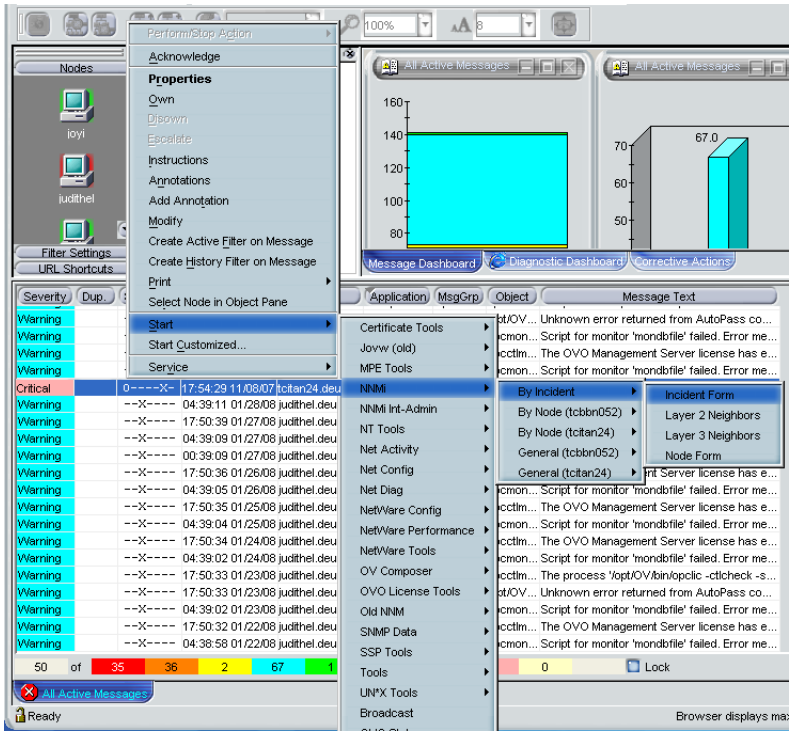
Launching an NNMi Incident Form

You can launch an NNMi Incident Form from your HPOM console.

1. Select a message forwarded from NNMi from the list of messages in the HPOM Message Browser.

2. Right click the message, then select `Start` → `NNMi` → `By Incident` → `Incident Form`.

Figure 6-1 Lanching the NNMi Incident Form

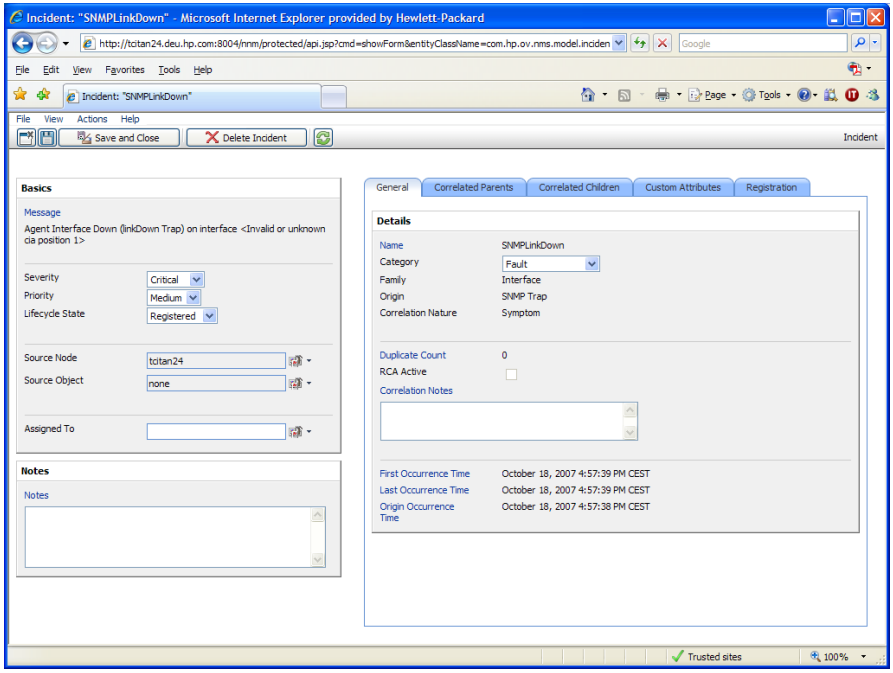


The log-in screen for NNMi opens the first time you run a tool.

3. Enter the User Name and Password and then click `Sign-In`.

The NNMi Incident Form opens.

Figure 6-2 NNMi Incident Form



Launching the NNMi Console

To launch the NNMi console from the HPOM user interface:

1. Select `Tools -> NNMi`.
2. Then select `General (<host>)`, where **<***host***>** is the short host name of the specific NNMi server node.
3. Select `NNMi Console`. The log-in screen for NNMi opens.

   Enter the `User Name` and `Password` and then click `Sign-In` to open the NNMi console.

7 About 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. It 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.

What Is a Notification Service or Trouble Ticket System?

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 Services

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 Systems

Trouble ticket systems are used to document, track, and resolve reported problems.

HP Service Desk

HP Service Desk is HP solution to successfully 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.

Writing Scripts and Programs

The configuration includes writing your own script or program that calls the external interface. The script serves as a link between HPOM and the notification service or trouble ticket system.

Example Script

To show you how to call an external notification service or trouble ticket system, HPOM provides the following example script:

```
/opt/OV/bin/OpC/extern_intf/ttns_mail.sh
```

This script sends an email to all operators responsible for the message.

Guidelines for Writing Scripts and Programs

When writing your script or program, follow these 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 281.

Configuring Notification Services and Trouble Ticket Systems

This section shows you how to integrate an external notification service or trouble ticket system into HPOM. The high-level steps in this section provide you with an overview of the configuration tasks.

Configuring Notification Services

To configure a notification service, follow these high-level steps:

1. **Set up the notification service.**

   Do the following:

   a. Write a script or program that calls the service.

      For details, see “Guidelines for Writing Scripts and Programs” on page 276.

   b. Set up a notification method by using the `opcnotiservice` command. See the corresponding man page for more information.

2. **Set the notification schedule.**

   Schedule your external notification services according to a timetable. Determine which services are used 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 setting the notification schedule, use the `opcnotischedule` command.

3. **Set external notification for a message condition.**

   Configure messages to be forwarded to the external notification service according to the schedule you have 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 could also set up a global flexible management policy for service hours and scheduled outages to define which messages are forwarded to the notification service. See “Forwarding Messages to a Trouble Ticket or Notification Interface” on page 123 for more information.

Configuring Trouble Ticket Systems

To configure a trouble ticket system, follow these high-level steps:

1. **Set up the trouble ticket system.**

   Do the following:

   a. Write a script or program that calls the trouble ticket system.

      For details, see “Guidelines for Writing Scripts and Programs” on page 276.

   b. Set up a trouble ticket call by using the `opctt` command. For example:

      ```
      /opt/OV/bin/OpC/opctt -enable /opt/OV/bin/OpC\
      /extern_intf/ttns_mail.sh
      ```

      See the corresponding man page for more information.

2. **Forward messages to a trouble ticket system.**

   Configure messages to be forwarded to the trouble ticket system. 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 123 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, and to forward a message to a trouble ticket system, HPOM uses the following parameters.

Table 7-1 Parameters for Notification Services and Trouble Ticket Systems

Parameter	Description and Example
1	Unique message number. Example: `c1c79228-ae12-71d6-1a8f-0f887ebe0000`
2	Message node name. Example: `hpbbxyz3.bbn.hp.com`
3	Node type. Example: `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. Example: `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. Example: `16:22:04`

Table 7-1 Parameters for Notification Services and Trouble Ticket Systems (Continued)

Parameter	Description and Example
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. Example: `08/02/2008`
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. Example: `16:22:05`
8	Application name. Example: `/bin/su(1) Switch User`
9	Message group. Example: `Security`
10	Object name. Example: `root`
11	Message severity (`unknown`, `normal`, `warning`, `minor`, `major` or `critical`). Example: `normal`
12	List of responsible HPOM operators. Names are separated with one space. Example: `opc_op Bill John`

Table 7-1 Parameters for Notification Services and Trouble Ticket Systems (Continued)

Parameter	Description and Example
13	Message text. Text is *not* enclosed in quotation marks (""). Example: `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. Example: `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 (;;). Example: `Customer=Hewlett-Packard;;Country=United States of America`
16	Number of suppressed duplicate messages. This 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. Example: `14`

8 About HPOM Language Support

In this Chapter

This chapter describes the language dependencies of the HP Operations Manager (HPOM) management server processes, managed node commands and processes, and the Java GUI. It also describes the languages and LANG settings supported for the various HPOM platforms. Finally, it lists the character sets supported by HPOM.

About 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 (for example, with `ovc -start ovoacomm` and `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 `ovc -start` command is issued on the management server from within the following shell script:

- **HP-UX**

  `/sbin/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 `ovc -start ovoacomm` 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 9.00, 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 8-1 are supported for the management server. HPOM has been verified to run in these languages.

Table 8-1 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, which is set during the HPOM installation, determines the internal processing character set of the management server. HPOM 9.00 supports only the AL32UTF8 character set for the database. All the data on the management server must likewise be entered by using the UTF-8 encoding.

In most cases you can use the default value, which is american_america.AL32UTF8. You can also use another value for NLS_LANG, but in that case the desired value must be using the AL32UTF8 character set. Make sure that you set the desired value before starting the HPOM installation. Enter the following command:

```
export NLS_LANG=<value>
```

HPOM supports the Oracle database character sets listed in Table 8-2.

Table 8-2 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 management server must be configured to accept UTF-8 input/output. When setting up the user environment, consider the following:

- Keyboard layout / code page
- If you use a terminal program, you must configure it to correctly send the user input as UTF-8, and to interpret the management server's response as UTF-8 as well.

  Depending on the case, you will need to enable certain options, to run the terminal with a special parameter, or even to recompile it with a multibyte option.
- A font capable of showing Unicode characters must be used for the terminal.

For detailed information about configuring these elements, refer to your program or operating system documentation.

About Language Support on Managed Nodes

HPOM language support for HPOM internal messages on managed nodes is shown in Table 8-3 and Table 8-4.

Table 8-3 Language Support for HPOM Internal Messages

Management Server	Managed Nodes	English	Japanese
HP-UX or Sun Solaris	AIX	✔	✔
	HP-UX	✔	✔
	Linux	✔	✔
	Solaris	✔	✔
	Tru64 UNIX	✔	✔
	Windows	✔	✔

Table 8-4 Language Support for HTTPS Agents Only

Management Server	Managed Nodes	Spanish, Korean, Simplified Chinese
HP-UX or Sun Solaris	HP-UX	✔
	Linux	✔
	Solaris	✔
	Windows	✔

NOTE Windows managed nodes use the System Language. A *LANG* environment variable is not available.

Setting the Language of Messages on Managed Nodes

Managed node processes determine the language of HPOM messages by the locale you have set. For example, if you want these processes to generate Japanese messages, 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.

To Set the Language of Messages on a Managed Node

To set the language of messages on a managed node, follow these steps:

1. Set the locale for the HPOM agents in the system startup script.
2. Set `START_LANG` to the locale in which you want the HPOM agent to start.
3. Restart the agents.

Locations of System Resource Files Adapted by HPOM

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*.

Synchronizing Commands with the Character Set of the HPOM Agent

The output of HPOM agent commands (for example, `opcagt -status`) is in the internal character set of 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.

Fileset Requirements on Managed Nodes

Some operating systems must have a specific fileset installed for code-set conversion. Refer to the *HPOM Software Release Notes* for software requirements on all managed node platforms.

Setting the Character Set 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.

Types of Character Sets in an English/Spanish-language Environment

Table 8-5 shows the English/Spanish-language character sets 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 8-5 Verified Character Sets on Managed Nodes (English/Spanish)

HPOM	Platform	Character Set
Management server on HP-UX and Sun Solaris	HP-UX, Solaris	UTF-8, ISO 8859-15, ISO 8859-1, ROMAN8, ASCII
	AIX, Linux, Solaris, Tru64 UNIX	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.

Types of Character Sets in a Japanese-language Environment

Table 8-6 shows the Japanese-language character sets that are supported for HPOM managed nodes.

Table 8-6 Verified Character Sets on Managed Nodes (Japanese)

HPOM	Platform	Character Set
Management server on HP-UX 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, Tru64 UNIX	UTF-8, Shift JIS, EUC[a], ASCII

a. 2-byte Extended UNIX Code.
b. Code Page 932 is analogous to Shift JIS.

About 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 interpret the character set of their command-line arguments by the locale setting. This character set may also 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.

Types of Character Sets in an English-language Environment

Table 8-7 shows the values of *LANG* and the related external character set in an English-language environment.

Table 8-7 External Character Sets for HPOM Management server on HP-UX and Sun Solaris (English/Spanish)

Node Platform	LANG	External Character Set
AIX	<*lang*>.8859-15	ISO 8859-15
	C	ASCII
	<*lang*>.ISO8859-1	ISO 8859-1
	<*lang*>.IBM-850	OEM Code Page 850
	<*lang*>.UTF-8	UTF-8
HP-UX 11.x	<*lang*>.iso885915	ISO 8859-15
	<*lang*>.iso885915@euro	ISO 8859-15
	C	ASCII
	<*lang*>.roman8	ROMAN8
	<*lang*>.iso88591	ISO 8859-1
	C.utf8 / <*lang*>.utf8	UTF-8

Table 8-7 External Character Sets for HPOM Management server on HP-UX and Sun Solaris (English/Spanish) (Continued)

Node Platform	LANG	External Character Set
Linux	<*lang*>@euro	ISO 8859-15
	C	ASCII
	<*lang*>	ISO 8859-1
	<*lang*>.UTF-8	UTF-8
Solaris	<*lang*>.ISO8859-15	ISO 8859-15
	C	ASCII
	<*lang*>	ISO 8859-1
	<*lang*>.UTF-8	UTF-8
Tru64 UNIX	<*lang*>.ISO8859-15	ISO 8859-15
	C	ASCII
	<*lang*>.ISO8859-1	ISO 8859-1
	<*lang*>.UTF-8	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.

Types of External Character Sets in a Japanese-language Environment

Table 8-8 shows the values of *LANG* and the related external character set in a Japanese-language environment.

Table 8-8 External Character Sets (Japanese)

Node Platform	LANG	External Character Set
AIX	C	ASCII
	ja_JP	Shift JIS
	ja_JP.IBM-932	
	ja_JP.IBM-eucJP	EUC
	ja_JP.UTF-8	UTF-8
HP-UX	C	ASCII
	ja_JP.SJIS	Shift JIS
	ja_JP.eucJP	2-byte EUC
	ja_JP.utf8	UTF-8
Linux	C	ASCII
	ja_JP	EUC
	ja_JP.eucJP	EUC
	ja_JP.UTF-8	UTF-8
Solaris	C	ASCII
	ja_JP.PCK	Shift JIS
	ja	EUC
	ja_JP.UTF-8	UTF-8
Tru64 UNIX	C	ASCII
	ja_JP.SJIS	Shift JIS
	ja_JP.eucJP	2-byte EUC
	ja_JP.UTF-8	UTF-8

Table 8-8 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 8-9 shows all the supported character sets for various logfile messages.

Table 8-9 Character Sets Supported by the Logfile Encapsulator

Character Set	Windows Nodes		HP-UX, Solaris, Linux, AIX, Tru64 UNIX 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 EventLog.

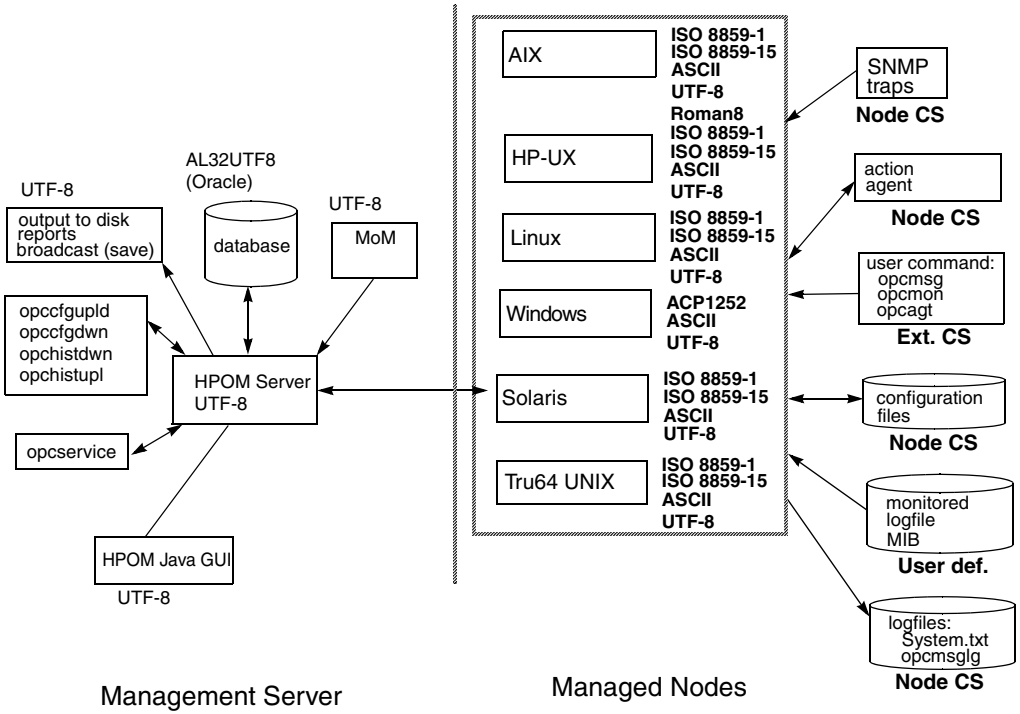
About Character Code Conversion in HPOM

This section describes how to configure HPOM and related character sets in English- and Japanese-language environments.

Configuring an English-language Management Server

Figure 8-1 shows the HPOM configuration and related character sets on an English-language management server.

Figure 8-1 Configuration and Related Character Sets (English)



Key:
SV CS = Server Character Set
Ext. CS = External Character Set

Processing Management Server Files with UTF-8

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`.

Converting Managed Node Files with ROMAN8 and ROMAN9

In an English-language environment, 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.

Processing Managed Node Files

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.

Example of Processing Files on Managed Nodes

In an English-language environment, HPOM could process managed node files as follows:

Scenario	HPOM agent-processing character set is **ROMAN8**. *LANG*=de_DE.iso88591 opcmsg msg_text="This is a message with ä, ü, ö"
Conversion	Input conversion of the `opcmsg` is from **ISO8859-1** to **ROMAN8** before the HPOM message interceptor evaluates the message attributes. Output conversion, before forwarding the message to the management server, is from **ROMAN8** to **UTF-8** (the database character set).

Tips for Processing Files on Managed Nodes

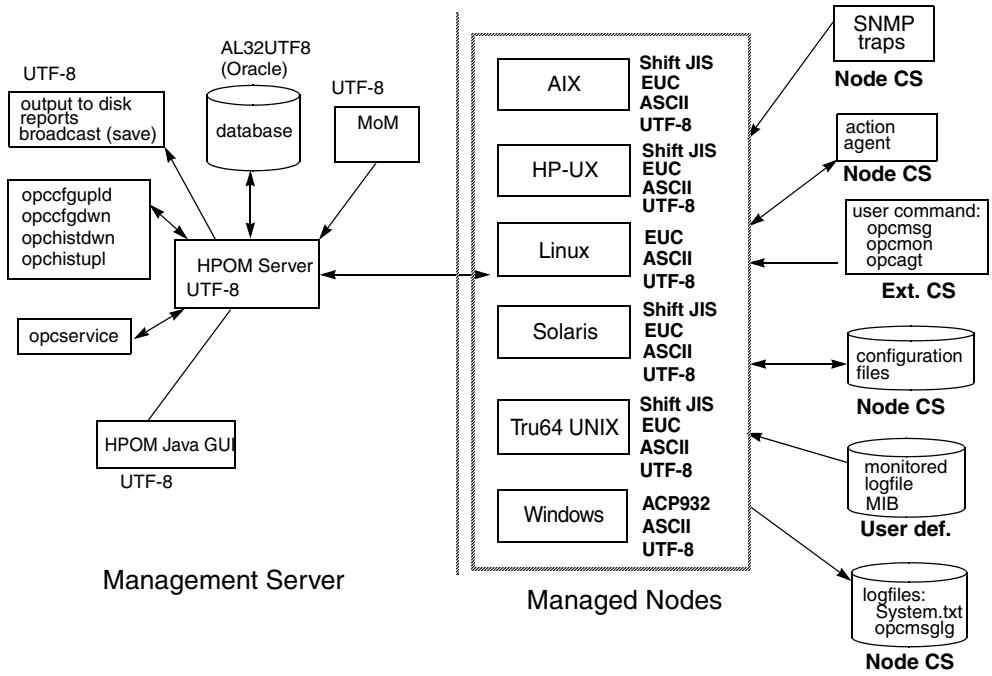
On HP-UX, you can define different character sets for different managed nodes. Define the character set most frequently used on each managed node. For example, if you use mostly monitor logfiles with **ISO 8859-15** characters, you should use **ISO 8859-15** for your managed nodes. When in doubt, use **UTF-8**.

NOTE 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.

Configuring a Japanese-language Management Server

Figure 8-1 shows the HPOM configuration and related character sets in a Japanese-language management server.

Figure 8-2 Configuration and Related Character Sets (Japanese)



Processing Management Server Files with UTF-8

On a Japanese-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`.

Converting Managed Node Files with EUC

In a Japanese-language environment, HPOM does not perform a runtime conversion on the management server. HPOM performs a runtime conversion only for managed node configuration files if the HPOM agents on HP-UX, Solaris, AIX, or Tru64 UNIX are running with the EUC character set.

Processing Managed Node Files

In a Japanese-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.

Example of Processing Managed Node Files

Scenario — HPOM agent-processing character set on an HP-UX managed node is **EUC**.

```
LANG=ja_JP.SJIS

opcmsg msg_text="This is a message with Shift
JIS characters"
```

Conversion — Input conversion of the `opcmsg` is from **Shift JIS** to **EUC**.

Output conversion, before forwarding the message to the management server, is from **EUC** to **UTF-8** (the database character set).

Tips for Processing Managed Nodes Files

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**.

NOTE 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.

About Flexible Management in a Japanese-Language Environment

If your management server runs with the character set UTF-8, you must do one of the following:

- Convert the management server configuration files for flexible management 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 management server configuration file for flexible management from UTF-8 to EUC.

- Convert the managed nodes from EUC to UTF-8.

To convert the MoM configuration file on the management server from UTF-8 to EUC, enter the following:

- **HP-UX**

  /usr/bin/iconv -f utf8 -t euc <mom_orig> > <mom_new>

- **Solaris**

  /usr/bin/iconv -f utf8 -t eucJP <mom_orig> > <mom_new>

  In this command, <*mom_orig*> is the name of the original configuration file in UTF-8, and <*mom_new*> is the IP address of the managed node in hexadecimal, as returned by the command `opc_ip_addr`.

Troubleshooting Other Language Environments

For details on installing the HP Operations management server in international environments, refer to the *HPOM Installation Guide for the Management Server*.

This section contains information about specific cases where HPOM functionality does not work as expected in international environments.

About 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.

About the PC Virtual Terminal Application

The application PC Virtual Terminal does not work and is not supported on Windows.

About 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.

Localizing Object Names

Although you can localize most of the HPOM-specific configuration, you must observe a few restrictions.

Use ASCII Characters

You should use ASCII characters when naming the following:

- 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, using `opcmon`)
- Operator names

  Operator names are used to create corresponding subdirectories and must therefore not be localized.
- Operator passwords
- HPOM administrator password

Localize Labels, Not Objects

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.

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.

9 About the HPOM Java-Based Operator GUI

In this Chapter

This chapter describes the HP Operations Manager (HPOM) Java-based operator graphical user interface (GUI). It also describes the integration of the HPOM Java GUI with the Network Node Manager (NNM).

For detailed installation requirements and instructions, see the *HPOM Installation Guide for the Management Server*.

What Is the HPOM Java-Based Operator GUI?

The HP Operations Manager (HPOM) Java-based operator graphical user interface (GUI) offers a Microsoft Windows-like interface that is extremely easy to use.

Because it is programmed in Java, the HPOM Java-based GUI runs on any platform where the Java Runtime Environment (JRE) is installed. This multiple-platform enables you to run HPOM on a variety of platforms to meet the specific needs of your organization. In addition, HPOM operators can access HPOM or the Network Node Manager (NNM) from anywhere, be it from laptops at home or workstations at the office.

Java-Based Operator 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 detailed information about the HPOM Java-based operator GUI functionality, refer to the *HPOM Java GUI Operator's Guide*.

Message Browsers

- **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 lets you sort messages according to message attributes, for example, by Date and Time, Node, or Application.

- **Displaying Messages**

  In the Java GUI, you can choose between displaying all messages or only the most recent messages. The number of messages displayed in the latest messages view is configurable.

- **Setting Flags**

  Java GUI does not constantly update the SUIAONE flags. That is, the Java GUI does not update flags immediately when the message status changes. For example, 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 their severity, open a View Message Browser, choose a level of severity as filtering criteria, and acknowledge all messages in the current view. Or 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 lets you 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.

General 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 working HPOM users. As a result, the reports `Unmonitored` and `Working HPOM Users` do not include Java GUI users.

About the ito_op Startup Options

This section describes the startup options evaluated by the Java GUI when it is started with the `ito_op` startup script.

You can start the Java GUI with the `ito_op` script by entering the following:

```
/opt/OV/www/htdocs/ito_op/ito_op &
```

When the Java GUI is started, options are read from the environment first, then the command line options passed with the startup script are evaluated, and finally the content of the `itooprc` file is read.

Table 9-1 shows the options evaluated by the Java GUI in the startup scripts:

Table 9-1 Startup Script Options Evaluated by the Java GUI

Option	Format	Default	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.
`colored_message_lines`	`yes|no`	`no`	Decides whether whole messages or just the severity column are colored in the message browser.
`def_browser`	*<filename>*	“”	Path to the web browser on a local host.
`def_look_and_feel`	*<string>*	Windows: `com.sun.java.swing.plaf.motif.MotifLookAndFeel`	Defines the appearance of the Java GUI.

Table 9-1 Startup Script Options Evaluated by the Java GUI (Continued)

Option	Format	Default	Description
display	<*host.domain*>:0	<*localhost*>:0	Hostname to which the display of the X application is exported.
initial_node	<*string*>	<*localhost*>	Hostname of the HP Operations management server to which the Java GUI will connect.
locale	<*lang_territory*>		Presets the locale name.
max_limited_messages	<*int*>	50	Maximum number of messages displayed in a browser.
nosec	true|false	false	Starts the SSL Secure Java GUI in standard mode without SSL functionality.
passwd	<*string*>	""	Password of the HPOM operator used for login.
refresh_interval	<*int*> (seconds)	30	Sequence of time after which the message browser will be refreshed.
server	<*string*>	<*localhost*>	Hostname of the HP Operations 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.

Table 9-1 Startup Script Options Evaluated by the Java GUI (Continued)

Option	Format	Default	Description
user	<*string*>	""	HPOM operator name used for login.

Timezone Settings in ito_op.bat

The Java GUI displays time-related information in the local timezone of the client. If the Java GUI and the HP Operations management server are located in different timezones, you can force the Java GUI to use the timezone of the management server by setting the -Duser.timezone=<*time_zone*> switch in the ito_op.bat file.

For example, to use the timezone 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 timezones are listed in the directory <*JRE_HOME*>\lib\zi, for example GMT, Asia/Singapore, or Europe/Warsaw. If you specify an invalid timezone, GMT is used.

About the itooprc Resource File

The Java GUI resource file `itooprc` is used to store operator preferences.

The `itooprc` file is created or updated automatically in the home directory of the user who started the Java GUI after each click the `[OK]` button in the `Preferences` dialog.

Operator preference options are listed in the `itooprc` file. Each defined option must be listed in a separate line and followed by its parameter.

NOTE The `itooprc` file should be edited by experienced administrators or operators only.

Table 9-2 on page 330 describes the options that can be added in the `itooprc` file with their parameters.

Table 9-2 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.

Table 9-2 itooprc Options and Parameters (Continued)

Option	Format	Description
display	<*hostname*>	Hostname of the exported display where X applications will be launched.
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.

Table 9-2 itooprc Options and Parameters (Continued)

Option	Format	Description
prompt_for_activate	on|off|true|false|yes|no	For HP internal use only.
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 9-2 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 popup 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

Accessing NNM from the Java GUI

By default, the HPOM Java GUI integrates Network Node Manager (NNM). This NNM integration enables users to highlight nodes in the IP Map of NNM systems, and to see and execute Applications directly from the HPOM Java GUI.

HPOM provides an integration with the NNM 7.xx installed on the system other than the 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 “Installing Subagents on Managed Nodes” on page 61. 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 “Integrating NNM 7.xx into HPOM” on page 256.

Accessing NNM 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 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.

❑ **Node Mapping Tool on Management Server**

Tool `opcmapnode` has been configured on the management server, to determine information about which NNM nodes are available on the system domain.

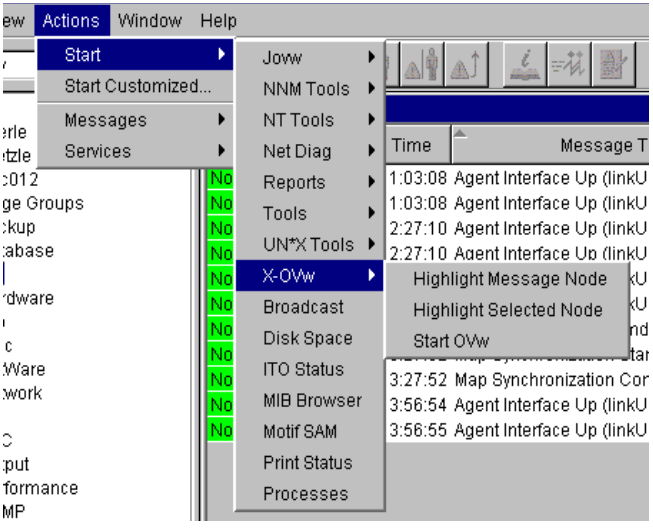
NOTE

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.

About Applications Available from 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 9-1.

Figure 9-1 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.

About the "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>...}
```

In this command, you use 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.

Configuring NNM Access with Command-line Tools

To configure and deploy NNM access, HPOM provides two command-line tools:

`opcctrlovw`	Controller tool. See “About the Controller Tool” on page 337.
`opcmapnode`	Node mapping tool. See “About the Node Mapping Tool” on page 338.

About the 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.

Syntax for the Controller Tool

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, see the man page `opcctrlovw(1m)`.

Configuring the Controller Tool

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>
```

About the Node Mapping Tool

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 to Return 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.

Syntax for the Node Mapping Tool

You use the `opcmapnode` tool as a dynamic target node command in the HPOM application, in backquotes, as follows:

‘`opcmapnode <node>`‘

For more information, see the man page *opcmapnode(1m)*.

Configuring the Node Mapping Tool

When passed, `opcmapnode` reads the following file:

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

This 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.

Accessing Jovw

Jovw is the Java-based web interface to the Network Node Manager (NNM). Jovw is integrated into the HPOM Tools. By default, Jovw is assigned to the itop and netop operators. This section describes how to access the default IP map with Jovw, and how to modify the integration so that other IP maps can be accessed.

To Access the Default IP Map with Jovw

To access the default IP Map with Jovw, follow these steps:

1. Start ovw on the remote NNM 7.xx system. As user root, enter:

   ovw

   When accessing Jovw, ovw must be running.

2. As HPOM administrator, assign the application group `Jovw` to other operators, as needed.

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.

To Access Other IP Maps with Jovw

If you want to access an IP map other than the default IP Map, modify the Jovw applications. Follow this 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:
   - 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. As user root, enter:

   ```
   ovw -map <new_map>
   ```

   where, <*new_map*> is the name of the IP map you have specified in the previous steps.

   When accessing Jovw, `ovw` must be running.

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.

Configuring Backup Management Servers for the Java GUI

Java GUI clients can automatically reconnect to one or more backup management servers, if the currently connected HP Operations management server suddenly becomes unavailable, for example because of a system failure.

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**

  Use the keyword `OPC_JGUI_BACKUP_SRV` to create a list of HPOM backup management servers for connecting 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**

  Use the keyword `OPC_JGUI_RECONNECT_RETRIES` to specify the number of reconnects a Java GUI client attempts before connecting 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.

See also the man page *ovconfchg(1)* for more information.

Operating with the Java GUI from Other Java Applications

It is possible to control certain Java GUI features remotely from other Java applications using the Java GUI Remote APIs.

For more information on the concept, integration details, and usage of the Java GUI Remote APIs, refer to *HPOM Application Integration Guide*.

For details about the available Java GUI Remote APIs, refer to the Java GUI Remote APIs Specification, which can be accessed through the following URL:

`http://<management_server>:3443/ITO_DOC`

In this instance, `<management_server>` is the fully qualified hostname of your management server.

Global Property Files in the Java GUI

When a Java GUI user customizes the GUI, the customized settings are stored in property files, which reside in the user's home directory. The property files include the following files:

- **Console settings files**

  - `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.

- **Resource files**

  The Java GUI resource file `itooprc`. See also "About the itooprc Resource File" on page 330.

- **Browser settings files**

  The browser settings file `itoopbrw`. Refer to the *HPOM Java GUI Operator's Guide* for more information.

To override these individual settings, you can configure the Java GUI to use global property files from a shared location. The global property files override all 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 individual property files of the administrator and, if so configured, of selected operators, if such files exist in the home directory of the user. See also "Using Individual Settings with Global Property Files" on page 350.

Enabling Global Property Files

Use the `ovconfchg` configuration tool on the HP Operations management server to enable global property files for the Java GUI:

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:`)

     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:

   - *Java GUIs running on Windows*

     ```
     ovconfchg -ovrg server -ns opc -set \
     OPC_JGUI_GLOBAL_SETTINGS_WIN <win_shared_location>
     ```

   - *Java GUIs running on 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 other 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.

Using 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.

To grant permission to selected operators to save and use individual property files, specify their user names, separated by commas, for the variable `OPC_JGUI_CONF_ALLOWED_USERS`, for example:

```
/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.

Polling Global Configuration Changes

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.

For example, to set the polling interval to one minute, add the following line to the `itooprc` file:

```
global_settings_poll_interval 1
```

Secure HTTPS-based Java GUI 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 secured 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:

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.

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.

All forwarded HTTPS requests are then handled by `inetd` process, as well as the requests from non-secure Java GUI clients.

The `opcuihttps` also processes replies from the HP Operations management server and mediates them to the Java GUI using the HTTPS protocol.

This way all communication requests, from Java GUI to HP Operations management server and the other way round, become trustworthy for secure exchange of data.

For information about how to configure `opcuihttps` settings as well as for the list the parameters related to HTTPS-based Java GUI, see “Configuring the opcuihttps Process” on page 353.

Figure 9-2 shows the client-server communication. Depending on the chosen communication type, the following applies:

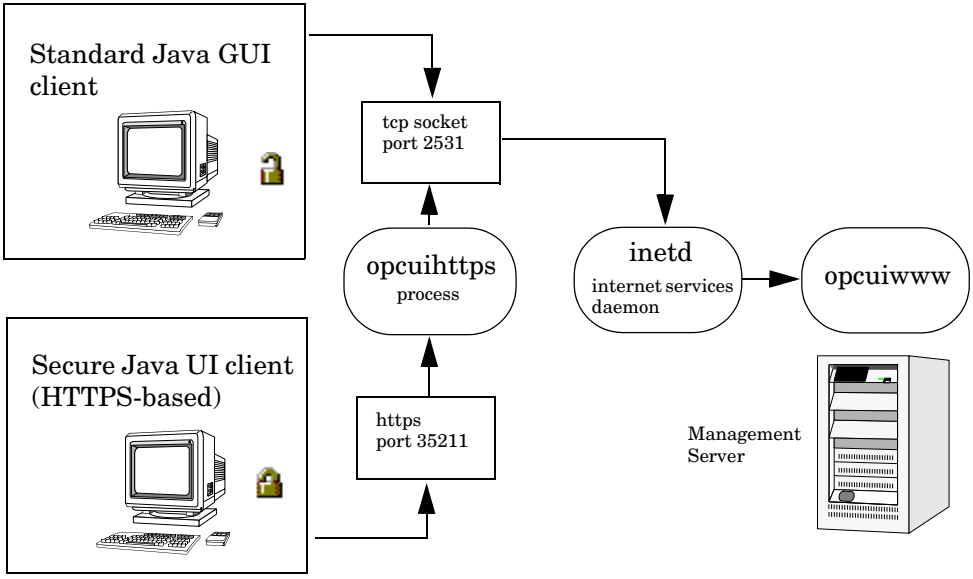
- **HTTPS-based communication**

  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 9-2 Client-server Communication



The authentication process which ensure establishing a secure communication, including providing and installing certificates is described in the *HPOM Java GUI Operator's Guide*.

Configuring the opcuihttps Process

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.

To change the `opcuihttps` parameters, perform the following steps:

1. Use the `ovconfchg` command-line tool to change a parameter:

   ```
   ovconfchg -ovrg server -ns opc.opcuihttps -set \
   <parameter> <value>
   ```

   See Table 9-3 on page 354 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 9-3 lists the parameters for configuring the opcuihttps process.

Table 9-3 The opcuihttps Parameters

Parameter	Format	Default value	Description
SERVER_PORT[a]	<*number*>	35211[b]	A port on which the Java GUI is listening.
OPCUIWWW_PORT	<*number*>	2531	The opcuiwww port number as defined in /etc/services, ito-e-gui entry.
SSL_CLIENT_ VERIFICATION_MODE	Anonymous|RequireCertificate	Anonymous	Specifies whether the opcuihttps server accepts anonymous connections from the clients. If set to RequireCertificate, the clients will require the certificate for (full) authentication[c].
MAX_CONNECTIONS	<*number*>	100	The maximum number of connections 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, 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 Internet Explorer or Mozilla. To do so, enter the following:

`https://<server>:<port>/opcuihttps/info`

Where <*server*> is an HP Operations management server hostname, and <*port*> is the port on which `opcuihttps` is listening.

Configuring the HTTPS-Based Java GUI Connection Through Firewalls

For the HTTPS-based Java GUI to communicate with an HPOM management server through a firewall, you can either configure the firewall to allow the HTTPS-based Java GUI direct access to the HPOM management server, or you can configure the HTTPS-based Java GUI to 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:

- Using the `ito_op` command line tool.
- Updating the `itooprc` file.
- In the `Login` dialog box.
- For Java GUI applets.
- Using the Core functionality.

See the *HPOM Java GUI Operator's Guide* for more information about each method.

Assigning Java GUI 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*.

To Assign Operator Defaults

To assign operator defaults, you have to be familiar with the following procedures:

- Creating application groups using the `opcappl` command-line tool.
- Adding applications to the application groups using the `opcappl` command-line tool.

NOTE

If you want to enable starting applications without a graphical user interface as local applications in the Java GUI, specify the application call value as follows:

- *Windows*

  `app_call='cmd /c start <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
```

❏ Assigning applications and application groups using the `opccfguser` command-line tool.

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 on these procedures, see the *opcappl(1m)* and *opccfguser(1m)* man pages.

Tips for Improved Performance

This section contains tips to help you improve performance of the HPOM Java-based operator GUI.

Identifying Logged-on Java GUI Users

Before stopping the HP Operations management server or the database processes for longer periods of time, it can be helpful to identify the HPOM operators who are currently logged into the Java GUI, and notify them of the upcoming downtime.

To find out who is currently logged into the Java GUI, start the following tool:

```
/opt/OV/contrib/OpC/listguis -java
```

The output lists the number of open Java GUIs, the operator names and the GUI hostnames. You can then either ask the operators to exit from the Java GUI, or kill the `opcuiwww` processes.

About Security Exception Warnings

If you receive a security exception warning when trying to run the Java GUI as an applet in a web browser, the security file `identitydb.obj` has not been downloaded in binary mode.

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 by entering:

   ```
   /opt/OV/httpd/bin/apachectl restart
   ```

3. Download the file `identitydb.obj` again.

10 About HPOM Processes

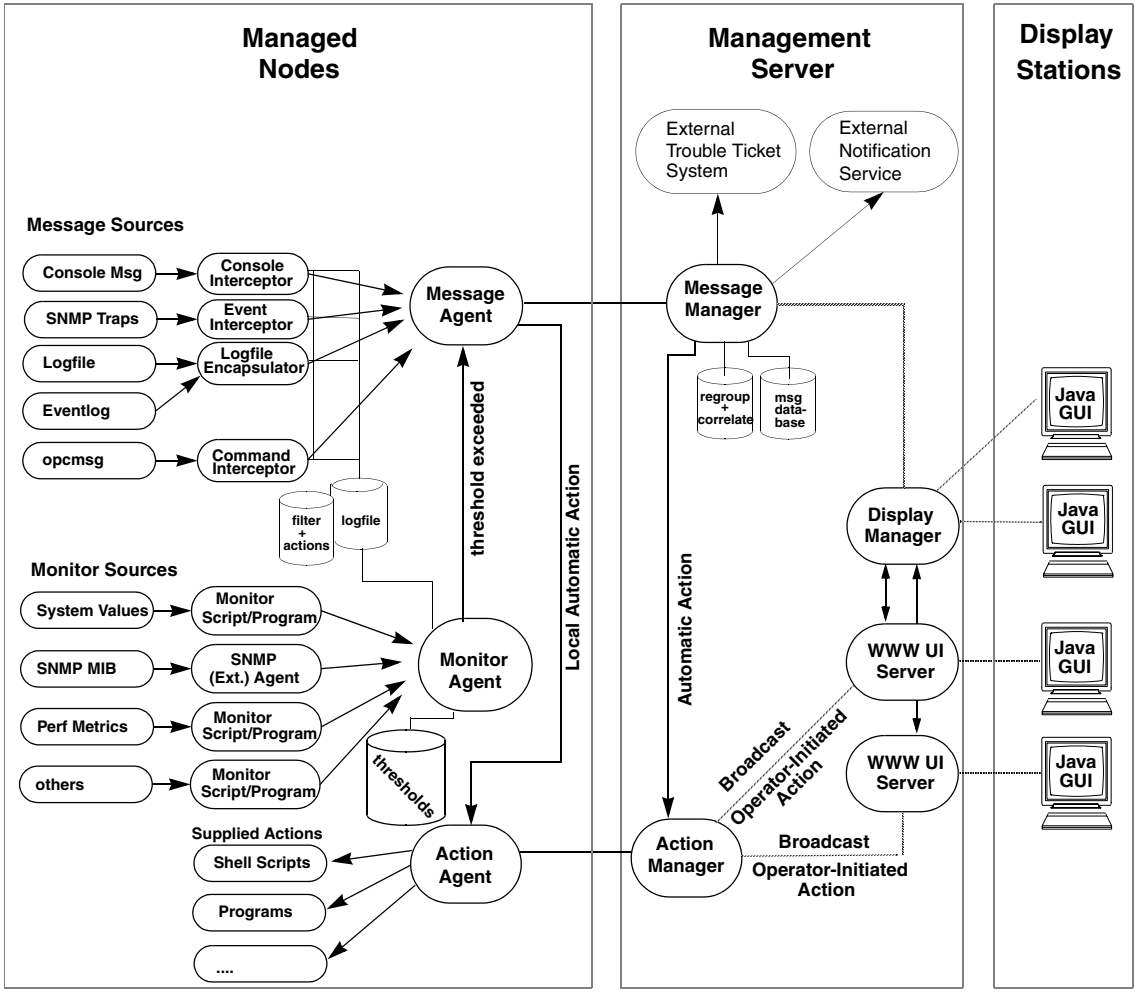
In this Chapter

This chapter provides a functional overview of the management server and managed node processes used by HP Operations Manager (HPOM).

About Communication in HPOM

The communication flow between the management server, managed nodes, and processes in HPOM is shown in Figure 10-1.

Figure 10-1 Functional Overview of HPOM



HP Operations agents and management servers communicate through Remote Procedure Calls (RPCs), based on BBC, queues, pipes, or signals. These 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.

For more information on how the processes communicate with one another and what each process does, see “About Management Server Processes” on page 363 and “About Managed Node Processes” on page 368.

About Management Server Processes

This section describes HPOM processes and their associated files on the management server.

Types of Processes on the Management Server

This section describes the processes that run on the HP Operations management server.

`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.

Types of Process Files on the Management Server

The files used for HP Operations management server processes are contained in the following directory:

`/var/opt/OV/share/tmp/OpC/mgmt_sv`

This section describes those pipes and queue files.

`actreqp/actreqq`	Queue/pipe used by the **display manager**, **message manager**, **TTNS manager**, (and **action manager**) to pass action requests to the action manager.
`actrespp/actrespq`	Queue/pipe used by the **message receiver**, **request sender**, and **action manager** to pass action responses to the action manager.
`ctrlq/ctrlp`	Queue/pipe between the **display manager** and **control manager**.
`forwmgrp/forwmgrq`	Queue/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/pipe between the **message dispatcher** and the **request handler**.
`mpicdmp/mpicdmq`	Queue/pipe used by the **display manager** and the message stream interfaces to transfer control sequences for message-change event handling.
`mpicmmp/mpicmmq`	Queue/pipe used by the **message manager** and message stream interfaces to transfer control sequences for message handling through the MSI.
`mpimmp/mpimmq`	Queue/pipe used by the **message manager** and the message stream interfaces to transfer messages from MSI-programs to the message manager.
`msgmgrq/msgmgrp`	Queue/pipe between the **message receiver** and **message manager**.

`opcecap/opcecaq`	Queue/pipe used to pass messages from the **message manager** to the **event correlation manager**.
`pids`	Process IDs of the HP Operations Manager that are controlled by the **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/pipe between the **request handler** and the **request sender**. Also used by the **display manager** and the **action manager**
`ttnsarp/ttnsarq`	Queue/pipe used by the t**rouble ticket manager** and **action manager** when message instructions have to be fetched by the **TTNS manager**.
`ttnsq/ttnsp`	Queue/pipe between the **message manager**, **trouble ticket manager**, and **notification service manager**.

About Managed Node Processes

This section describes the processes used on the HPOM managed node.

Types of Processes on the Managed Node

This section describes the HPOM processes on the managed node. The files for these processes are described in “Types of Process Files on the Managed Node” on page 371.

`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 command broadcasting and for 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, this process 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:

- ❏ System parameters (for example, CPU load, disk utilization, 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.

Types of Process Files on the Managed Node

This section describes the pipes and queue files used by the HPOM processes outlined in “Types of Processes on the Managed Node” on page 368. The location of these process files are listed in “Location of Process Files on the Managed Node” on page 373.

`actagtp/actagtq`	Queue/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/pipe used by the **message agent** and the message stream interfaces to transfer control sequences for message handling through the MSI.
`mpimap/mpimaq`	Queue/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/pipe for local buffering of messages to be sent to the **message receiver** when the management server is not accessible.
`msgip/msgiq`	Queue (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/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 10-1 shows the location of the files used by the HPOM processes described in “Types of Processes on the Managed Node” on page 368. These files are described in “Types of Process Files on the Managed Node” on page 371.

Table 10-1 Locating Process-related Files on the Managed Nodes

Platform	File Location
AIX	`/var/lpp/OV/tmp/OpC`
HP-UX 11.x Linux Solaris Tru64 UNIX	`/var/opt/OV/tmp/OpC`
Windows	`\usr\OV\tmp\OpC\<node>`

Types of HPOM Agent Configuration Files

Table 10-2 describes the HPOM agent configuration files, and indicates whether the contents of the files are encrypted. The location of these files are listed in Table 10-3 on page 375.

Table 10-2 Agent Configuration Files and their Contents

File	Contents	Encrypted?
`le`	Logfile encapsulation configuration.	Yes
`mgrconf`	MOM configuration file.	No
`monitor`	Monitor agent policy file.	Yes
`msgi`	Message interceptors `opcmsg(1)` and `opcmsg(3)`.	Yes
`nodeinfo`[a]	Node-specific HPOM configuration information (for example, the logging directory and the type of managed node internal character set).	No
`primmgr`	MOM configuration file.	No
`trapi`	SNMP event interceptor.	Yes

a. Only on RPC-based managed nodes.

Location of HPOM Agent Configuration Files

Table 10-3 lists the locations of the HPOM agent specific configuration files described in Table 10-2 on page 374.

Table 10-3 Locating Agent Configuration Files on the Managed Nodes

Platform	Agent File Location
AIX	`/var/lpp/OV/conf/OpC`
HP-UX 11.x Linux Solaris Tru64 UNIX	`/var/opt/OV/conf/OpC`
Windows	`\usr\OV\conf\OpC\<node>`

About Process Registration

Process Control component (ovcd) controls all HPOM server processes starting, stopping, autorestaring in correct order. Each server process is registered to Process Control component through the XML registration files. These registration files are located on the management server at /etc/opt/OV/share/ovc/.

All the HPOM processes are automatically registered with ovcd and can be started, stopped, and listed using the ovc command with the -start, -stop, and -status options respectively. Each server process has its own XML registration file. This registration file defines how the processes are handled. The configuration of the registered process is stored at /var/opt/OV/conf/ctrl/.

To Add a Customer component to OV Control

HPOM provides a possibility to add a custom process and register it with the ovcd, so it can be managed the same way as the HPOM processes.

Follow the procedure below to register a custom process with the ovcd:

1. You need to create an XML registration file to register a process. You can use a sample XML file opccustproc1.xml provided with HPOM:

   a. Copy and rename the /etc/opt/OV/share/ovc/opccustproc1.xml according to your needs:

   # cp /etc/opt/OV/share/ovc/opccustproc1.xml /etc/opt/OV/share/ovc/*<my_process>*.xml

   where *<my_process>* is the name of the process you want to register.

   b. Modify the following tags in the *<my_process>*.xml file according to your needs. 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 *<my_process>*.xml file as follows:

   # ovcreg -check /etc/opt/OV/share/ovc/*<my_component>*.xml

3. Register the *<my_process>*.xml file as follows:

   # ovcreg -add /etc/opt/OV/share/ovc/*<my_component>*.xml

Now you can start, stop, and check the process status using the ovc command. For example, start the custom process by running:

#ovc -start *<my_process>*

To unregister the custom process, run:

 # ovc -del *<my_process>*

11 About HPOM Security

In this Chapter

This chapter explains security in HP Operations Manager (HPOM).

Types of Security

To improve the security of your HPOM system, you need to do much more than configure software.

In particular, you should investigate the following:

- **System Security**

  Enable the HP Operations management server and managed node to run on a "trusted" system.

  For details, see "About System Security" on page 382.

- **Network Security**

  Protect data that is exchanged between the management server and the managed node.

  For details, see "About Network Security" on page 384.

- **HPOM Security**

  Investigate security-related aspects of application setup and execution, operator-initiated actions, and HPOM auditing.

  For details, see "About Security in HPOM" on page 390 and "About HPOM Auditing" on page 403.

NOTE To find out how HPOM behaves in an environment protected by firewalls, see the *HPOM Firewall Configuration* white paper.

About 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 C2 system developed by the United States Defense Department, 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 a pluggable 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 "About PAM Authentication" on page 393.

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 “About HPOM Auditing” on page 403.

- **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.

About 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. It is not important to HPOM 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 allows 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.

About HTTPS Security

HTTPS 1.1 based communication is the communication technology used by HP for HP BTO Software products and allows applications to exchange data between heterogeneous systems.

HTTPS communication, through application of the Secure Socket Layer (SSL) protocol, uses authentication to validate who can access data, and encryption to secure data exchange. Now that businesses are sending and receiving transactions across the Internet and private intranets more than ever before, 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*.

About 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 RPC calls.

To execute an RPC call, HPOM needs 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.

Configuring HPOM Security Levels

HPOM allows 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 `ovconfchg` command-line tool. For more details, refer to *HPOM HTTPS Agent Concepts and Configuration Guide*. See also *ovconfget* and *ovconfchg* man 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, if a management server process (for example, the request sender) receives an authentication failure when calling a control agent on a managed node, an error message is generated. 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.

About Secure Shell (SSH)

The HPOM agent software can alternatively be installed using the Secure Shell (SSH) installation method. For details, see “Secure Shell Installation Method” on page 47.

Secure Shell (SSH) is a UNIX shell program for logging into, and executing 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 passwordless login for user `root` on the managed node. The best way to set up this login is to establish an RSA-based passwordless login. For more information, see “To Install HPOM Agent Software Using SSH Installation Method” on page 49.

SSH-based Virtual Terminal

An SSH (Secure Shell) 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 for UNIX.

To open secure virtual terminals on the managed nodes, run the following command:

```
opcrlogin -h <hostname> -u <username> -ssh Y
```

Where *<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.

About Security in HPOM

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.

Accessing HPOM

Only registered HPOM users can access the HPOM GUI. By default, the users **opc_adm** and **opc_op** are available.

Changing User Names

HPOM user names and passwords have no direct relation to UNIX user names and passwords. However, you can use UNIX user names. If you do so, and if the user name is defined in the HPOM database, the user is not prompted for HPOM password. This is the fastest way to open an HPOM GUI. If you use UNIX user names, you should map UNIX user names (1:1) to HPOM operator names.

Changing Passwords

As an HPOM administrator, you can change operator passwords. However, you cannot see new passwords set by operators (that is, the characters are masked with asterisks). By default, operators can change their own passwords.

To Prevent Operators from Changing Passwords

To remove the change password functionality from all operators, follow these steps:

1. Open the following file:

   ```
   /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"
   {
   }
   ```

About Java GUI Permissions

This section describes permissions in the Java-based operator GUI.

Accessing the Java-based Operator GUI

The HPOM Java-based operator GUI communicates with the HP Operations management server through port 2531. The `inetd` listens at 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. You can restrict client acceptance to specific systems by editing the `/var/adm/inetd.conf` file on the management server. Make sure to specify the systems for the service `ito-e-gui`.

About Program Security

This section describes security for HP-UX programs.

Accessing HP-UX Programs

The HP-UX 11.x programs `/opt/OV/bin/OpC/opc` and `/opt/OV/bin/OpC/opcuiadm`) have the s-bit (set user-ID on execution).

About Database Security

Security of the database is controlled by the operating system and by the database itself. Users must have an operating system logon for either remote or local access to the data. After a user is logged on, security mechanisms of the database control access to the database and tables.

For more information about database security, see *Using Relational Databases with HP Network Node Manager* and the vendor's manuals supplied with the database.

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, that is, it switches to the user specified and then uses the name and password stored in the application request to start the application.

About 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, see the man page *opcswitchuser(1M)*.

About Password Aging

Application execution can be compromised by the use of password aging.

Password aging is a feature of some system security standards such as C2 that requires passwords to expire after:

- ❏ Specified period of time has passed.
- ❏ Specified date has been reached.
- ❏ Specified number of unsuccessful login attempts have been made.

If password aging is enabled, application startup failures may occur due to the account that a given application uses being temporarily inaccessible. Such failures can be avoided by implementing the HPOM pluggable authentication module (PAM) interface, which enables third-party authentication methods to be used while preserving existing system environments.

About PAM Authentication

You can use PAM (pluggable authentication modules) to retrieve and check user and password information. The user information is saved into a central repository and is accessed by a PAM module. To use PAM for authentication, use the command-line tool `ovconfchg` on the HP Operations management server. For more information, refer to the *ovconfchg* man page.

Setting up 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:

- ❏ Use of a common user database shared with the operating system and other applications. User accounts and passwords have to be set up and maintained only in one place.
- ❏ Higher security measures like stronger encryption, password aging, account expiration etc. are available and can be enforced.

NOTE This only applies to the user authentication itself; the HPOM user accounts must still exist to determine the user's capabilities.

To Configure PAM User Authentication

1. To 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 the HPOM authentication requests to the desired PAM module.

   Add the following entry to the PAM configuration file pam.conf: *pam.conf(4)*:

   ovo auth required <*module*>

ovo	The HPOM application ID.
auth	Defines that the module is used for authentication only.
required	The authentication step must succeed.
<*module*>	The PAM module to be used, or technically a shared library which implements the authentication mechanism like UNIX passwd, Kerberos, NIS, or LDAP.

   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 10*

     ```
     ovo auth requisite pam_authtok_get.so.1
     ovo auth required pam_unix_auth.so.1
     ovo account required pam_unix_account.so.1
     ```

3. Further configuration, such as user-based or module-specific flags, may be applicable (see the general PAM and module documentation).
4. For the HPOM administrator (opc_adm) and each of the HPOM operators, create user names and corresponding passwords using external tools, depending on the selected PAM mechanism.
5. Log on to HPOM as opc_adm using the password specified in the previous step. Then create the remaining HPOM operators accounts from step 4 in HPOM and assign the required responsibilities.

PAM User Authentication Restrictions The following restrictions apply to PAM user authentication with HPOM:

- **No account or session management**

  HPOM PAM does not support PAM account nor session management. It uses PAM purely for authentication.

- **Account setup and management**

  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.

- **Multiple password requests**

  It is not possible to use authentication stacks which request multiple passwords.

To Disable 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.

PAM Failed Login Counter Functionality With the PAM failed login counter functionality, the number of PAM authenticated failed logins to the Java GUI can be counted. Functionality automatically counts failed login attempts 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 failed login counter functionality, do the following:

1. Set PAM user authentication by executing the following:

   `/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_USE_PAM_AUTH TRUE`

2. To set PAM failed login counter, execute the following command:

   `/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 secs since epoch)

`LOGIN_ATTEMPT_DELAY=60` (Delay in secs)

You can get 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`

About Remote Access

This section describes security for remote login and command execution in UNIX environments.

Starting Applications and Broadcast Commands

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.

Starting I/O Applications

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.

Assigning Passwords on Managed Nodes

This section explains how to assign passwords on UNIX and Microsoft Windows managed nodes.

Assigning Passwords 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 a **Window (Input/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 be:

`<management_server>` `opc_op`

Assigning Passwords 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.

Protecting Configuration Distribution

The command `opctmpldwn` provides a way of bypassing the standard HPOM policy distribution mechanism: it allows you to download and encrypt HPOM policies and configuration data on the management server and then copy it to the target location on the managed nodes. Only assigned logfile, SNMP trap, opcmsg, threshold monitor, scheduled action, event correlation, and Manager-of-Manager (MoM) policies are downloaded.

The 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)* manpage for more information.

Protecting 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 have to pass through a firewall system or over the Internet, where packets may be routed through many unknown gateways and networks, then you should take measures required to improve security.

Protecting 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.

Switching the User 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 details, see the *ovswitchuser(1M)* man page.

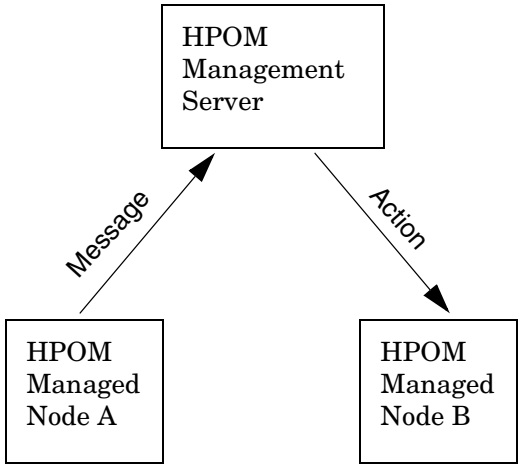
Protecting Remote Actions

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 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 11-1 shows how Managed Node A sends a message to the HP Operations management server which then executes the action on Managed Node B.

Figure 11-1 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.

Types of Security Mechanisms for Remote Actions

To prevent the misuse of remote actions, HPOM offers the following security mechanisms:

- **Assigning Trusted User to 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 details, see the man page *opcswitchuser(1M)*.

- **Encrypting 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.

- **Disabling 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`

- **Detecting 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 an IP address and hostname mismatch, 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.

About 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.

About HPOM Auditing

HPOM 9.00 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 like what kind of action took place, who ordered it, when, and what area does it affect. Each entry has a default severity level, depending on the kind of action. The severity level can be `MINOR` , `MAJOR`, `SERIOUS`, or `INTERNAL` (being the highest severity level).

NOTE

When upgrading from HPOM 8.xx to HPOM 9.00, all previous audit information is lost. To create a copy before the data is deleted, use the `opcauddwn` command line utility.

For usage details, refer to the *opcauddwn (1M)* man page.

Setting an Audit Level

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

If you set the audit level to `OFF`, you do not disable auditing. To disable auditing, use the `opcsrvconfig -audit -disable` command.

To enable or disable the audit system, use the `opcsrvconfig` command line utility. For example:

- 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 usage details, refer to the *opcsrvconfig (1M)* man page.

The HP Operations management server checks the entry severity. Depending on the chosen audit level, entries with the specified severity are written to the `audit.opc.txt` file. For example:

- If the audit level is set to `OFF`, only entries with the `INTERNAL` severity are written.
- If the audit level is set to `MINIMAL`, entries with the `INTERNAL` and `SERIOUS` severity are written.
- If the audit level is set to `ADVANCED`, entries with the `INTERNAL`, `SERIOUS`, and `MAJOR` severity are written.
- If the audit level is set to `FULL`, all entries are written.

Changing the 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 usage details, refer to the *ovconfchg (1M)* and *opcsrvconfig (1M)* man pages.

For more information about variables, see “About HPOM Audit Areas” 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 a predefined format.

The audit entry format is as follows:

```
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>...]]
```

Where:

<Time> is the time when the audit entry was received.

<Severity> is the severity level (`MINOR`, `MAJOR`, `SERIOUS` or `INTERNAL`).

<Area> defines an element or an action on which the audit entry is based (Nodes, Policies, Server config, and so on).

<Action> is one of the following actions: `Read`, `Write`, `Execute`, `Start`, `Stop`, or `Login / Logout`.

<Source> is OMU.

<OS User> is the root or the user who caused the action.

<App User> is `opc_adm`, `opc_op`, or the HPOM user who created the action. If not known, `N/A` or `Admin (N/A)` is shown.

<Text> is the text describing the action that caused that entry.

Audit Areas

Table 11-1 provides a complete overview of all audit areas.

Table 11-1 Audit Areas

Audit Areas
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

Table 11-1 Audit Areas (Continued)

Audit Areas
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

Creating the HPOM GUI Startup Message

According to the NIST 800-37 standard, usage and criticality of any application should be acknowledged before its startup, as well as allowance for its usage. This is achieved with a warning message which is displayed before the application is started.

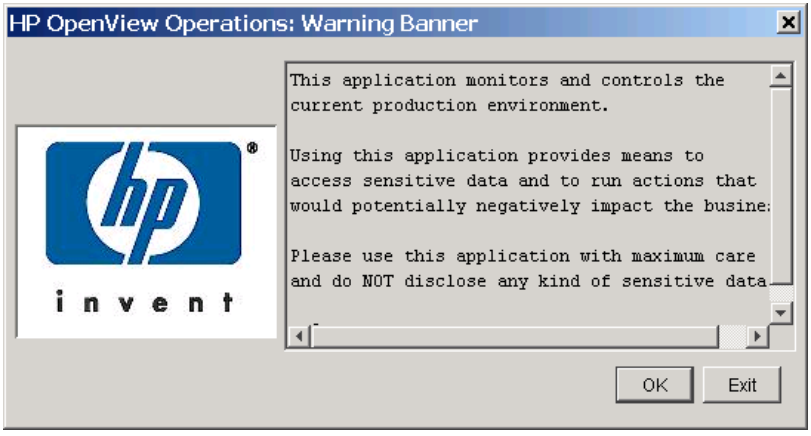
By default, the HPOM GUI startup message does *not* exist. You can create it by writing your own text in a text editor and storing the message in the database. You can also set and change its status (enabled or disabled). See “To Create the HPOM GUI Startup Message” on page 409 for details.

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 11-2 shows an example of the HPOM GUI startup message.

Figure 11-2 Example of the HPOM GUI Startup Message



HPOM GUI Startup Message Considerations

Before you create the HPOM GUI startup message, consider the following points:

- **Customizations**

  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_mgmt_config` table in the attribute `ovou_license_text`. Refer to the *HPOM Reporting and Database Schema* for details about the database tables.

To Create the 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 or 1024 multi byte characters.

   To ensure that the startup message is displayed correctly in the startup message window, pay attention to the line fields in the text editor while writing 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, see the *opcuistartupmsg(1M)* manpage.

To display the current startup message and its status, use `opcuistartupmsg` or `opcuistartupmsg -s`.

12 Maintaining HPOM

In this Chapter

This chapter contains information for administrators who are responsible for maintaining HPOM, and who may need to change the hostname and IP address of the management server and managed nodes.

Maintaining the Management Server

Maintaining the HP Operations management server includes the following:

- ❏ Downloading Configuration Data
- ❏ Backing up Data on the Management Server
- ❏ Maintaining a Database
- ❏ Maintaining the HP Software Platform
- ❏ Maintaining HPOM Directories and Files

Maintaining the Managed Nodes

Maintaining the managed nodes includes the following:

- ❏ Managed Node Directories Containing Runtime Data
- ❏ Location of Local Logfiles

Maintaining Licenses and Hostnames

In addition, this chapter contains information about:

- ❏ Maintaining Licenses
- ❏ Changing Hostnames and IP Addresses

Downloading Configuration Data

You should download configuration data as part of your standard maintenance or backup routine. Also, before you significantly change your HPOM configuration, you should download configuration data or back up your configuration data. To back up your configuration, see “Backing up Data on the Management Server” on page 414.

Method for Downloading Configuration Data

You can download configuration data by using the `opccfgdwn(1M)` command.

This method enables you to select the parts of the configuration that you want to download. For example, instead of downloading the entire configuration, you may choose to download only the policies.

Parts of the Configuration to be Downloaded

The different parts of the configuration to be downloaded are specified in the following file:

`/var/opt/OV/share/tmp/OpC_appl/cfgdwn/download.dsf`

This specification file is required as a parameter by the `opccfgdwn(1M)` command.

Backing up Data on the Management Server

HPOM provides two methods for backing up data on the HP Operations management server:

- **Offline Backup**

  `opcbackup_offline`

- **Automatic Backup**

  `opcbackup_online`

Redistributing Scripts to All Managed Nodes

HPOM configuration data is stored on the management server and 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, action, command and monitor scripts to all managed nodes by using the `-force` option of `opcragt`.

About Backup and Recover Tools

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`. Use `opcrestore_online` to recover data backed up with `opbackup_`online. And so on.

About Archive Log Mode in Oracle

Archive log mode is mode used by Oracle 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 418.

About Offline Backups

You can use the `opcbackup_offline` tool to perform partial or full backups of data on the management server:

- **Partial Backup**

  HPOM configuration data only. Includes current messages and history messages.

- **Full Backup**

  Includes the HPOM binaries and installation defaults.

In either case, you have to shut down the Java GUI and stop all HP services, including the HPOM server processes.

Advantages of Offline Backups

Backing up data offline has the following advantages:

- Archive log mode is not needed:
  - Better overall performance
  - Less disk space required
- Binaries are backed up (if full mode is used).

Disadvantages of Offline Backups

Backing up data offline has the following disadvantages:

- 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.
- You must stop all HP services and the Java GUI.

Types of Offline Backup Functions

For an overview of the backup functions, see man pages `opcbackup_offline(1M)` and `opcrestore_offline(1M)`.

About Online Backups

To carry out a complete automatic backup of the database while the GUI and server processes are running, HPOM provides the following scripts:

- `opcbackup_online`
- `opcrestore_online`

Run the online backups using cron jobs or through scheduled HPOM actions.

Advantages of Online Backups

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:

  - Up to a given time
  - Individual damaged tablespaces

Disadvantages of Online Backups

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

Excluding Temporary Files from 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 OVW 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 is finished. After the backup is finished, the task resumes and completes.

About the 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 have to 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.

To Enable Archive Log Mode in Oracle

For more information about enabling archive log mode, see the "Backup Prerequisites" on page 418.

About the opcwall Command

The command-line utility `opcwall(1)` enables you to notify all running HPOM GUIs of an imminent automated backup.

This command accepts the following options:

`opcwall {-user <user_name>} <Message Text>`

<user_name>	Name of the operator you want to receive the message.
<Message Text>	Text of the message you want the operator to see.
`-user`	If not specified, all operators receive the message.

Backup Prerequisites

Before performing online or offline backup , some prerequisites need to be met. 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`.

For online backup use `opcpackup_online` and `opcrestore_online`, and for offline backup use `opcpackup_offline` and `opcrestore_offline`.

Perform the following steps for creating online or offline backup (procedure is the same for both tipes 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 `RMAN`:

NOTE This step is done 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 the database setup.

```
# 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, error `OPW-00005: File with same name exists - please delete or rename` may appear. Ignore the error message.

4. Write down the 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 RMAN version must be compatible with the Oracle server.

About the opcbackup_online Command

When you use the online backup command `opcbackup_online`, database does not have to be stopped.

The command accepts the following options:

`opcbackup_online [-c] [-r] [-s] [-v]`

`-c` This option specifies 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 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 database backup files. It is preferred that the folder is new and empty.

-s	Use this option to specify the HPOM data backup folder.
-v	Verbose mode.

NOTE The opcbackup_online command stores progress information in the file /var/opt/OV/tmp/ovbackup.log.

About the 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	This option specifies connection string to the database on which the remote manager (RMAN) will perform the backup.
-s	Use this option to specify the folder where HPOM backup files are stored.
-l	Use this option to restore the latest recoverable state of the database.
-b	Use this option to restore the data until the time of backup.
-v	Verbose mode.

NOTE

The `opcrestore_online` command stores progress information in the same file as `opcbackup_online`:

`/var/opt/OV/tmp/ovbackup.log`

About the 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 stoped.

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`	Non-interactive
`-v`	Verbose mode

For more information on the command-line options, refer to the *opcbackup_online(1M)* man page.

About the 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, refer to the *opcrestore_offline(1M) man page*.

Recovering Configuration 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 some 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 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 succesfully completing this kind of restore, you will need to create a new backup.

Recovering a Database to its Latest State

Recovering the database to the latest state is more complicated than restoring the database to its state at the time of the last backup. Recovering the database to its last state uses not only the data contained in the backup but also data on the system itself (that is, online redo logs and archive logs since the last backup). In addition, this method may introduce inconsistencies between the configuration files (restored to the state of the backup) and the data in the database (restored to the latest possible state).

Recovering a database to its latest state works only if the following restrictions apply:

- **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. Also, it can be extracted from the backup. However, this should be done by an Oracle DBA. The scripts will only restore to the latest state if all control files exist.

- **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. The scripts will only restore to the latest state if all redo log files exist.

- **Oracle Log Number**

  The Oracle log number has not been reset since the backup.

- **Archived Redo Logs**

  All archived redo logs made since the backup still exist.

- **HPOM Users**

  No HPOM users have been modified since the backup, which modifies files in the file system.

- **ECS Policies**

  No ECS policies have been added since the backup.

To Remove 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, it must be shut 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 instance should be running at this point, after which you can try to recover the damaged file or the damaged files:

- If 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.

Maintaining a Database

To ensure that your HPOM database runs efficiently, you should perform the following tasks periodically:

- **Download 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)* man page, and *opchistdwn (1M)* man page for downloading history messages.

- **Back up the HPOM Configuration**

  Back up the HPOM configuration regularly. For details, see "Backing up Data on the Management Server" on page 414.

- **Move Messages into the History Database**

  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)* man pages.

- **Add Disks**

  The HPOM database files automatically consume the extra disk space required to cope with any growth. If a disk runs out of space, you can use other disks to add additional files for a tablespace. For details, see the Oracle information.

- **Review 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.

Configuring a Database 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.

To Move Oracle Control Files to the Second Disk

To move one or more Oracle control files to the second disk, follow these steps:

1. Create the directories on the second disk:

   ```
   mkdir -p /u02/oradata/openview
   ```

   ```
   chown oracle:dba /u02/oradata/openview
   ```

2. Shutdown the database

3. Move selected control file(s) to a directory on the other disk, for example from disk /u01 to disk /u02:

   ```
   mv /u01/oradata/openview/control03.ctl \
   /u02/oradata/openview/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/openview/control01.ctl,
                    /u01/oradata/openview/control02.ctl,
                    /u01/oradata/openview/control03.ctl)
   ```

   Example of *new* control file names:

   ```
   control_files = (/u01/oradata/openview/control01.ctl,
                    /u01/oradata/openview/control02.ctl,
                    /u02/oradata/openview/control03.ctl)
   ```

5. Restart the database.

To Create Another Set of Mirrored Online Redo Logs

You can create a second (or even third) set of mirrored, online redo logs on the second (or 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 creates a second set of redo log files in the directory. `/u02/oradata/openview`. Modify the directory names (and repeat the steps) as required.

To create a second set of redo logfiles, follow these steps:

1. Create the directories on the second disk.

   Example:

   ```
   mkdir -p /u02/oradata/openview

   chown oracle:dba /u02/oradata/openview
   ```

2. As user `oracle`, enter the following:

   ```
   sqlplus /nolog

   SQL>connect / as sysdba

   alter database add logfile member
   '/u02/oradata/openview/redo01.log' to group 1;

   alter database add logfile member
   '/u02/oradata/openview/redo02.log' to group 2;

   alter database add logfile member
   '/u02/oradata/openview/redo03.log' to group 3;

   exit
   ```

Maintaining the 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:

```
/var/opt/OV/log/trapd.log.old
```

If you no longer need the entries, erase the trap daemon logfile:

```
/var/opt/OV/log/trapd.log
```

For details about system maintenance in HP NNM, see *Managing Your Network with HP Network Node Manager*.

Maintaining HPOM Directories and Files

To maintain HPOM directories and files, follow these guidelines:

- **Do Not Clean Up the Management Server Directory**

  Important runtime data is contained in the `mgmt_sv` 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.

- **Back Up and Erase the Software Installation File**

  If you no longer need the logfiles, you should backup and then erase the continuously growing HPOM software installation, update, and de-installation 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 (de-)installation and update.

- **Back up and Erase the Error Logfile**

  You should backup and then erase the HPOM error and warning logfile and its backups (for HTTPS-based managed nodes):

  `/var/opt/OV/log/System.txt` (Plain text) , or
  `/var/opt/OV/log/System.bin` (Binary)

  HPOM uses an automatic backup logfile mechanism having up to ten files.

  If the `System.txt` logfile size is greater than 1 MB, HPOM automatically does the following:

  - Moves `System.txt.008` to `System.txt.009` (if exists).
  - Moves `System.txt.007` to `System.txt.008` (if exists).
  - Moves `System.txt.006` to `System.txt.007` (if exists).
  - Moves `System.txt.005` to `System.txt.006` (if exists).
  - Moves `System.txt.004` to `System.txt.005` (if exists).

- Moves `System.txt.003` to `System.txt.004` (if exists).
- Moves `System.txt.002` to `System.txt.003` (if exists).
- Moves `System.txt.001` to `System.txt.002` (if exists).
- Moves `System.txt` to `System.txt.001`

Maintaining the 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` (if exists).
  - Moves `opcmsgl1` to `opcmsgl2` (if exists).
  - 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` (if exists).
  - Moves `System.txt.007` to `System.txt.008` (if exists).
  - Moves `System.txt.006` to `System.txt.007` (if exists).
  - Moves `System.txt.005` to `System.txt.006` (if exists).
  - Moves `System.txt.004` to `System.txt.005` (if exists).
  - Moves `System.txt.003` to `System.txt.004` (if exists).
  - Moves `System.txt.002` to `System.txt.003` (if exists).
  - Moves `System.txt.001` to `System.txt.002` (if exists).
  - Moves `System.txt` to `System.txt.001`

About Managed Node Directories with Runtime Data

Table 12-1 shows the managed node directories that contain important runtime data.

Table 12-1 Managed Node Directories Containing Runtime Data

HPOM	Operating System on the Managed Node	Directories Containing Runtime Data

Management server on HP-UX and Sun 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 and Tru64 UNIX	`/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 12-2 shows where local logfiles reside on HP-UX 10.x/11.x and Windows HTTPS-based managed nodes.

Table 12-2 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/ warnings	`System.txt System.txt.(001-003)`	`System.txt System.txt.(001-003)`
HPOM messages	`opcmsglg, opcmsgl(1-3)`	`opcmsglg opcmsgl(1-3)`

Table 12-3 shows where local logfiles reside on AIX HTTPS-based managed nodes.

Table 12-3 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 12-4 shows where local logfiles reside on other UNIX managed nodes.

Table 12-4 Local Logfiles on Other UNIX HTTPS-based Managed Nodes

Logfile	Tru64 Unix, 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)`

Maintaining Licenses

HP Operations Manager uses the HPOM licensing component to manage licenses and check them for licensed objects.

Configuration

There are two prerequisites for the HPOM licensing component to function properly: `mailx` and configuration parameters.

`mailx`

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.

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 defines the 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 determines whether warning messages should be sent when the number of licenses for a licensed product component reaches the dedicated level. This can be set to *TRUE* or *FALSE*.

This setting works in conjunction with the Severity configuration parameter. Critical license warning messages are always sent, regardless of the configuration settings.

Severity defines the 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 specifies the detail level for license reports. The level can be set to *Summarized* or *Detailed*. The initial 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*.

Use the following command to set the configuration parameters:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opr.el \
   -set LicenseAdminEmailAddress license_admin@company.com \
   -set SwitchOffWarning FALSE \
   -set Severity Major \
   -set Content Summarized
```

Reporting

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.

The `ovolicense` Tool

The `ovolicense` tool is the central tool for the management of the HPOM licenses and the generation of license reports. This 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.

`-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 that `JAVA_HOME` must be set to a valid runtime. GUI features require Java and an X11 display.

`ovolicense -help`

Shows detailed help.

`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 allows you to select a sub-set 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` HPOM

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.

HPOM License Report

The license report shows details for all licensed HPOM components.

Figure 12-1 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
```

Figure 9-1 shows an HPOM license report. 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.

- Agent Count

  Agent Count is a license type and is 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 above report shows that there is an insufficient number of installed HPOM agent licenses.

- HP Operations management server

  Shows the HP Operations management server license status. The server license status in the above report is OK.

- HP Operations Manager Tier Agent

  Shows the HP Operations agent license status. The number of Used Licenses for Desktop Agent and Tier 0 Agent to Tier 4 Agent will always be 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 get the license status.

- Number of unpatched nodes

  The number of nodes that are not using up-to-date HPOM agent software (HPOM 8.17 and later). Licenses required for the node will only be reported by the HPOM agent software if it is up-to-date.

- Number of unreachable nodes

  The number of nodes that sent license and node details but have not refreshed their data for 14 days.

The final part of the report shows an overview of the configuration parameters.

Unregistered Components

It is possible for the report to display a licensed object that is not registered for licensing, as shown in Figure 12-2 and Figure 12-3 on page 445.

Figure 12-2 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.
  =====================================================
```

The report might display node details as shown below:

Figure 12-3 License Report - Unregistered Component

```
Not Registered: noregspi: 4
```

This may happen 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. This means that the first server has license requirements that cannot be met by the second server.

To overcome this problem, the components or SPIs must be installed on all servers sharing a configurations with each other, or removed from the HPOM nodes whose configuration is shared by the servers.

Changing 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:

- `/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 (that is, 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 447 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 and, if the hostname has changed, that 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 of the managed node.

`-oldaddr <old_IP_addr>`

Current IP address 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`

Updates NNM with the information specified for the `-netmask` option and the Adapter/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>`

Specifies the adapter/MAC address of the managed node in hexadecimal notation.

`-hook <cmdname>`

Specifies the adapter/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`

Troubleshoots and solves problems with hostname and IP address changes. Note that this option has a high time and resource consumption.

To Change 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 HP Operations 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 intelligent agents on HPOM managed nodes start buffering their messages.

3. **Make sure the database is running.**

   a. Verify that the database is running by entering:

   ```
   ps -ef | grep ora
   ```

   b. If the database is not running, start it by entering:

   ```
   /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.**

   Use the following command to change the IP address and 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 <new_FQDN> -newaddr <new_IP_addr>
   ```

<old_FQDN>	Current fully qualified domain name of the management server.
<old_IP_addr>	Current IP address of the management server.
<new_FQDN>	New fully qualified domain name of the management server.
<new_IP_addr>	New IP address of the management server.

   See “opc_node_change.pl” on page 447 for more information about this command line tool.

5. **Shut down the database.**

   ```
   /sbin/init.d/ovoracle stop
   ```

6. **Modify the HP Operations management server configuration.**

   Update the HP Operations management server configuration, enter the following:

   ```
   /opt/OV/bin/ovconfchg -ovrg server -ns opc \
   -set OPC_MGMT_SERVER <new_FQDN>
   ```

NOTE

Also update any other customized settings on the management server, such as `bbc.cb.ports:PORTS`.

7. **Update the local agent configuration on the management server.**

   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, the CERTIFICATE_SERVER variable must also be updated. Enter:

```
/opt/OV/bin/ovconfchg -ns sec.cm.client \
-set CERTIFICATE_SERVER <new_FQDN>
```

c. Update the OPC_IP_ADDRESS setting with the new value:

```
/opt/OV/bin/ovconfchg -ns eaagt \
-set OPC_IP_ADDRESS <new_IP_addr>
```

8. **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*>.

9. **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

To change the hostname permanently, run the special initialization script /sbin/set_parms. Refer to the *set_parms(1M)* man page for more information.

For details, refer to the *HP-UX System Manager's Guide*.

If you are moving from a non-name-server environment to a name-server environment, make sure the name server has the new hostname or IP address available.

b. Restart the system for your changes to take effect.

To Reconfigure the Management Server after Changing its Hostname or IP Address

To reconfigure the management server after changing its hostname or IP address, follow these steps:

1. **Stop the 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 HP Software.**

   a. Start the HPOM management server processes:

   ```
   /opt/OV/bin/OpC/opcsv -start
   ```

   b. Start the HPOM agent on the management server:

   ```
   /opt/OV/bin/ovc -start
   ```

NOTE At this point, the agent starts forwarding its buffered messages.

4. **Log in to the Java GUI**.

   Enter the following:

   ```
   /opt/OV/bin/OpC/ito_op
   ```

5. **Verify the policies.**

   Verify that the policies are still assigned to the new node.

6. **Redistribute all Event Correlation policies.**

   If you have changed the hostname, redistribute all Event-correlation policies assigned to the management server.

   ```
   # opcragt -dist -force "$MGMTSV"
   ```

The string $MGMTSV is a management server name (not the agent on the management server).

7. **Update all managed nodes with the new hostname 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 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, the CERTIFICATE_SERVER variable must also be updated. Enter:

      ```
      /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
      ```

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 flexible management environments.**

    - 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, see man page *opcmom(4)*.

    - If you have set up manager-to-manager message forwarding, modify the hostname and IP address manually on all management servers that have the changed system in their node bank.

      Also, check the message forwarding policy on the management servers for occurrences 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 management servers, as needed.

To Change the Hostname or IP Address of a Managed Node

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 (MoM) environment, make sure that you perform all steps described below also 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.

To Change 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. **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.

2. **Change the node name or IP address of the managed node in the HPOM database.**

   On the management server, execute the `opc_node_change.pl` script:

   ```
   opc_node_change.pl -oldname <old_FQDN> \
   -oldaddr <old_IP_addr> -newname <new_FQDN> \
   -newaddr <new_IP_addr> [,<new_IP_addr>,...]
   ```

   See “opc_node_change.pl” on page 447 for more information about this command line tool.

3. **IP address changes only.**

   Set `OPC_IP_ADDRESS` to the new IP address. Enter the following command on the management server:

   ```
   /opt/OV/bin/OpC/opcragt -set_config_var \
   eaagt:OPC_IP_ADDRESS=<new_IP_addr> <new_FQDN>
   ```

Changing Hostnames and IP Addresses in a Cluster Environment

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 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 (that is, DNS or BIND), make sure the name server can access the new IP address.

To Change 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 ov-server disable
   ```

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 447 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, enter the following:

   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>
      ```

   c. If the certificate server is located on the same system as the management server, the CERTIFICATE_SERVER variable must also be updated. Enter:

      ```
      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.**

   Start HPOM integrated services by entering:

   ```
   /opt/OV/bin/ovc -start
   ```

10. **Set the cluster configuration.**

    a. Stop the HP Operations server HA Resource group by entering:

    ```
    /opt/OV/bin/ovharg_config ov-server -stop <node_name>
    ```

    b. Change the cluster configuration to use the new IP address.

    HP Serviceguard

    Edit the `/etc/cmcluster/ov-server/ov-server.cntl` file on *all* cluster nodes. Replace `IP[0]=<old_IP_addr>` with `IP[0]=<new_IP_addr>`.

    c. Start the HP Operations server HA Resource group by entering:

    ```
    /opt/OV/bin/ovharg_config ov-server -start \
    <node_name>
    ```

To Reconfigure the HP Operations Management Server After Changing Its Virtual Hostname or IP Address

To reconfigure the management server after changing its virtual hostname or IP address in a cluster environment, follow these steps:

1. **Disable the HARG monitoring.**

   Enter the following:

   ```
   /opt/OV/lbin/ovharg -monitor ov-server disable
   ```

2. **Stop the management server.**

   Enter the following:

   ```
   /opt/OV/bin/OpC/opcsv -stop
   ```

3. **Make sure the database is running.**

   If the database is not running, start it by entering the following:

   ```
   /sbin/init.d/ovoracle start
   ```

   For information on the Oracle database, refer to the *HPOM Installation Guide for the Management Server*.

4. **Start HP Software.**

   Start HP Software and all other integrated services (including HPOM):

   ```
   /opt/OV/bin/OpC/opcsv -start
   ```

5. **Enable the HARG monitoring.**

   Enter the following:

   ```
   /opt/OV/lbin/ovharg -monitor ov-server enable
   ```

NOTE At this point, the agent starts forwarding its buffered messages.

6. **Log in to the Java GUI.**

   Enter the following:

   ```
   /opt/OV/bin/OpC/ito_op
   ```

7. **Verify the policies.**

   Verify that the policies are still assigned to the new node.

8. **Reassign and redistribute all Event Correlation policies.**

   If you have changed the hostname, reassign and redistribute all Event-correlation policies assigned to the management server.

   ```
   # opcragt -dist -force "$MGMTSV"
   ```

   The string $MGMTSV is a management server name (not the agent on the management server).

9. **Update all managed nodes with the new hostname 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 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, the CERTIFICATE_SERVER variable must also be updated. Enter:

      ```
      /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 flexible management environments.**

    - 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, see man page *opcmom(4)*.

    - If you have set up manager-to-manager message forwarding, modify the hostname and IP address manually on all management servers that have the changed system in their node bank.

      Also, check the message forwarding policy on the management servers for occurrences of the old hostname or IP address.

      Check the following files:

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

      Modify the message forwarding policy on the management servers, as needed.

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 “To Change the Hostname or IP Address of a Managed Node” on page 455.

13 Administration of the HP Operations Management Server in a Cluster Environment

In this Chapter

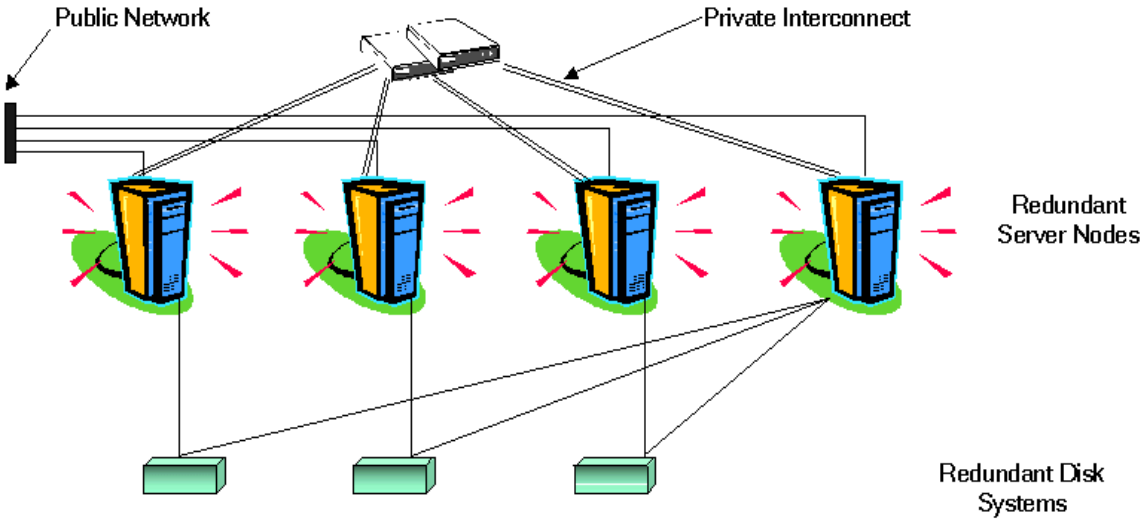
This chapter provides information for system administrators working with HPOM in a cluster environment. It assumes that you are familiar with the general concepts of HPOM and with High Availability (HA) concepts.

For detailed information about clusters, refer to the appropriate chapters in the *HPOM Installation Guide for the Management Server*.

About the Cluster Architecture

Cluster architecture provides a single, globally coherent process and resource management view for the multiple nodes of a cluster. Figure 13-1 shows an example of a cluster architecture.

Figure 13-1 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.

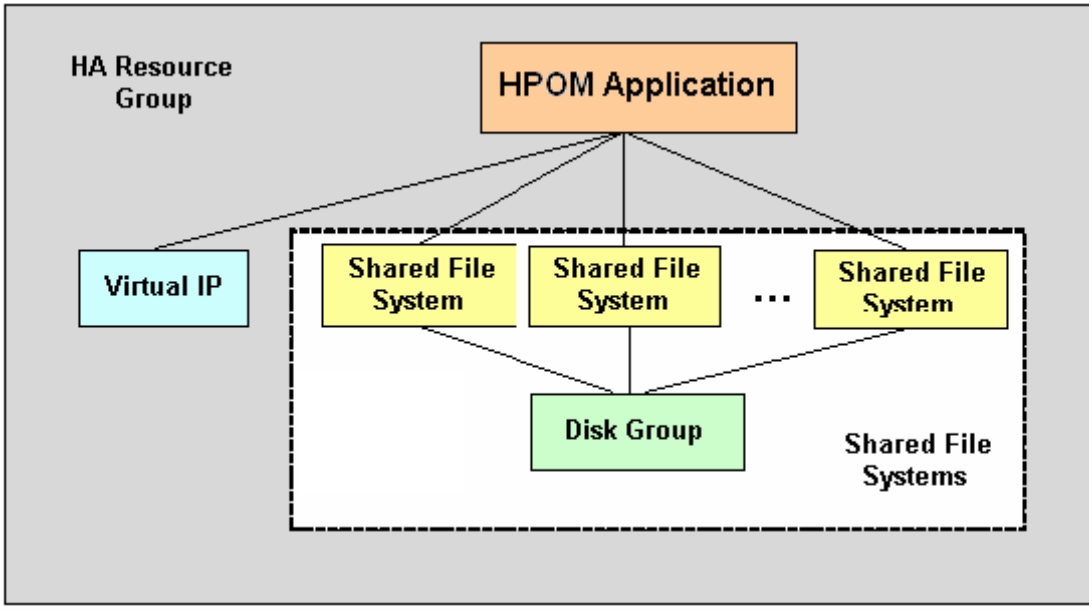
Applications running in a cluster environment are configured as HA Resource Groups. HA Resource Group is a generic term for cluster objects representing HA Applications.

The HP Operations Management Server Running as an HA Resource Group

Concepts

In modern cluster environments such as VERITAS Cluster, Sun Cluster or HP Serviceguard, applications are represented as compounds of resources, simple operations enabling application to run in a cluster environment. The resources construct a **Resource Group**, which represents an application running in a cluster environment.

Figure 13-2 Typical HA Resources Group Layout



The HA Resource Group is differently represented by the various cluster environments. Table 13-1 indicates these differences.

Table 13-1 Resource Group in Cluster Environments

Cluster Environment	Abbreviation	HA Resource Group Represented As...
HP Serviceguard	HP SG	Package
VERITAS Cluster Server	VCS	Service Group
Sun Cluster	SC	Resource Group

Instead of cluster specific terms, HA Resource Group is used in this document as a generic term that designates a set of resources in a cluster environment.

Administering HA Resource Group

Administration of the HA Resource Group is performed by using the `/opt/OV/bin/ovharg_config` command. You can start, stop, and switch the HA Resource Group.

Before starting, stopping, or switching the HA Resource Group, you can check whether the target node is active:

```
/opt/OV/bin/OpC/opcsv -startable
```

You will get the following return exit codes:

0 - active cluster node is detected

2 - inactive cluster node is detected

To avoid starting optional processes whose initial configuration has not been done, or require some manual steps, you can use:

```
/opt/OV/bin/OpC/opcsv -available [<process1> <process2> <...>]
```

You will get the following return exit codes:

0 - all specified processes are properly configured or no processes were specified

1 - not all specified processes are properly configured

To Start the HA Resource Group

To start the HA Resource Group, enter:

/opt/OV/bin/ovharg_config ov-server -start <*node name*>

where <*node name*> is the name of the node on which the HA Resource Group should be started.

NOTE The Resource Group name is normally `ov-server`, but you can also choose an alternative name.

You will get the following return codes:

`0` - HPOM application was started successfully.

`1` - Start operation failed.

To Stop the HA Resource Group

To stop the HA Resource Group, enter:

/opt/OV/bin/ovharg_config ov-server -stop <*node name*>

where <*node name*> is the name of the node on which the HA Resource Group should be stopped.

You will get the following return codes:

`0` - HPOM application was stopped successfully.

`1` - Stop operation failed.

To Switch the HA Resource Group

To switch the HA Resource Group from one node to another, enter:

/opt/OV/bin/ovharg_config ov-server -switch <*node name*>

where <*node name*> is the name of the node to which the HA Resource Group should be switched.

You will get the following return codes:

`0` - HPOM application was switched successfully.

`1` - Switch operation failed.

Manual Operations for Starting, Stopping, and Monitoring HP Operations Management Server in a Cluster Environment

The HP Operations management server in a cluster environment is represented as an application which is a part of the HA 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.

To Start HP Operations Management Server

To start the HP Operations management server, enter:

```
/opt/OV/lbin/ovharg -start ov-server
```

You will get the following return codes:

`0` - HP Operations management server was started successfully.

`1` - Start operation failed.

To Stop HP Operations Management Server

To stop the HP Operations management server, enter:

```
/opt/OV/lbin/ovharg -stop ov-server
```

You will get the following return codes:

`0` - HP Operations management server was stopped successfully.

`1` - Stop operation failed.

To Monitor HP Operations Management Server

The Cluster Manager permanently monitors the HP Operations management server by using the following action:

```
/opt/OV/lbin/ovharg -monitor ov-server
```

If the HP Operations management server is running properly, this command returns `0`, otherwise it returns `1`, which causes switching of the `ov-server` HA Resource Group to another cluster node.

To Disable HP Operations Management Server Monitoring

However, there are situations in which you need the HP Operations management server to be stopped, while all other parts of the HA Resource Group should continue to run. In such situations, you will need to disable monitoring manually.

To disable the HP Operations management server monitoring manually, use the `disable` option:

```
/opt/OV/lbin/ovharg -monitor ov-server disable
```

When the monitoring process is disabled manually, you will be able to stop the HP Operations management server. This will *not* cause the HA Resource Group to be switched to another cluster node. The Cluster Manager will *not* detect this event, because the return code of the monitor command will still be `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 runs properly, use the following command:

```
/opt/OV/bin/OpC/opcsv
```

- If the management server is running, enable monitoring again by using the following command:

  ```
  /opt/OV/lbin/ovharg -monitor ov-server enable
  ```

- 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 decoupled management server configuration, you can temporarily disable monitoring of the Oracle HA Resource Group with the following command:

```
/opt/OV/lbin/ovharg -monitor ov-oracle disable
```

To enable Oracle HA Resource Group monitoring, use the `enable` option:

```
/opt/OV/lbin/ovharg -monitor ov-oracle enable
```

To Monitor the Oracle Database

In a decoupled management server configuration, the HP Operations management server and the Oracle database server are configured as separate HA Resource Groups. Nevertheless, the HP Operations management server monitor scrips also monitor the Oracle HA Resource Group.

The management server monitor scripts react in the following ways to the current status of the Oracle HA Resource Group:

- **Oracle HA Resource Group is not yet running**

  If the HP Operations HA Resource Group is started before the Oracle HA Resource Group is running, the HP Operations HA Resource Group starts, but the management server processes are not started.

  As soon as the Oracle HA Resource Group is running, the server processes are started and the command returns `0`.

- **Oracle HA Resource Group is stopped**

  If the Oracle HA Resource Group is stopped, is switched, or is failed over, the HP Operations management server processes are also stopped.

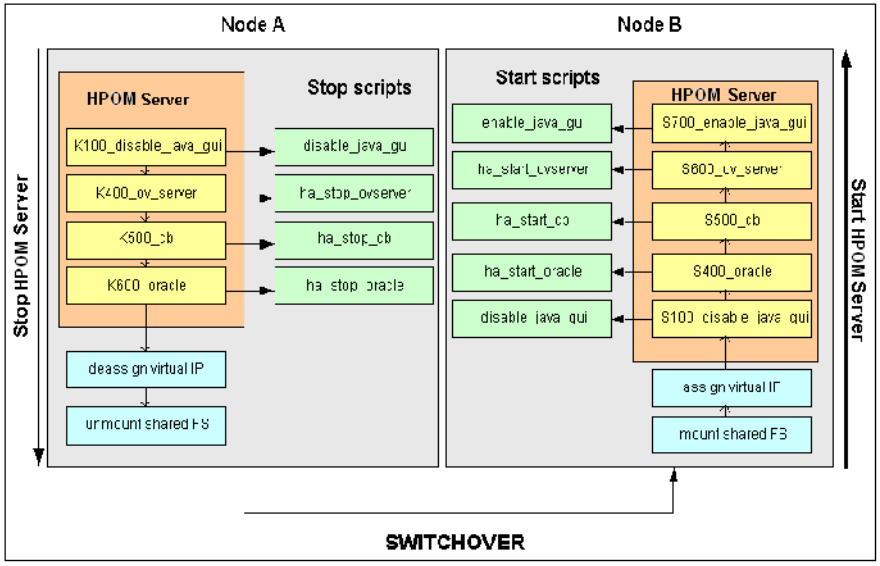
- **Oracle HA Resource Group is restarted**

  As soon as the Oracle HA Resource Group is running, the server processes are started and the command returns `0`.

Switchover Example

The example illustrates the switchover procedure in a two node cluster in which the HA 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 13-3.

Figure 13-3 Switchover Procedure



Switchover Procedure

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 procedure is conducted as follows:

1. On `Node A`:
   a. Cluster Manager stops the HP Operations management server running as an application by performing the following action:

      ```
      /opt/OV/lbin/ovharg -stop 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`:
   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 ov-server
      ```

      The `ovharg` script reads all start links and executes start scripts in the appropriate sequence.

The Resource Group `ov-server` is now active on `Node B`.

Troubleshooting HPOM in a Cluster Environment

HA Resource Group Cannot Be Started on a Particular Cluster Node

Using the Tracing Option

If HA Resource Group cannot be started on one of cluster nodes, first try to resolve this problem by enabling the trace option. Perform the following steps:

1. Make sure that HA Resource Group is not running on any cluster node. If the HA Resource Group is running, stop it with the following command:

   /opt/OV/lbin/ovharg_config ov-server -stop <*node name*>

2. Enable tracing by entering:

   /opt/OV/lbin/ovharg -tracing ov-server enable

3. Enter the following command:

   /opt/OV/lbin/ovharg_config ov-server -start <*node name*>

If you receive the output `0`, the HP Operations management server has been successfully started. If the output is `1`, the start operation failed. To find out more about the causes of the problem, check the output of the trace file:

`/var/opt/OV/hacluster/ov-server/trace.log`

If the HP Operations management server failed to start, perform the steps described in the section entitled “Manual Operations” on page 476.

Manual Operations

If the HP Operations management server could not be started properly, it is possible to start the whole HP Operations management server or parts of it manually.

To start the whole 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. Run the command:

   `/opt/OV/lbin/ovharg -start ov-server`

If you receive the output `0`, the HP Operations management server has been successfully started. If the output is `1`, the start operation failed. Check the output of the trace file to find out the problem causes.

If you failed to start the whole HP Operations management server, perform the steps described in the section entitled "Using Links".

Using Links

You can start any of the HP Operations management server components by using the links placed in the `/var/opt/OV/hacluster/ov-server` directory. When activated, these scripts perform start, stop, and monitor operations for the HP Operations management server components. The links are given in the following format:

`S<index>_<operation name>`	Start Links
`K<index>_<operation name>`	Stop Links
`M<index>_<operation name>`	Monitor Links

Where `S`, `K`, or `M` designate the action to be executed (start, stop, or monitor), `<index>` is represented by a number which indicates the sequence of execution, while `<operation name>` indicates the operation to be executed.

NOTE It is very important to execute links in the correct sequence defined by *<index>*.

The following tables show the links that are used within the cluster High Availability concept.

Table 13-2 Start Links

Link Name	Script Location	Action Description
S100_disable_java_gui	/opt/OV/bin/OpC/utils/disable_java_gui	Disables the Java GUI
S400_oracle	/opt/OV/bin/OpC/utils/ha/ha_start_oracle	Starts Oracle
S500_cb	/opt/OV/bin/OpC/utils/ha/ha_start_cb	Starts the BBC communication broker
S600_ov_server	/opt/OV/bin/OpC/utils/ha/ha_start_ovserver	Starts the HPOM management server
S700_enable_java_gui	/opt/OV/bin/OpC/utils/enable_java_gui	Enables the Java GUI

Table 13-3 Stop Links

Link Name	Script Location	Action Description
K100_disable_java_gui	/opt/OV/bin/OpC/utils/disable_java_gui	Disables the Java GUI
K400_ov_server	/opt/OV/bin/OpC/utils/ha/ha_stop_ovserver	Stops the HPOM management server
K500_cb	/opt/OV/bin/OpC/utils/ha/ha_stop_cb	Stops the BBC communication broker

Table 13-3 Stop Links (Continued)

Link Name	Script Location	Action Description
K600_oracle	/opt/OV/bin/OpC/utils/ha/ha_stop_oracle	Stops Oracle

Table 13-4 Monitor Links

Link Name	Script Location	Action Description
M100_oracle	/opt/OV/bin/OpC/utils/ha/ha_mon_oracle	Monitors Oracle
M200_cb	/opt/OV/bin/OpC/utils/ha/ha_mon_cb	Monitors the BBC communication broker
M300_ov_server	/opt/OV/bin/OpC/utils/ha/ha_mon_ovserver	Monitors the HPOM management server

Monitored HP Operations Management Server Processes Cause an Unwanted Switchover of the HP Operations Management Server HA Resource Group

Changing the List of Monitored HP Operations Management Server Processes

If specific monitored processes abort and cause switchover of the HP Operations management server HA Resource Group, remove these processes from the list of monitored processes by performing the following procedure:

1. Open the `/opt/OV/bin/OpC/utils/ha/ha_mon_ovserver` file for editing.
2. At the end of the file, look for the list of monitored HP Operations management server processes and comment out all aborting processes. These processes will not be monitored anymore.

Trap Interception in a Cluster Environment

On the active cluster node, 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 HA Resource Group is switched again.

There is no need to manually stop the `opctrapi` process when the HA Resource Group switches. The process continues to attempt connecting to `pmd` because the configuration setting `OPC_HA_TRAPI` is set to `TRUE` in the `eaagt` namespace. It is set automatically during the installation of HPOM in a cluster environment. If the setting is not enabled, `opctrapi` would exit after several connection attempts and you would receive HPOM messages notifying you of this problem when the agent starts again.

Preconfigured Elements

Policies and Policy Groups

HA Management Server policy group

- HA Virtual Management Server

  This subgroup is assigned to the Virtual IP and contains the following policies for the virtual management server node:

  - SNMP 7.01 Traps
  - SNMP ECS Traps

  When distributing the trap policy, it is automatically distributed to all cluster nodes. Because the policy is assigned to the Virtual IP, it is only active on the cluster node where the HA Resource Group ov-server is currently active.

- HA Physical Management Server

  This subgroup contains the following policies for the physical management server:

  - distrib_mon
  - opcmsg (1|3)
  - Cron
  - disk_util
  - proc_util
  - mondbfile

The policy group HA Management Server contains the HP Operations management server policies for cluster environments and consists of the following policy subgroups:

Files

The HP Operations Management Server HA Files

❑ **HP Operations management server files**

The HP Operations management server HA files are located in the following directory:

`/opt/OV/bin/OpC/utils/ha`

- `ha_mon_cb`
- `ha_mon_oracle`
- `ha_mon_ovserver`
- `ha_remove`
- `ha_start_cb`
- `ha_stop_oracle`
- `ha_stop_ovserver`

HP Software HA scripts

❑ `/opt/OV/lbin/ovharg`

❑ `/opt/OV/bin/ovharg_config`

HP Software Cluster Specific HA Files

❑ **HP Serviceguard Files**

HP Serviceguard specific files are located in the following directory:

`/opt/OV/lbin/clusterconfig/mcsg`

- `ov_rg.cntl`
- `ov_rg.conf`
- `ov_rg.mon`

❑ **Sun Cluster Files**

The following Sun Cluster specific files are located in the directory `/opt/OV/lbin/clusterconfig/sc3`:

- `monitor_start`
- `monitor_stop`
- `start`
- `stop`
- `probe`
- `gettime`
- `HP.OVApplication`

The following Sun Cluster specific files are located in the directory `/opt/OV/lbin/clusterconfig/sc3/OVApplication`:

- `monitor`
- `online`
- `offline`

A About HPOM Managed Node APIs and Libraries

In this Appendix

This chapter provides information about the following:

- About HPOM APIs on Managed Nodes
- About HPOM Managed Node Libraries

About HPOM APIs on Managed Nodes

Table A-1 describes commands associated with application program interfaces (APIs) on HP Operations Manager (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)`	Feeds the current value of a monitored object into 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 detailed information about these commands, see the man pages.

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*.

About HPOM Managed Node Libraries

NOTE

Customer applications must be linked to HPOM using the libraries, 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.

HPOM C functions are available in a shared library. The related definitions and return values are defined in the HPOM include file, `opcapi.h`. For the location of the include file, the required libraries and the makefile on your managed node platform, see the *HPOM HTTPS Agent Concepts and Configuration Guide*.

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 About HPOM Tables and Tablespaces in the Database

In this Appendix

This appendix describes HP Operations Manager (HPOM) tables and tablespaces in databases.

For detailed information about the HPOM tables in the RDBMS, see the *HPOM Reporting and Database Schema*.

About 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.

To increase the size of a tablespace, you must add a datafile of a particular size to the tablespace. You can do this interactively using the Oracle tool, Server Manager, or using the `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

About non-HPOM Tables and Tablespaces

Table B-2 describes non-HPOM tablespaces.

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 About HPOM Audit Areas

In this Appendix

This appendix describes HP Operations Manager audit areas.

HPOM Audit Areas

The following table describes the HPOM audit areas:

Table C-1 HPOM Audit Areas

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
Authorization - Login	User connection established successfully	Disabled by default	LOGIN_SUCCESS
Authorization - Login	User connection failed	MAJOR	LOGIN_FAILURE
Authorization - Login	User logon from the Java GUI succeeded - Client process	SERIOUS	LOGIN_SUCCESS
Authorization - Login	User logon from the Java GUI succeeded	SERIOUS	LOGIN_SUCCESS
Authorization - Login	User logon from the Java GUI failed	MAJOR	LOGIN_FAILURE
Authorization - Logout	User connection closed	Disabled by default	LOGOUT
Authorization - Logout	User logout from the Java GUI - Client process	MAJOR	LOGOUT
Authorization - Logout	User logout from the Java GUI	MAJOR	LOGOUT
Authorization - User	Modify user	SERIOUS	OM_CFG_CHG_USER
Authorization - User	Delete user	MAJOR	OM_CFG_DEL_USER

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
Authorization - User	Assigning user responsibility	SERIOUS	OM_CFG_USER_RESP
Authorization - User	Deassigning user responsibility	SERIOUS	OM_CFG_USER_RESP
Authorization - User	Change the user password	SERIOUS	OM_CFG_USER_PWD_CHANGE
Authorization - User	Create the user with admin privileges	SERIOUS	OM_CFG_ADD_USER
Authorization - User	Create the user	MAJOR	OM_CFG_ADD_USER
Authorization - User	Assign the user profile to the user/profile	SERIOUS	OM_CFG_CHG_USER
Authorization - User	Deassign the user profile from the user/profile	SERIOUS	OM_CFG_CHG_USER
Authorization - User	Assigned the application to the user	MINOR	OM_CFG_CHG_USER
Authorization - User	Deassigned the application from user	MINOR	OM_CFG_CHG_USER
Authorization - User	Assign the application group to the user	MINOR	OM_CFG_CHG_USER
Authorization - User	Deassign the application group from the user	MINOR	OM_CFG_CHG_USER
Authorization - Profile	Create the profile	MINOR	OM_CFG_ADD_USER_PROFILE

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
Authorization - Profile	Copy the profile	MINOR	none
Authorization - Profile	Modify the profile	MINOR	OM_CFG_CHG_USER_PROFILE
Authorization - Profile	Delete the profile	MAJOR	OM_CFG_DEL_USER_PROFILE
Authorization - Profile	Assigned the application to the user profile	MINOR	OM_CFG_CHG_PROFILE
Authorization - Profile	Deassigned the application from the user profile	MINOR	OM_CFG_CHG_PROFILE
Authorization - Profile	Assign the application group to the profile	MINOR	OM_CFG_CHG_PROFILE
Authorization - Profile	Deassign the application group from the profile	MINOR	OM_CFG_CHG_PROFILE
Authorization - Certificate	New certificate request created	MAJOR	OM_SV_REQUEST_CERTIFICATE
Authorization - Certificate	Certificate request granted	SERIOUS	OM_SV_GRANT_CERT_REQUEST
Authorization - Certificate	Certificate request denied	MAJOR	OM_SV_DENY_CERT_REQUEST
Authorization - Certificate	Certificate request deleted	MAJOR	OM_SV_DEL_CERT_REQUEST
Authorization - Certificate	Generic certificate event	MINOR	none

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Message	Operator owned the message	MINOR	OM_MESSAGE_OWN
HPOM objects - Message	Operator disowned the message	MINOR	OM_MESSAGE_OWN
HPOM objects - Message	Message was forwarded to the Trouble Ticket interface	MINOR	OM_MSG_FWD_NS_IF
HPOM objects - Message	Message was forwarded to the Notification Service interface	MINOR	OM_MSG_FWD_TT_IF
HPOM objects - Message	User deletes one or multiple HPOM messages	MINOR	OM_MSG_DEL
HPOM objects - Message	Operator acknowledged the list / all HPOM messages	MINOR	OM_MSG_MULTI_ACK
HPOM objects - Node	Create the node	MINOR	OM_CFG_ADD_NODE
HPOM objects - Node	Modify the node	MINOR	OM_CFG_CHG_NODE
HPOM objects - Node	Delete the node	MAJOR	OM_CFG_DEL_NODE
HPOM objects - Node	Assigned the policy to the node	MINOR	OM_CFG_CHG_NODE

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Node	Deassigned the policy from the node	MINOR	OM_CFG_CHG_NODE
HPOM objects - Node	Assigned the policy to the node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM objects - Node	Deassigned the policy from the node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM objects - Node	Assigned the policy group to the node	MINOR	OM_CFG_CHG_NODE
HPOM objects - Node	Deassigned the policy group from the node	MINOR	OM_CFG_CHG_NODE
HPOM objects - Node	Assigned the policy group to the node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM objects - Node	Deassigned the policy group from the node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM objects - Node	Assigned the category to the node	MINOR	OM_CFG_CHG_NODE
HPOM objects - Node	Deassigned the category from the node	MINOR	OM_CFG_CHG_NODE
HPOM objects - Node	Subagent installed	SERIOUS	OM_SUBAGT_INSTALL
HPOM objects - Node	Subagent deinstalled	SERIOUS	OM_SUBAGT_DEINSTALL
HPOM objects - Node	Subagent reinstalled	SERIOUS	OM_SUBAGT_INSTALL

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Node	Subagent activated	SERIOUS	OM_SUBAGT_INSTALL
HPOM objects - Node	Agent software deployed to the node	SERIOUS	OM_AGT_SW_INSTALL
HPOM objects - Node	Agent software removed from the node	SERIOUS	OM_AGT_SW_DEINSTALL
HPOM objects - Node	Updated MoM policy deployed	SERIOUS	OM_AGT_MGRCONF_DEPLOY
HPOM objects - Node	Instrumentation deployed to the managed node	SERIOUS	OM_AGT_INSTR_DEPLOY
HPOM objects - Application	Start the terminal application	MAJOR	OM_TERMINAL_APP_LAUNCH
HPOM objects - Application	Start the application	MAJOR	none
HPOM objects - Application	Creation of the HPOM application	MINOR	OM_CFG_ADD_APPL
HPOM objects - Application	Modify the HPOM application	MINOR	OM_CFG_CHG_APPL
HPOM objects - Application	Delete the HPOM application	MAJOR	OM_CFG_DEL_APPL
HPOM objects - External application	Register to MSI	MINOR	OM_SV_REGISTER_MSI

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - External application	Unregister from MSI	MINOR	OM_SV_REGISTER_MSI
HPOM objects - Config	Config download performed	MINOR	OM_SV_HIST_MSG_DOWNLOAD
HPOM objects - Config	Config upload performed	SERIOUS	OM_SV_HIST_MSG_UPLOAD
HPOM objects - Config	Config upload performed	SERIOUS	OM_CFG_UPLOAD
HPOM objects - Config	Modification of the database maintenance config	SERIOUS	OM_CFG_DB_MAINTENANCE
HPOM objects - Config	Modification of the management server config	SERIOUS	OM_CFG_DB
HPOM objects - Config	Config download performed	MINOR	OM_CFG_DOWNLOAD
HPOM objects - Config	Administrator activated heartbeat monitoring for the node	SERIOUS	OM_CFG_CHG_NODE_HEARTBEAT
HPOM objects - Config	Administrator deactivated heartbeat monitoring for the node	SERIOUS	OM_CFG_CHG_NODE_HEARTBEAT
HPOM objects - Config	Administrator changed the heartbeat monitoring interval for the node	SERIOUS	OM_CFG_CHG_NODE_HEARTBEAT

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Config	Generic policies uploaded from the directory	MAJOR	OM_CFG_UPLOAD_POLICY_TYPE
HPOM objects - Config	Generic policies uploaded from the file	MINOR	OM_CFG_UPLOAD_POLICY_TYPE
HPOM objects - Config	Enable duplicate message suppression	SERIOUS	OM_CFG_DUP_MSG_SUPPRESS
HPOM objects - Config	Disable duplicate message suppression	SERIOUS	OM_CFG_DUP_MSG_SUPPRESS
HPOM objects - Config	Change management server global options: Parallel distribution	SERIOUS	OM_CFG_MISC
HPOM objects - Config	Service Navigator configuration was read	MAJOR	OM_CFG_READ_SERVNAV
HPOM objects - Config	Service Navigator configuration was changed	SERIOUS	OM_CFG_WRITE_SERVNAV
HPOM objects - Config	Backup was made	MINOR	OM_SV_BACKUP
HPOM objects - Config	Customized startup message enabled	MINOR	OM_STARTUPMSG
HPOM objects - Config	Customized startup message disabled	MINOR	OM_STARTUPMSG
HPOM objects - Config	Customized startup message modified	MINOR	OM_STARTUPMSG

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Config	Customized startup message deleted	MINOR	OM_STARTUPMSG
HPOM objects - Other	Created the new category	MINOR	OM_CFG_ADD_CATEGORY
HPOM objects - Other	Modified the category	MINOR	OM_CFG_CHG_CATEGORY
HPOM objects - Other	Deleted the category	MAJOR	OM_CFG_DEL_CATEGORY
HPOM objects - Other	Generic policy type registered	MINOR	OM_CFG_ADD_POLICY_TYPE
HPOM objects - Other	Generic policy type modified	MINOR	OM_CFG_CHG_POLICY_TYPE
HPOM objects - Other	Generic policy type deleted	MAJOR	OM_CFG_DEL_POLICY_TYPE
HPOM objects - Other	Create the application group	MINOR	OM_CFG_ADD_APPL_GRP
HPOM objects - Other	Modify the application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM objects - Other	Delete the application group	MAJOR	OM_CFG_DEL_APPL_GRP
HPOM objects - Other	Assigned the application to the application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM objects - Other	Deassigned the application from the application group	MINOR	OM_CFG_CHG_APPL_GRP

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Other	Assign the application group to the application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM objects - Other	Deassign the application group from the application group	MINOR	OM_CFG_CHG_APPL_GRP
HPOM objects - Other	Create the condition	MINOR	OM_CFG_CHG_POLICY
HPOM objects - Other	Delete the condition	MINOR	OM_CFG_CHG_POLICY
HPOM objects - Other	Add/Set the instruction interface	MINOR	OM_CFG_DEL_INSTR_IF
HPOM objects - Other	Copy the instruction interface	MINOR	OM_CFG_CPY_INSTR_IF
HPOM objects - Other	Modify the instruction interface	MINOR	OM_CFG_CHG_INSTR_IF
HPOM objects - Other	Delete the instruction interface	MAJOR	OM_CFG_DEL_INSTR_IF
HPOM objects - Other	New message group created	MINOR	OM_CFG_ADD_MSG_GRP
HPOM objects - Other	Message group modified	MINOR	OM_CFG_CHG_MSG_GRP
HPOM objects - Other	Message group name modified	SERIOUS	OM_CFG_CHG_MSG_GRP

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Other	Message group deleted	MINOR	OM_CFG_DEL_MSG_GRP
HPOM objects - Other	Message group deleted	MAJOR	OM_CFG_DEL_MSG_GRP
HPOM objects - Other	Node layout hierarchy created	MINOR	OM_CFG_NODE_LAYOUT
HPOM objects - Other	Node layout hierarchy modified	MINOR	OM_CFG_NODE_LAYOUT
HPOM objects - Other	Node layout hierarchy deleted	MAJOR	OM_CFG_NODE_LAYOUT
HPOM objects - Other	Layout group created	MINOR	OM_CFG_LAYOUT_GRP
HPOM objects - Other	Layout group modified	MINOR	OM_CFG_LAYOUT_GRP
HPOM objects - Other	Layout group deleted	MAJOR	OM_CFG_LAYOUT_GRP
HPOM objects - Other	Create the notification schedule	MINOR	OM_CFG_CHG_NOTIFY_SCHEDULE
HPOM objects - Other	Modify the notification schedule	MINOR	OM_CFG_CHG_NOTIFY_SCHEDULE
HPOM objects - Other	Delete the notification schedule	MINOR	OM_CFG_CHG_NOTIFY_SCHEDULE
HPOM objects - Other	Create the notification service	MINOR	OM_CFG_CHG_NOTIFY_SERVICE

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Other	Modify the notification service	MINOR	OM_CFG_CHG_NOTIFY_SERVICE
HPOM objects - Other	Delete the notification service	MINOR	OM_CFG_CHG_NOTIFY_SERVICE
HPOM objects - Other	Create the node group	MINOR	OM_CFG_ADD_NODE_GRP
HPOM objects - Other	Modify the node group	MINOR	OM_CFG_ADD_NODE_GRP
HPOM objects - Other	Delete the node group	MAJOR	OM_CFG_ADD_NODE_GRP
HPOM objects - Other	Change the MSI setting - Enable	SERIOUS	OM_CFG_CHG_MSI
HPOM objects - Other	Change the MSI setting - Disable	SERIOUS	OM_CFG_CHG_MSI
HPOM objects - Other	Change the MSI setting - Allowing for externally defined actions	SERIOUS	OM_CFG_CHG_MSI
HPOM objects - Other	Assigned the category to the policy	MINOR	OM_CFG_CHG_POLICY
HPOM objects - Other	Deassigned the category from the policy	MINOR	OM_CFG_CHG_POLICY
HPOM objects - Other	Assigned the category to the policy group	MINOR	OM_CFG_CHG_POLICY_GRP
HPOM objects - Other	Deassigned the category from the policy group	MINOR	OM_CFG_CHG_POLICY_GRP

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM objects - Other	Created the category directory under the instrumentation directory	MINOR	OM_CFG_ADD_CATEGORY
HPOM objects - Other	Removed the category directory under the instrumentation directory, if existing	MINOR	OM_CFG_DEL_CATEGORY
HPOM objects - Other	Created the policy group	MINOR	OM_CFG_ADD_POLICY_GRP
HPOM objects - Other	Assigned the node to the node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM objects - Other	Deassigned the node from the node group	MINOR	OM_CFG_CHG_NODE_GRP
HPOM objects - Other	New policy created	MINOR	OM_CFG_ADD_POLICY
HPOM objects - Other	Policy modified	MINOR	OM_CFG_CHG_POLICY
HPOM objects - Other	Policy deleted	MAJOR	OM_CFG_DEL_POLICY
HPOM objects - Other	Policy edited by using the `poledit` application	MINOR	OM_CFG_CHG_POLICY
HPOM script/binaries access - Execute	CLI started	MINOR	none

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM script/binaries access - Execute	Run the scheduled action	MAJOR	OM_AGT_RUN_SCHED_ACT
HPOM script/binaries access - Execute	License check failed when adding the new node	MAJOR	OM_LICENSE_CHECK_FAILURE
HPOM script/binaries access - Execute	License check failed when adding the new agentless node	MAJOR	OM_LICENSE_CHECK_FAILURE
HPOM script/binaries access - Execute	Nightly license check failed	MAJOR	OM_LICENSE_CHECK_FAILURE
HPOM processes - Startup	Administrator started the HP Operations agent software locally	MINOR	OM_AGT_START
HPOM processes - Startup	Administrator started the HP Operations agent software remotely	MINOR	OM_AGT_START
HPOM processes - Startup	Administrator started up the HP Operations management server software	MAJOR	OM_SV_START

Table C-1 HPOM Audit Areas (Continued)

Audit Area	Use Case	Default Audit Level (Minor, Major, Serious, Internal)	ovoconf variable in audit name space
HPOM processes - Shutdown	Administrator shut down the HP Operations management server software	SERIOUS	OM_SV_STOP
HPOM processes - Shutdown	Administrator shut down the HP Operations agent software locally	SERIOUS	OM_AGT_STOP_ON_SV
HPOM processes - Shutdown	Administrator shut down the HP Operations agent software remotely	MAJOR	OM_AGT_STOP

D About HPOM Man Pages

In this Appendix

This appendix describes the man pages available in the following areas:

- Man Pages in HPOM
- Man Pages for HPOM APIs
- Man Pages for HP Operations Service Navigator
- Man Pages for the HPOM Developer's Kit APIs

Accessing and Printing Man Pages

You can access the HPOM man pages from the command line, from online help, or in HTML format on your management server.

To Access an HPOM Man Page from the Command Line

To access an HPOM man page from the command line, enter the following:

man <*manpagename*>

To Print a Man Page from the Command Line

To print an HPOM man page from the command line, enter the following:

man <*manpagename*> | col -lb | lp -d *printer_name*

To Access the Man Pages in HTML Format

To access the HPOM man pages in HTML format, from your Internet browser, open the following location:

`http://<management_server>:3443/ITO_MAN`

In this URL, <*management_server*> is the fully qualified hostname of your management server.

Man Pages in HPOM

This section describes man pages in HPOM.

Table D-1 HPOM Man Pages

Man 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 HP Operations agent software.
ito_op(1M)	Launches the HPOM Java-based operator or Service Navigator GUI.
ito_op_api_cli(1M)	Enables calling the Java GUI Remote APIs.
opcbackup_offline(1M)	Interactively saves 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.
opcrecover_offline(1M)	Interactively recovers the HPOM environment for Oracle.
opcrecover_offline(5)	Recovers the HPOM configuration.
opcack(1M)	Externally acknowledges active messages.
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 HP Operations agent.
opcadddbf(1M)	Adds a new datafile to an Oracle tablespace.
opcagt(1M)	Administers agent processes on a managed node.

Table D-1 HPOM Man Pages (Continued)

Man Page	Description
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 into the database.
opccltconfig(1M)	Configures HPOM client filesets.
opcconfig(1M)	Configures an HPOM management server.
opccsa(1M)	Provides the functionality for listing, mapping, granting, denying and deleting specified certificate requests.
opccsacm(1M)	Performs the ovcm's functionality for manually issuing new node certificate and 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 destroys the HPOM database scheme.
opcdbpwd(1M)	Changes the password of the HPOM database user opc_op.
opcdbsetup(1M)	Creates the tables in the HPOM database.
opcdcode(1M)	Views HPOM encrypted policy files.
opcerr(1M)	Displays instruction text for HPOM error messages.
opcgetmsgids(1m)	Gets message IDs to an original message ID.
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 into the HPOM database.

Table D-1 HPOM Man Pages (Continued)

Man Page	Description
opcinstrumcfg(1M)	Manages category info in the filesystem and database level simultaneously.
opcmack(1)	Acknowledges an HPOM message by specifying the message ID.
opcmom(4)	Provides an overview of HPOM MoM functionality.
opcmomchk(1)	Checks syntax of MoM 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.
opcpat(1)	Tests a program for HPOM pattern matching.
opcragt(1M)	Remotely administers 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)	Administers HPOM manager services.
opcsw(1M)	Sets the software status flag in the HPOM database.
opcswitchuser(1M)	Switches the ownership of the HP Operations agents.
opcpolicy(1M)	Maintains policies in files.
opcpolicy(1M)	Enables and disables policies.
opctmpldwn(1M)	Downloads and encrypts HPOM message source policies.
opcwall(1)	Sends a message to currently logged in HPOM users.
ovocomposer(1M)	Performs tasks related to OV Composer.
ovocomposer(5)	Describes the Correlation Composer, an HPOM event correlation feature.

Table D-1 HPOM Man Pages (Continued)

Man Page	Description
`ovtrap2opc(1M)`	Converts the `trapd.conf` file and the HPOM policy file.

Man Pages for HPOM APIs

This section describes man pages for HPOM application program interfaces (APIs).

Table D-2 HPOM API Man Pages

Man 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.

Man Pages for HP Operations Service Navigator

This section describes man pages for the HP Operations Service Navigator.

Table D-3 Service Navigator Man Pages

Man Page	Description
`opcservice(1M)`	Configures HP Operations Service Navigator.
`opcsvcattr (1M)`	Add, change or remove service attributes.
`opcsvcconv(1M)`	Converts service configuration files of HP Operations Service Navigator from the previous syntax to the Extensible Markup Language (XML).
`opcsvcdwn(1M)`	Downloads service status logs of HP Operations Service Navigator to a file.
`opcsvcterm(1M)`	Emulates an interface to HP Operations Service Navigator. The interface inputs Extensible Markup Language (XML) markup into `stdin` and outputs Extensible Markup Language (XML) markup to `stdout`.
`opcsvcupl(1M)`	Uploads service status logs of HP Operations Service Navigator into the HPOM database.

Man Pages for the HPOM Developer's Kit APIs

This section describes man pages for the HPOM Developer's Kit application program interfaces (APIs).

Table D-4 HPOM Developer's Toolkit Man Pages

Man Page	Description
`msiconf(4)`	Configures the HPOM message manager.
`opc_comif_close(3)`	Closes an instance of the communication queue interface.
`opc_comif_freedata(3)`	Displays free data that was allocated by `opc_comif_read()`.
`opc_comif_open(3)`	Opens an instance of the communication queue interface.
`opc_comif_read(3)`	Reads information from a queue.
`opc_comif_read_request(3)`	Reads information from a queue.
`opc_comif_write(3)`	Writes information into a queue.
`opc_comif_write_request(3)`	Writes information into a queue.
`opc_connect_api(3)`	Connects HPOM.
`opc_distrib(3)`	Distributes the HP Operations agent configuration.
`opcagtmon_send(3)`	Forwards the value of a monitored object to HPOM.
`opcagtmsg_api(3)`	Handles messages on HP Operations agents.
`opcanno_api(3)`	Manages HPOM message annotations.
`opcapp_start(3)`	Starts an HPOM application.
`opcappl_api(3)`	Configures and starts HPOM applications.
`opcapplgrp_api(3)`	Configures HPOM application groups.
`opcconf_api(3)`	Gets HPOM configuration.

Table D-4 HPOM Developer's Toolkit Man Pages (Continued)

Man Page	Description
opcdata(3)	Accesses the attributes of the HPOM data structure.
opcdata_api(3)	Describes how to access the HPOM data structure using the HPOM Data API.
opcif_api(3)	API to work with the HPOM Message Stream Interface.
opciter(3)	HPOM iterator to step through opcdata container.
opcmsg_api(3)	Manages HPOM messages.
opcmsggrp_api(3)	Manages HPOM message groups.
opcmsgregrpcond_api(3)	Creates and modifies HPOM message regroup conditions.
opcnode_api(3)	Configures HP Operations managed nodes.
opcnodegrp_api(3)	Configures HP Operations node groups.
opcnodehier_api(3)	Configures HP Operations node hierarchies.
opcprofile_api(3)	Configures HPOM user profiles.
opcregcond(3)	Accesses fields of the HPOM registration condition structure.
opcsvc_api(3)	C++ classes for Service Navigator.
opctempl_api(3)	Configures HPOM message source policies.
opctempfile_api(3)	Configures HPOM policies using policy files.
opctemplgrp_api(3)	Configures HPOM policy groups.
opctransaction_api(3)	Starts, commits, and rolls back transactions.
opcuser_api(3)	Configures HPOM users.
opcversion(3)	Returns the string of the HPOM library that is currently used.

D

E

H

I

J

N

O

Q

R

S

T

U

V

W

X

Z