HP Operations Manager for UNIX

Release Notes
for
HP Integrity Itanium-2 Servers

Version 8.35
Edition 24

Management Server on HP-UX Itanium

Manufacturing Part Number: None
November 2009

U.S.

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 in 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.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This product includes software written by Info-ZIP (http://www.info-zip.org/license.html)

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

This product includes lsof ©Copyright 2002 Purdue Research Foundation, West Lafayette, Indiana 47907.

Trademark Notices.

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

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

UNIX® is a registered trademark of the Open Group.

Contents

Contents

Contents

Contents

Contents

Contents

Contents

1 What's in This Version

Your company's business success relies on high-quality IT services and IT infrastructure agility. To keep your IT services available and well performing, you need a proven operations management solution that gives you control over your ever-changing IT infrastructure. That solution is HP Operations Manager for UNIX, or in short HPOM for UNIX. Due to a recent product name change, you will find in this document as well as in most other HPOM for UNIX related materials still the old names referenced: HP OpenView Operations for UNIX, or in short OVO/UNIX or just OVO.

HPOM for UNIX discovers, monitors, controls and reports on the availability and performance of your heterogeneous, large-scale IT environment. It consolidates information for all IT components that control your business: network, systems, storage, databases, and applications. With its service-driven approach, it shows what IT problems affect your business processes, helping you to focus on what's most important for your company's business success.

For a general overview about HPOM for UNIX's feature set, refer to the *Concepts Guide*, which is available in PDF format on the HP product manual website.

The following readme file describes the HPOM for UNIX media CD contents and layout and help you to locate products and documentation:

`/READMEHPUX_Itanium.txt`

For more information about the new features included with HPOM, download the HPOM for UNIX presentation *What's New in HP Operations Manager for UNIX 8* from the documentation web site listed below:

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

NOTE Check the following web site periodically for the latest versions of these release notes and other HPOM for UNIX manuals:

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

HP passport login is required to access the HP Software manuals.
Select "Operations Manager for UNIX" and version 8.0.

The Release Notes document is a summary of the latest status of HPOM. As new functionality is added, it will be reported here under the latest release number. Workarounds that are required can also be found in a section dedicated to each edition of these release notes. Cross references are also hyperlinks in pdf format and help you to find related sections more easily.

NOTE The overview of the latest HPOM patches is available at the following location:

`http://support.openview.hp.com/selfsolve/document/KM322544`

This section provides information about the following topics:

- New Announcements with Release Notes Edition 24
- New Features with HPOM for UNIX 8
- Changed Features
- Changed Features with HP Operations Manager for UNIX Developer's Toolkit

- Obsolete Features
- What's Not Yet Supported
- What's Not Supported
- Obsolescence Announcements for the Next HPOM for UNIX Release

New Announcements with Release Notes Edition 24

This section describes the new announcements and features that are introduced in this edition of the Release Notes.

HP Operations Management Server Enhancements

The following HP Operations management server patch is available for all supported operating system platforms:

Table 1-1 Management Server Patch 8.35

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
HPOM 8 consolidated server 8.35	PHSS_40357	PHSS_40355	ITOSOL_00715

The following enhancements are available with this patch:

- Since HPOM 8.33, it is possible to send the forward manager information to the trouble ticket if `OPC_TT_SHOW_FORW_MGR` is set to `TRUE`. However, if a message was not forwarded, no Forward Manager information was sent to trouble-ticketing system. Starting with HPOM 08.35, an empty string is sent as a Forward Manager information for non-forwarded messages.
- The `MGMTSV_KNOWN_MSG_NODE_NAME` variable can now be used in message key relations.

Supported High Availibility Environments

The following high availibility environments are now supported on the HP Operations management server:

- Veritas Cluster Server 5.0 on HP-UX 11.31
- HP Serviceguard 11.19 on HP-UX 11.31

Java UI Changes

The following Java GUI client patch is available:

Table 1-2 Java GUI Client Patch 8.35

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
Java GUI client 8.35	PHSS_40468	PHSS_40467	ITOSOL_00721

The following enhancement is available with this patch:

- A newer JRE 1.6.0_16 is provided for Microsoft Windows managed platforms.

New Features with HPOM for UNIX 8

This section describes the new announcements and features that are available with HPOM for UNIX for UNIX 8 compared with HPOM for UNIX 7.

Management Server

This section describes the new announcements and features available on the management server.

Supported Platforms

The following platforms and operating system versions are supported with HPOM for UNIX 8, and not with HPOM for UNIX 7:

- ❏ HP-UX Itanium 11.31
- ❏ HP-UX Itanium 11.23
- ❏ HP Integrity Virtual Machines for the HPOM Management Server running in a standalone and clustered configurations

For more information about installing HPOM for UNIX on HP-UX PA-RISC 11.31 and HP-UX Itanium 11.31, see "Installing HPOM for UNIX on HP-UX PA-RISC 11.31 and HP-UX Itanium 11.31" on page 121.

For additional information about installing HPOM for UNIX in an environment with existing HP software components installed, see also "New Installation of the HPOM for UNIX Management Server" on page 156.

Administration Enhancements

HPOM for UNIX administration enhancements include:

- New variables:
  - A new variable is introduced - `OPC_REPLACE_MGMTSV_VARIABLE_IN_CMAS`. If this variable is set to `TRUE`, the Message Manager replaces the `<$OPC_MGMTSV>` variable with the management server hostname in the custom message attribute's value when a message is received.
  - Messages can be suppressed before being passed to the MSI by setting the `OPC_SUPPRESS_OUTAGE_BEFORE_MSI` configuration variable to `TRUE`.
  - The default scripts for the policy-based message storm detection remove the template version string from the message source, which is needed for 8.51 or newer agents. In case older agents are used and some template names are ending with a version string, the new `OPC_POLICYSTORM_LEAVE_VERSION` setting can be set to `TRUE` in order to prevent the removal of the version string.
  - If the `OPC_TT_SHOW_FORW_MGR` configuration variable is set to `TRUE`, the name of the HP Operations server that forwarded the message to the current server is passed as a parameter to the trouble ticket system and the notification service system (after the number of suppressed duplicate messages).
  - Messages with duplicate message IDs can be suppressed before being passed to the MSI. If the `OPC_SUPPRESS_DUPL_MSGID_BEFORE_MSI` configuration variable is set to `TRUE`, `opcmsgm` maintains a list of message IDs, so that it can discard the messages with the already existing IDs before passing them to the MSI.
  - In a MoM environment an operator initiated action defined to be executed on `$OPC_MGMTSV` is by default executed on the primary server of the originating node.

By setting a newly introduced config variable OPC_DONT_REPLACE_MGMTSV_VARIABLE to TRUE, such action is executed on the management server from which it is initiated. This can be useful when messages are forwarded to another server and operators want to execute the action on their local server.

Enable this behavior as follows:

```
ovconfchg -ovrg server -ns opc -set \
OPC_DONT_REPLACE_MGMTSV_VARIABLE TRUE
```

— The internal web browser (embedded or ActiveX) can now be disabled for all operators by using the OPC_JGUI_INTERNBRW_DISABLED server variable. The following values are available with this variable: ACTIVEX (the ActiveX internal web browser is disabled), EMBEDDED (the embedded web browser is disabled), BOTH (ActiveX and embedded web browsers are disabled), and NONE (all web browsers are allowed, which is the same as not setting the variable).

— The value of the OPC_ACCEPT_ACTION_SIGNATURES_FROM variable is a string, which contains a comma-separated list of foreign server CORE IDs used in the MoM environment to inform the current management server that additional action signatures in the list can be accepted.

— If the OPC_RESTRICT_ACTIONS_WITH_FOREIGN_SIGNATURE variable is set to TRUE, all actions that are not signed by the current management server are discarded unless the CORE ID of the foreign management server is listed in the OPC_ACCEPT_ACTION_SIGNATURES_FROM variable.

— To instruct HPOM to use PAM as an authentication mechanism, set the OPC_USE_PAM_AUTH variable to TRUE.

If the OPC_USE_PAM_FAILED_LOGIN_COUNTER and OPC_USE_PAM_AUTH variables are set to TRUE, the failed login counting is enabled for each user.

— A new configuration setting is introduced - OPC_SUPPRESS_ERROR_LIST - a comma-separated list of values used to suppress the output of error messages to all error message output targets.

— The following four variables are introduced with the auto-granting feature of certificate request handling:

  — OPC_CSA_AUTOMATION: for enabling and disabling the automatic processing of certificate requests from HTTPS agents and allowing the automatic addition of systems to the HPOM for UNIX node bank before granting a certificate request.

  — OPC_CSA_ACTION_TIMEOUT: for configuring the maximum execution time period of PRE_ACTION and POST_ACTION (the default value being 60 seconds).

  — OPC_CSA_RULES: for specifying a list of rules and subnet patterns for automatic certificate processing.

  — OPC_CSA_NAT_RULES: for specifying a list of rules and subnet patterns for automatic certificate processing in a NATed environment.

— The MGMTSV_KNOWN_MSG_NODE_NAME template variable is introduced as an alternative to MSG_NODE_NAME. The only difference is that the newly introduced variable is resolved on the management server, and not on the agent, as it is the case with MSG_NODE_NAME.

— If the target server is unreachable, the MAX_ALIVE_TIMEOUT variable can be used together with the OPC_HTTPS_MSG_FORWARD=TRUE setting to determine the time after which a message is generated.

— When inst.sh is run non-interactively, its timeout (120 seconds) can be overridden by setting the OPC_TIME_OUT environment variable.

— Because under some circumstances `opcsvcam` fails to register to service events after connecting to `opcsvcm`, the `OPCSVCAM_REGISTER_RETRIES` variable is introduced to specify how often `opcsvcam` retries to register to service events after successfully connecting to `opcsvcm`.

— Message processing for count and suppress duplicates is improved. A new variable is introduced - `OPC_SUPPRESS_DUPL_MSG_KEY_ONLY`. If this variable is set to `TRUE`, the count and suppress duplicates check is performed only for messages, which have a message key defined.

A new `opcmsgm` thread is introduced for updating the counter.

— Updating the message text and severity is also possible if `OPC_UPDATE_DUPLICATED_MSGTEXT` and `OPC_UPDATE_DUPLICATED_SEVERITY` are set.

— Startup time of HPOM server processes is significantly improved because the name resolution is done in a separate thread of the Message Manager (`opcmsgm`). A new variable is introduced to completely disable the building of the IP address mapping table - `OPC_DISABLE_IP_MAPPING_TABLE`.

This enhancement also includes an improved message trace to show the IP address and node name for the purposes of troubleshooting.

— Aborted HPOM for UNIX processes can be restarted automatically and independently. The following new variables are introduced:

  — `OPC_RESTART_PROCESS`: If this variable is set to `TRUE`, the controlling process (`opcctlm` or `OVOareqsdr`) tries to restart aborted processes.

  — `OPC_RESTART_COUNT`: Defines how often the aborted server process should be restarted within the specified timeframe interval.

  — `OPC_RESTART_DELAY`: Defines the time the controlling process waits before it restarts the aborted server process.

  — `OPC_RESTART_TIMEFRAME`: Defines a timeframe during which the aborted process is restarted up to the specified amount of times.

— `opcragt` now supports parallel agent queries. The following new variables are introduced - `OPCRAGT_USE_THREADS` (informs `opcragt` to use multiple threads) and `OPCRAGT_MAX_THREADS` (defines how many agents can be contacted in parallel by `opcragt`).

Non-reachable nodes are now logged into `/var/opt/OV/share/tmp/OpC/mgmt_sv/opcragt-<parameter>-fail.log`

— Notification messages can now go directly to the history log. A new variable is introduced - `OPC_NOTIFICATION_LOGONLY`.

— The `OPC_SKIP_DCE_FORWARDING` variable is introduced, which if used together with `OPC_HTTPS_MSG_FORWARD=TRUE`, can improve forwarding performance.

— A new variable is introduced - `OPC_LOG_DROPPED_MSGS`. If this variable is set to `TRUE`, HPOM logs all dropped message errors (OpC40-648) to the `System.txt` file. HPOM discards messages received from the nodes, which are not managed by HPOM.

— The `OPC_CHECK_READFILE` variable is used for the `READFILE` (the file to be read) to be checked when the `EXEFILE` (the file to be executed) is specified in the logfile template.

NOTE For a detailed description of all new config variables, refer to the *Server Config Variables* document, which can be downloaded from the following location:

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

- It is possible to register for messages and message events at the same time by using the message change event interface. The new `OPCSVIF_MSG_EVENTS_ALL` define has been added for the interface type, as well as the new `OPC_MSG_EVENT_ALL_MSG` event mask, which allows getting both new messages and change events in one stream.
- If a policy is assigned to both a virtual node and a physical node, a warning is printed to `System.txt`, and a warning message is generated during the distribution.
- It is possible to set the `RES_RETRY` and `RES_RETRANS` configuration variables for the management server.
- The HP Operations management server copies the agent bundle XML file to the target node during the remote deployment. This is necessary for a proper switch of the agent to the HPOM for Windows management server later on.
- The `opclaygrp` tool is introduced to manage layout groups and node hierarchies. It enables to create, delete, list layout groups and node hierarchies and move layout groups within the same node hierarchy. See `opclaygrp` man page for more details on this utility.
- The `opcack` tool is enhanced to acknowledge messages based on different criteria, for example, severity, message group, message text string, etc. It can be used non-interactively with the `-c` option. See `opcack` man page for more details on this utility.
- `opcdbck` performance and usability are improved, so that the `opcdbck` output is now more readable and the tool reports only real errors.
- The database update algorithm was improved to reuse the `node_id` and `commit` once per message bulk. The time for database update was reduced.
- Server backup and restore scripts are updated to support the `log_archive_dest_n` parameter. The old `log_archive_dest` parameter is deprecated by Oracle 10g.
- `opc_recover` now works in a cluster environment.
- The `opcdbsetup` script now works with a non-default Oracle user and sets the `system` password for an Oracle user.
- The `opccfgupld` option is used for deleting templates, which do not exist in upload files. For example, in case of repetitive opccfgdwn/opccfgupld to synchronize a failover server, if templates are removed after a previous opccfgdwn on the active server the subsequent `opccfgupld -replace` does not remove them on the failover server. The options `-deloldtempls` and `-delalltempls` were added to enable this.
- For HTTPS agents, the `opcragt -cleanstart` functionality is added. The queue files and `opcragt` temporary files on the agent are cleared.
- Java API wrappers for *opcmon(3)* and *opcmsg(3)* for HTTPS agents.
- Improved heartbeat monitoring for HTTPS agents
- Discarded HPOM messages now contain the hostname of the unknown node in the corresponding error message logged in `system.txt`. OpC50-330 is now used instead of OpC50-29.
- Profile reports show which users have a certain profile assigned.
- `itochecker` properly handles nodes with multiple IP addresses, which resolve to the same node name.

  The `itochecker` report was enhanced as follows:

  — In a cluster environment, the `itochecker` report includes the output of the `ovdeploy -inv` command from all cluster nodes. The content of `/var/opt/OV/hacluster` is put in the `TAR` file and is also included in the report.

  — After upgrading the Oracle database, the `initopenview.ora` file is parsed correctly.

- The internal error message of `opccfgout` for nodes with unresolvable IP assigned is modified in such a way that the node name was added to the warning, so the warning can be filtered based on the node name.
- Motif Administrator GUI: Invisible Node Groups to keep user responsibility matrix configuration small, but use additional node group for other HPOM Administrator tasks.
- OS-SPI for HP-UX, Solaris, Windows, Linux, AIX and Tru64 HTTPS agent platforms.
- Improved Cluster Error Handling and Logging, see page 129.
- It is now possible to allow actions that were defined or modified in the agent MSI. In the `remactconf.xml` file, a new condition can be set:

  ```
  <if>
    <certified>msi</certified>
  </if>
  ```

  This means that either regular actions or MSI created actions (not modified) from an HTTPS node are allowed. On the other hand, actions from a DCE node are not allowed.
- To better deal with changed `OvCoreId`s (for example, because the agent was reinstalled), the following new error message and the variable are introduced:

  — `OpC40-649`

  If `OPC_LOG_DROPPED_MSGS` is set to `TRUE`, `opcmsgm` now also logs messages received from the nodes for which the `OvCoreId` is different from the one known to the management server.

  — `OPC_MSGFORW_SYNC_COREIDS`

  If the `OPC_MSGFORW_SYNC_COREIDS` variable is set to `TRUE`, the `OvCoreId` of a node is automatically updated by received messages in a MoM environment. When a message that was forwarded from another server is received, and the `OvCoreID` of the node from the message is different than the one in the database, the `OvCoreId` is automatically updated in the database and the `OpC40-664` internal message is sent to notify the operators.
- The agent hotfix deployment tool together with the PDF file is installed on the server with this patch:

  `/opt/OV/contrib/OpC/Hotfix_deployment_tool`
- So far, deploying templates, heartbeat polling, and getting status information of a node behind the firewall or proxy failed if the firewall or proxy between a server and an agent could not perform name resolution. Now it is possible to use an IP address to connect to a node by setting a new configuration variable - `OPC_COMM_USEIP_URI`.

NOTE For detailed information about configuration variables, see the latest edition of the HPOM Server Configuration Variables document, which is available for download from the following location:

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

- `listguis` now also displays template administrator sessions.
- The `ovoremove` script now asks if the database should be left intact during the HP Operations management server deinstallation.

API Enhancements:

HPOM for UNIX API enhancements include the following:

- New APIs for adding, modifying, and deleting custom message attributes for HPOM messages that are already stored in the HPOM Oracle database.

  These APIs are defined in `/opt/OV/include/opcsvapi.h`, their use is illustrated in example `/opt/OV/OpC/examples/progs/itomessage.c`.

- New functions of APIs:

  - HPOM Operator API

    The following API function is used for deleting the container element without deleting the object itself:

    `opcdata_unlink_element`

  - Trouble Ticket API

    For getting and modifying the trouble ticket interface, you can use the following API functions:

    `opctroubleticket_get`

    `opctroubleticket_set`

  - Instruction Text Interface API

    This API provides the following functions for configuring the instruction text interface:

    `opcinstruction_add()`: adds the specified instruction text interface to the HPOM database.

    `opcinstruction_del()`: deletes the specified instruction text interface.

    `opcinstruction_get()`: gets the full configuration of the instruction text interface.

    `opcinstruction_modify()`: modifies the specified instruction text interface.

NOTE The `opccfgttest` utility is improved to test `opcinstruction_*()` APIs.

  - Notification Service API

    For adding, deleting, getting, and modifying notification services, the following API functions are available:

    `opcnotiservice_add()`

    `opcnotiservice_del()`

    `opcnotiservice_get()`

    `opcnotiservice_modify()`

  - Notification Schedule API

    The following API functions are used for adding, deleting, getting, and modifying the notification schedule:

    `opcnotischedule_add()`

    `opcnotischedule_del()`

    `opcnotischedule_get()`

`opcnotischedule_modify()`

- Database Maintenance API and Management Server Configuration API

  For interacting with the database, the following API functions are used:

  `opcdbmaint_get()`

  `opcdbmaint_set()`

  `opcdbmgmtsv_set()`

  `opcdbmgmtsv_get()`

- Pattern Matching API

  For accessing the pattern matching code, which is needed for pattern matching tests, use:

  `opcpat_match`

Server CLI Enhancements

HPOM for UNIX server CLI enhancements include:

- New CLIs:
  - for getting and modifying the trouble ticket interface:

    `opctt -help | -status | -enable <TT call> | -disable`
  - for getting, adding, modifying, and deleting the instruction text interface:

    `opcinstrif -help | -add | -delete | -get | -modify | -list`
  - for adding, getting, modifying, and deleting notification services (including the schedule):

    `opcnotiservice -help | -add | -delete | -modify | -get | -list`

    `opcnotischedule -help | -add | -delete | -modify | -get | -list`
- The user responsibility matrix can now be modified by using the `opccfguser` command line interface as well. The `opccfguser` command line interface is enhanced with `assign_respons_user` for assigning responsibilities, `deassign_respons_user` for deassigning responsibilities, and `listrespons` for displaying all assigned responsibilities.
- Command Line Utility `opcownmsg`

  The `opcownmsg` command can be used for owning, disowning, and changing HPOM messages ownership.
- Command Line Utility `opctmpldwn`

  The `-dir` option has been implemented for the `opctmpldwn` command. Signing the file on the HPOM for UNIX server by adding a new parameter to the `opctmpldwn` command is also enabled.
- Command Line Utility `opcdelmsgs`

  The `opcdelmsgs` command can be used for deleting messages from the Message Manager queue, and it can be used while other management server processes are running, without the need to restart the server.

  `opcdelmsgs` can also be used for deleting elements from other queue files besides the message manager queue. It has been enhanced by adding the `-all` option (for deleting all elements of all types from the queue) and the `event_type` parameter (for selecting other event types).

  Note that it is also possible to delete queue entries based on time by using the `from` and `until` parameters.

  For more details refer to the `opcdelmsgs` usage information when entering the `-help` option.

- Command Line Utility `opccfguser`

  The `opccfguser` command can be used for adding, modifying, and removing a user, as well as for displaying user information.

- Command Line Utility `opcwall`

  Sending `opcwall` messages from the Java UI Console is enabled.

- Command Line Utility `opchbp`

  The interval of heartbeat monitoring can be changed by using the `opchbp` command.

- Command Line Utility `opccmachg`

  `opccmachg` is a command-line tool for handling Custom Message Attributes, making it possible to add, modify, remove, and list Custom Message Attributes.

  The `opccmachg` utility resides in `/opt/OV/bin/OpC`. For more information refer to the `opccmachg` man page.

- Command Line Utility `opcqschk`

  The `opcqschk` command can be used for verifying the status, version, number of items, and maximum allowed size of the queue file.

- Command Line Utility `opcqchk`

  Dumping contents of the queue file or interactively inspecting the queue file is enabled by using the `opcqchk` command.

- Avoiding duplicate `OvCoreId`s is enhanced in the following ways:

  — `itochecker` now checks for duplicate core IDs during the HPOM database check.

  — The new `opcdbidx` option `-ovcoreid` is added to check for duplicate `OvCoreId`s in the database.

  — `opcnode -chg_id` now checks if another node already uses the same `OvCoreID`, and in that case issues an error.

NOTE For command line interface changes and enhancements, refer to the corresponding manpages.

Security Enhancements

PAM failed login counter is implemented for each operator in the corresponding namespace to reduce the number of attempts to use invalid/expired passwords.

For example, if the `opc_adm` operator fails to log in five times, the following config parameters are set in the corresponding `user.opc_adm` name space (`ovrg = server`):

```
[user.opc_adm]
FAILED_LOGIN_ATTEMPT_COUNTER=5
LAST_FAILED_LOGIN_ATTEMPT=1197550378
LOGIN_ATTEMPT_DELAY=240
```

For more information, see "PAM Failed Login Counter Functionality" on page 114.

New ovoinstall Scripts

New `ovoinstall` scripts for the following operating system platforms are available for download:

- HP-UX PA-RISC 11.11, 11.23, and 11.31
- HP-UX Itanium 11.23 and 11.31
- Solaris 8, 9, and 10

The `ovoinstall` scripts can be downloaded from the following site:

`ftp://ovweb.external.hp.com/pub/cpe/ito/latest_ovoinstall/`

For detailed information about the updates, see the `README.txt` file that is located on the same site.

HTTPS Agent Installation Enhancements

Installation of the HTTPS agents was improved as follows:

- The HTTPS agent installation now detects and reports if the `rexec` or `remsh` service is not enabled to prevent the installation failure.
- The HTTPS agent installation on virtual cluster nodes is prevented to eliminate possible damage to the HPOM server.

Java GUI Client Version Control Feature

For more information about the Java GUI Client Version Control feature, see page 116.

Customizing XPL Config Variables Locally

It is now possible to customize threshold policy locally on the node using the XPL config variables file. For more information, refer to the *HTTPS Agent Concepts and Configuration Guide*.

Assignment of Services to User Profiles

The assignment of services to user profiles is disabled by default. To enable it, follow these steps:

1. Enable the feature of assigning services to user profiles by entering the following:

   ```
   ovconfchg -ovrg server -ns opc -set OPCSVC_CONSIDER_PROFILES TRUE
   ```

2. Restart the server processes:

   ```
   opcsv -start
   ```

3. To assign the services, enter the following:

   ```
   opcservice -assign <profile> <serviceid>
   ```

Message Counter Feature: Severity and Message Text Updates

HPOM for UNIX has expanded the message counter feature for duplicate messages in the Java and Motif UIs. For more information, see page 134.

Motif UI SSH-based Virtual Terminal

With HPOM for UNIX 8, a new internal application type is available in the Motif UI Application Bank. For more information about the Secure Shell application type, see "Motif UI SSH-Based Virtual Terminal" on page 123.

High Availability Environments

HPOM for UNIX 8 supports High Availability environments as listed in "High Availability Environments" on page 78.

HTTPS agents are used to run on and to manage High Availability environments.

HP Operations Manager (HPOM) and Business Availability Center (BAC) Integration

With this free-of-charge integration module you can accelerate MTTR (Mean Time to Repair) by automatically correlating IT infrastructure information with end-user transactions. It provides HPOM users visibility into the associated service levels and status.

NOTE This integration is available for HPOM for UNIX 8, and HPOM for Windows 7.5 and 8.

To enable this integration, you must install certain software components on the HPOM management server. The integration software is part of Business Availability Center (BAC), starting with BAC 6.6.

For detailed installation and configuration instructions, refer to the *HPOM Integration* document, which is part of the BAC documentation. Use the following website as an entry point to the BAC documentation:

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

Select "Business Availability Center (BAC)", and then the *Read Me* document.

HP Operations Manager (HPOM) and SiteScope Integration

This free-of-charge integration module enables consolidated agentless (by using SiteScope) and HPOM agent-based event monitoring from the central HP Operations Manager consoles.

NOTE This integration is available for HPOM for UNIX 8, and HPOM for Windows 7.5 and 8.

HP Operations Manager (HPOM) and SiteScope integration includes the following:

- ❏ Consolidated event monitoring from the central HP Operations Manager consoles, such as HPOM for UNIX Java UI
- ❏ Synchronization of the SiteScope monitor state and the HPOM service map status by using messages
- ❏ SiteScope configuration and monitor groups discovered by HPOM Agents (discovered information is published to service maps)
- ❏ Context-sensitive launch of the SiteScope dashboard from the HP Operations Manager console

The software for the HPOM-SiteScope adapter is available for download from the following location:

`http://h20229.www2.hp.com/products/ss/download_0001.html`

For more information, refer to the *SiteScope Adapter User's Guide*, available by selecting "Operations Manager for UNIX" at the following website:

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

HP Operations Manager (HPOM) and NNMi Integration

HPOM and NNMi integration is possible with the following product versions:

- HPOM for Windows version 8.10 or higher
- HPOM for UNIX version 8.30 or higher
- NNMi version 8.03 or higher

Make sure that you do not install NNMi and HPOM on the same machine. The two products must be installed on two different physical or virtual machines in either of the following configurations:

- *Different operating systems.* For example, the NNMi management server is a Linux system, and the HPOM management server is a Solaris system.
- *The same operating system.* For example, the NNMi management server is an HP-UX system, and the HPOM management server is a second HP-UX system.

For the most recent information about supported hardware platforms and operating systems, refer to the support matrices for both products.

IMPORTANT The NNMi8 integration will work only after you have installed an HPOM add-on package, which is available for download from the following site:

`ftp://ovweb.external.hp.com/pub/cpe/ito/OM-Installation/`

For more information about the HPOM and NNMi integration, refer to the *NNMi - HPOM Integration User's Guide*.

HPOM and NNMi Trap-based Integration Starting with NNMi 8.12, a new, trap-based integration between NNMi and HPOM is available. For more information, refer to the *NNMi - HPOM Integration User's Guide*.

HPOM Incidents Web Services The HPOM Incidents Web Services (requiring the HPOM 8.30 management server patch and NNMi version 8.03) are also provided with the HPOM add-on package, which can be downloaded from the following site:

`ftp://ovweb.external.hp.com/pub/cpe/ito/OM-Installation/`

For detailed information about the HPOM Incidents Web Services, refer to the *Incident Web Service Integration Guide*.

HPOM and SAM SiSAdmin Integration

The HPOM add-on package provides the HPOM and SAM SiSAdmin integration. Note that HP Operations Manager (HPOM) and SiteScope integration, which is described in “HP Operations Manager (HPOM) and SiteScope Integration” on page 25, has also become part of the updated package, which is available at the following location:

`ftp://ovweb.external.hp.com/pub/cpe/ito/OM-Installation/`

For detailed information, refer to the following user documentation:

- *SiteScope Administration Integration Read Me*
- *Operation Manager SiteScope Administration Integration Release Notes*
- *SiteScope Adapter User's Guide*
- *SiteScope Administration Integration Installation Guide*

Pluggable Authentication Module (PAM)

Pluggable Authentication Module (PAM) integration to externally authenticate the HPOM for UNIX user during login into the Motif UI and the Java UI. This is the alternative to HPOM for UNIX's internal authentication based on a username and corresponding password stored in the HPOM database.

PAM provides a configuration file where the system administrator of the HPOM for UNIX management server can specify the type of authentication mechanism to be used. It is possible to apply various authentication modules, such as UNIX /etc/passwd, Kerberos, and LDAP.

NOTE Due to missing HP-UX Operating System patches, the PAM/Kerberos module is not yet officially certified with HPOM for UNIX 8.

Deployable HP Performance Agent

With HPOM for UNIX 8, Deployable HP Performance Agent versions 4.60 and 4.70 are supported. Deployable HP Performance Agent 4.60 packages are available for HPOM for UNIX 8 as part of the HPOM for UNIX 8 media kit update as of January 2007 and support HTTPS communication. Deployable HP Performance Agent 4.70 packages are available for HPOM for UNIX 8 as part of the HPOM for UNIX 8 media kit update as of January 2008.

- Support for the following agent platforms is available.:

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

The latest release of the HP Performance Agent deployables for HPOM for UNIX 8 Management Servers integrates the ability to deploy HP Performance Agent to the following platforms:

Table 1-3 Deployable Performance Agent Support

Managed node platform	Management server platform	
	HP-UX	**Solaris**
HP-UX HPOM for UNIX 8 (HTTPS)	HP Performance Agent 4.70 HP Performance Agent 4.60	HP Performance Agent 4.70 HP Performance Agent 4.60
Solaris HPOM for UNIX 8 (HTTPS)	HP Performance Agent 4.70 HP Performance Agent 4.60	HP Performance Agent 4.70 HP Performance Agent 4.60
Linux HPOM for UNIX 8 (HTTPS)	HP Performance Agent 4.70 HP Performance Agent 4.60	HP Performance Agent 4.70 HP Performance Agent 4.60
AIX HPOM for UNIX 8 (HTTPS)	HP Performance Agent 4.70 HP Performance Agent 4.60	HP Performance Agent 4.70 HP Performance Agent 4.60
Tru64 HPOM for UNIX 8 (HTTPS)	HP Performance Agent 4.60	HP Performance Agent 4.60
Windows HPOM for UNIX 8 (HTTPS)	HP Performance Agent 4.70 HP Performance Agent 4.60	HP Performance Agent 4.70 HP Performance Agent 4.60

The latest release of HP Performance Agent deployables also provides templates, commands, and actions for HP Performance Agent group for the following managed nodes:

- HP-UX
- Solaris
- Linux
- AIX

Refer to HP Performance Agent documentation for more information.

Certificate Server Patch

The Certificate Server patch is not a regular server patch, but it is used only for upgrading the appropriate server component. By upgrading the appropriate server component, the updated Certificate Server (`ovcs`) process is installed.

Before installing the `HPOvSecCS` component from 8.30 Certificate Server patch, make sure that the following have been installed on the server node:

- 8.51 HTTPS Agents
- `HPOvSecCC` version 6.00.055

  This component is available as a hotfix. For detailed information, contact HP support.
- 8.30 server patch

Table 1-4 8.30 Certificate Server patch

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
Certificate Server Patch	PHSS_38209	PHSS_38208	ITOSOL_00676

ECS 3.31 - 3.33 Runtime Support

ECS 3.31 - 3.33 run-time files are supported on HPOM for UNIX management servers and Solaris, HP-UX, and Microsoft Windows managed nodes.

ECS 3.2 Designer Support

ECS 3.2 Designer is supported for HP-UX 11.11, and for Solaris 8 and 9. See "What's Not Supported" on page 69 for more information about platforms which are *not* supported by ECS Designer. For more information on using ECS Designer for configuring circuits for platforms that are not supported by ECS Designer, see the *Using ECS Designer Remotely Whitepaper*.

HP Composer 3.31/3.33 Support

HPOM 8 comes with a completely new integration module for HP Composer 3.31, HP's easy and free-of-charge component for event correlation. HP Composer 3.33 is offered with NNM 7.5. For more information, refer to the HPOM Administrator's Reference.

Localized Support for Japanese, Korean, Simplified Chinese and Spanish

With HPOM 8 the localized support in the following languages is supported:

- Japanese
- Korean

- Simplified Chinese
- Spanish

The extent of this support is detailed in the following tables as it is not the same for all languages.

Table 1-5 Localized Software and Online Help

Locale		English	Japanese	Korean	Simplified Chinese	Spanish
Java UI and Online Help		✔	✔	✔	✔	✔
Motif UI and Online Help		✔	✔			
Man Pages		✔				
Installation		✔	✔	✔	✔	✔
HTTPS Agent Message Catalogs	Event Action	✔	✔	✔	✔	✔
	Embedded Performance Agent	✔				
Encoding/Database Character Set		ISO-885915 WE8ISO8859P15	Shift-Jis JA16SJIS	eucKR KO16KSC5601	hp15CN ZHS16CGB231280	ISO-885915@euro WE8ISO8859P15

NOTE Updated localized Java UI online help is not available on the HPOM for UNIX 8.20 CDs, but is provided with a dedicated patch for the Java UI online help (see Table 1-6), for all supported languages stated in the Table 1-5.

Table 1-6 Java GUI Online Help Patch

	Management Server Platform		
Patch Name	**HP-UX PA-RISC**	**HP-UX Itanium**	**Solaris**
JavaGUI Online Help Patch 8.26 (Japanese only)	PHSS_37124	PHSS_37123	ITOSOL_00616
JavaGUI Online Help Patch 8.25 (English Only)[a]	PHSS_36475	PHSS_36474	ITOSOL_00590
JavaGUI Online Help Patch 8.21	PHSS_34598	PHSS_34597	ITOSOL_00506

a. JavaGUI online help patch 8.25 contains an important update that allows the advanced filtering capabilities in the message browser.

Table 1-7 HPOM for UNIX Related Manuals and Whitepapers

Locale	English	Japanese	Korean	Simplified Chinese	Spanish
HPOM Installation Guide for the Management Server	Aug 06	Feb 06			
Basic Installation Scenario with Local Database for HP Serviceguard Cluster Installation Guide	Feb 07				

Table 1-7 HPOM for UNIX Related Manuals and Whitepapers (Continued)

Locale	English	Japanese	Korean	Simplified Chinese	Spanish
HPOM Concepts Guide	July 08	Nov 08	Nov 05	Nov 05	
HPOM Administrator's Reference	May 08	Nov 08	Nov 05	Nov 05	
HPOM Java GUI Operator's Guide	May 07	Feb 06	Nov 05	Nov 05	Feb 06
HPOM HTTPS Agent Concepts and Configuration Guide	Apr 08	Nov 08	Nov 05	Nov 05	
Service Navigator Concepts and Configuration Guide	Aug 06	Feb 06	Nov 05	Nov 05	
HPOM Firewall Configuration	Aug 06				
Metrics for HP OpenView Performance Agent and HP OpenView Operations Agent	Jan 05				
Performance Agents Metrics Help Text	Jan 05	Oct 04			
HPOM Reporting and Database Schema	Dec 05				
HPOM Entity Relationship Diagrams	Oct 04				
HPOM for UNIX Release Notes	Aug 09 Edition 23	March 09[a] Edition 21			
HP Operations Agent Release Notes	Feb 09				
HPOM Application Integration Guide	Sept 04				
HPOM Developer's Reference	Aug 06				
HPOM Security Advisory Guide	Mar 06				
HTTPS Agent Clone Imaging Whitepaper	Feb 08				
Dynamic Service Engine Extensions using Perl	Sept 05				
Performance Guide 8.10 on HP-UX PA-RISC	Mar 05				
Performance Guide 8.21/8.30 on HP-UX Itanium	Mar 09				
Product Support Matrix[b]	✔				
Independent Database Server Whitepaper	Dec 08				
Service Navigator Automatic Actions Whitepaper	Sept 06				
Oracle Real Application Clusters (RAC) Support Whitepaper	Sept 06				
High Availability through HPOM for UNIX Server Pooling Whitepaper	Nov 08				
Configuring Outbound-Only Communication Whitepaper	Dec 08				
Using ECS Designer Remotely Whitepaper	Feb 07				
Deploying HPOM HTTPS Agents Using Radia Whitepaper	Jan 07				
Java GUI Message View Filtering and Detaching Windows Whitepaper	part of the Java UI OLH	Apr 07			
SiteScope Adapter for HP Operations for Windows and UNIX Whitepaper	May 07				

Table 1-7 HPOM for UNIX Related Manuals and Whitepapers (Continued)

Locale	English	Japanese	Korean	Simplified Chinese	Spanish
Certificate Management in Environments with Multiple HP BTO Software Products Whitepaper	June 07				
MessageStorm Detection Whitepaper	Aug 09				
HPOM Server Configuration Variables[c]	Aug 09				
HPOM HTTPS Agent Configuration Variables	Apr 08				
Configuration Value Pack 3.1.x Installation Guide	Mar 08				
Configuration Value Pack 3.1.x Release Notes	Feb 09				
Incident Web Service Integration Guide	July 08				
Calling OM Incident Web Services from Perl, PHP and Visual Basic Whitepaper	Mar 09				
SiteScope Administration Integration Read Me	July 08				
Operation Manager SiteScope Administration Integration Release Notes	July 08				
SiteScope Adapter User's Guide	July 08				
SiteScope Administration Integration Installation Guide	July 08				
Correlation Techniques White Paper	Aug 08				
NNMi - HPOM Integration User's Guide	Aug 08				
Additional License Restrictions for HP Operations Center Software Products	Mar 09				
Target Connector Check Utility User's Guide	Mar 09				
Configuring ServiceCenter/Service Manager for SCAuto for OMW/OMU-Configuration Guide	June 09				
HP SCAuto for Operations Manager for Unix - User Guide	June 09				

a. The latest available version of the HPOM for UNIX Release Notes may not be available in languages other than English yet. Consult also the English version of the Release Notes until the version in your preferred language is available.

b. *Product Support Matrix* is available through `http://support.openview.hp.com/selfsolve/document/KM323488`

c. This document describes server configuration variables used with HP Operations Manager for UNIX 8.xx and 9.00. This edition consolidates previous publications for both product versions.

NOTE Check the following web site periodically for the latest versions of localized manuals:

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

Miscellaneous

- **$AGENT_USER**

  Instead of hard coding a user name in a preconfigured application, you can set the `$AGENT_USER` variable. This allows you to always execute the application under the same user as the HPOM agent.

- **Other New Variables**

  The following variables allow you to use the template name, condition name and condition number in a message. These variables can be used for logfile monitoring, SNMP trap interception and the HPOM message interceptor.

  - `$CONDITION_NAME`
  - `$CONDITION_NUMBER`
  - `$TEMPLATE_NAME`

  Using these variables, for example, filled into Custom Message Attributes, will enable you to quickly identify the matched template and condition numbers for situations where you want to refine your current configuration in a subsequent step.

NOTE These variables cannot be applied to Advanced Monitoring and the monitor agent.

- **New opctemplate Output for HTTPS Nodes**

  The opctemplate listing format is changed for HTTPS nodes.

  For example, for an HTTPS node, the output of the command:

  `opctemplate -l`

  takes the following format:

```
'configsettings' 'OVO settings' enabled
'le' 'Cron (10.x/11.x HP-UX)' enabled
'le' 'OSSPI-HPUX-BadLogs' enabled
'le' 'OSSPI-HPUX-Boot' enabled
```

NOTE `opctemplate` on HTTPS agents is only a wrapper for `ovpolicy`, but `opctemplate` does NOT list the `mgrconf` file as a policy when you are running HPOM in a Flexible Management Server (MoM) environment.

- **File Permissions Remain Unchanged for HTTPS Agents**

  Files deployed to HTTPS managed nodes retain their original permission after deployment using `opcdeploy` or `ovdeploy`.

HP Operations Network Node Manager 7.53 Support

HP Operations Network Node Manager 7.53 is certified for HPOM 8 server with 8.30 server patch. For more information about NNM 7.53, refer to the documents linked below:

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

Select the "network node manager" product and version 7.53.

IMPORTANT HPOM for UNIX management server URLs are inaccessible when NNM 7.53 is installed. See "Known Problems and Workarounds" on page 149 for instructions on resolving the problem.

IMPORTANT After NNM installation is finished `nettl` fails to start. See "NNM 7.51 and NNM 7.53 CD-ROM/DVD-ROM Installation Important Update" on page 130 for instructions on resolving the problem.

NOTE It is very important that you consult the Migration Guide For Network Node Manager (NNM) 7.53 before migrating. There are some additional steps necessary if you are using Extended Topology or the dupip functionality in NNM.

Supported Migration Paths

- Update NNM and HPOM installation by using the latest version of `ovoinstall`[1].
- Install HPOM for UNIX 8 on top of a stand-alone NNM 7.53 installation.
- Migrate HPOM for UNIX 8 with NNM 7.01 installation to NNM 7.53.

IVM 3.x and 4.x Support

HP Integrity Virtual Machines 3.x and 4.x for the HP Operations management server 8.xx are supported for both standalone and cluster configurations.

NOTE The HP Operations management server patch 8.30 or higher is recommended.

Web-based Administration for HPOM for UNIX

HP no longer sells the Configuration Value Pack product. Current CVP customers under support should contact blue elephant systems (BES) directly for their entitlement to the MIDAS Configurator product. The URL for this migration is the following:

http://www.besint.com/content/view/149/182/

If you are interested in acquiring a web-based administrative tool for HP Operations Manager, there are a number of solutions provided by several HP Partners. Refer to the HP Partner portal at the following location:

http://h20229.www2.hp.com/partner/directory/partners.html?c=22-2-4

1. The latest version of `ovoinstall` is available at the following location:
`ftp://ovweb.external.hp.com/pub/cpe/ito/latest_ovoinstall`

The existing CVP customers are strongly encouraged to migrate to the MIDAS Configurator. The two products are functionally identical (CVP was an OEM of the BES MIDAS Configurator), and migrating now allows you to receive updates and support directly from BES.

IBM zOS and OS/A400 Management Solutions for HPOM

HP no longer sells the OV OS/390 and OV OS/400 products. Current customers with a valid HP support contract are eligible to receive the support entitlement directly from Eview Technology and thus are able to improve their total customer experience with those products.

The URL for this migration is the following:

`http://www.eview-tech.com/support_transition.php`

HP strongly encourages existing OV OS/390 and OV OS/400 customers to migrate to the corresponding Eview products, which provide also additional features.

Migrating also allows you to receive further updates and support directly from Eview Technology.

Dependency Mapping Automation 8

HP has launched a completely new product - HP Operations Manager Dependency Mapping Automation (HPOM DMA).

DMA enables IT operations teams to align their activities more fully with the business services that the IT infrastructure supports. By providing automated dependency mapping and configuration consistency across multiple HP Operations Manager (HPOM) servers, DMA optimizes the ability of IT organizations to support their businesses and enables enhanced productivity and efficiency within the operations teams.

DMA helps you to:

- Automate and simplify the creation and maintenance of business service views within HPOM to enable business-focused impact and root cause analysis for operational incidents.
- Streamline incident analysis activities by providing drill-down from managed nodes or services in HPOM into their change history within the HP Universal CMDB (UCMDB).
- Consolidate systems and managed services information in a single place, the UCMDB, to provide shared and consistent views across multiple HPOM servers.
- Rationalize the process of identifying new servers and applications, and the deployment of appropriate HPOM monitoring to business critical infrastructure.

For more information about DMA, refer to the `Operations Manager Dependency Mapping Automation` product at the following website:

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

or consult the HP literature in the `Business Technology Optimization Software / Operations` section at the following location:

`www.openview.hp.com`

A new version of Dependency Mapping Automation is available, DMA 8.20. For an overview of new features coming with this version, refer to the *Dependency Mapping Automation 8.20 Release Notes*, available from `http://support.openview.hp.com/selfsolve/manuals`.

Hands-on Technical Training for HPOM

The hands-on technical training for HP Operations Manager for UNIX (HPOM for UNIX) is provided by HP Education, and includes the following:

- H4356S HPOM Admin 1 (Administration)
- H4357S HPOM Admin 2 (Advanced Administration)
- UC342S Managing Events with NNM, HPOM, and ECS Composer

Topics of the technical training include:

- Creating users, applications, and policies.
- Customizing the Java GUI and Service Navigator.
- Configuring secure communication through firewalls and proxies.
- Providing flexible management and high availability, for example, server pooling.
- Reducing events using duplicate suppression, message keys, or Composer correllators.

NOTE For more information about the training schedule, visit `http://www.education.hp.com/hpsw/` and select your country in the upper right corner.

Java UI Enhancements

Below you will find a list of Java UI enhancements in HPOM for UNIX. For a complete description of Java UI functionality, read the HPOM Java GUI Operator's Guide, available from the following location:

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

- Supported Java Runtime Environments
  - Java Runtime Environment 1.6 support. JRE 1.6 is bundled with the Microsoft Windows installation package. See "Java UI" on page 188 for additional information on using JRE 1.6.
  - A newer JRE 1.6.0_16 is provided for Microsoft Windows managed platforms. See Table 2-7, "Support Matrix - Java UI," on page 82 for more information.
- Service Enhancements
  - Setting up HP Operations Manager Service Navigator automatic actions, which are triggered on a service status change, see the *Service Navigator Automatic Actions Whitepaper*.
  - Auditing for Service Navigator, see page 137
  - Setting up HP Operations Service Navigator automatic actions
  - Java GUI is now configurable to either sort services by name or by label. Sorting by 'Label' is default. It can be configured in the Preferences dialog.
  - The Service Label attribute is shown in the Message Browser, see page 188.
- Message Enhancements
  - Java GUI Message View Filtering, refer to the *Java GUI Operator's Guide*
  - Introduction of R Flag for Read-Only Messages in Java UI Message Browser, see page 128

  - Full Support for INFORM Own Mode in Java UI, see page 128
  - Acknowledging messages with bulk operations
  - Separating message fields with tabs. See "Separating Message Fields with Tabs" on page 136
  - Graphical objects can be displayed as part of the HPOM message in the Event Browser.
  - Custom Message Attributes customization of HPOM messages: add, modify and delete.
  - Alignment of column content in Java UI Message Browser
  - Customize Browser Layout by using pop-up menu in Message Browser
  - Message field sorting enhanced to support numerical data
  - Different number of messages for active and history message browser
  - Ability to cancel loading of history messages
  - Displaying URLs as hyperlinks in message browser columns and the Message Properties dialog box
  - Forwarding Manager field in Java GUI
  - Popup and menu item for creating a new history filter on the selected message
  - The History Message Browser functionality can be fully disabled for operators by setting the `OPC_JGUI_HISTBRW_DISABLED` variable on the management server. For example, by setting `ovconfchg -ovrg server -ns opc -set OPC_JGUI_HISTBRW_DISABLED opc_op1,opc_op2`, the History Message Browser functionality is disabled for `opc_op1` and `opc_op2` users.

- Configuration Enhancements
  - Java GUI Connection Port Setting, see page 129
  - The HTTPS-based Java GUI can be configured without the need for having the core agent installed on the Java GUI client. For more information about how to configure the port for the HTTPS-based Java GUI, refer to the following manuals: HPOM Java GUI Operator's Guide and HPOM Administrator's Reference, as well as to the *ito_op.1m* man page.
  - HPOM Java GUI is able to reconnect to one or more backup management servers in case of server failure. For information about configuring backup management servers by setting one or more variables, refer to the HPOM Administrator's Reference.
  - Local Java GUI Configuration Files Loaded Before Global QXCR1000310425, see page HIDDEN
  - Ability to use global Java GUI property files
  - Saving the Java UI settings while using the global Java UI settings
  - Allowed users local configuration files loaded before the global configuration
  - Custom File Name for Configuration File, see page 124
  - If an operator clicks the `OK` button (to connect through `ovbbccb`), the Java GUI keeps trying to connect to the management server. To avoid this, the fallback mechanism can now be configured by using two new `itooprc` parameters:
    - `https_fallback` (if secure communication is used)
    - `socket_fallback` (if non-secure communication is used)

    They both belong to the category of startup parameters, which are set and read only once, that is, at the startup (same as `https`, `https_only`, and so on).

    Possible values for the above parameters are the following:

— `https_fallback <to_socket | to_bbc | none>`

— `socket_fallback <to_bbc | none>`

Where `none` means that the fallback is disabled, `to_socket` means that the fallback to the socket will be triggered, and `to_bbc` means that the fallback to `ovbbccb` will be triggered.

NOTE The following two parameters affect the behavior of the fallback mechanism:

— `https_only < true | false >`

If it is set to `true`, the fallback to the socket is not possible.

— `lcore_defaults < true | false >`

If it is set to `false`, the fallback to `ovbbccb` is not possible.

- Support for Web Browsers
  - — Internet Explorer 7 Support for Java GUI Applet, see page 125
- GUI Enhancements
  - — The improved appearance of the Java GUI console window owing to the `-disableD3D` command line parameter, which is added to `ito_op.bat`.
  - — The possibility to disable the internal web browser (embedded or ActiveX) for all operators by using the `OPC_JGUI_INTERNBRW_DISABLED` server variable.
  - — To avoid a bug with some graphic cards when using Direct3D in Java GUI, the `-disableD3D` command line parameter is added to `ito_op.bat`. This command line parameter disables Direct3D for the Java Runtime Environment and significantly improves the appearance of the Java GUI console window.
  - — Java GUI Detaching Windows, see the HPOM Java GUI Operator's Guide.
  - — Customized Message Group Icons, see page 129.
  - — Changed Behavior of the Java GUI 'Lock' Feature, see page 137.
  - — Customizeable tool bar, for example, different areas for messages, message browser, services; additional tool bar options & buttons; customizeable layout.
  - — Drag and drop operations inside the Java GUI and on other applications on the system.
  - — Support of Cocoa style for Mac OS platform.
  - — New Java UI Key Accelerators.
  - — Customizing animated GIF images.
  - — HP One Voice look & feel.
  - — A new check box is added to the `Preferences` dialog to enable or disable the `Communication Status` dialog – the `Show Communication Status` dialog.

    The `Communication Status` dialog is enabled by default. In addition, a new variable in `itooprc` is introduced - `show_comm_status_dlg` (with `yes` being the default value).
- Miscellaneous
  - — Java GUI Startup Options, see page 125

— HTML Application Output as an Internal Webpage, see page 124

— opcwall utility for Java GUI

— HTTPS-based Java GUI support. For more information, refer to the HPOM Administrator's Reference manual.

— Remote APIs, for example for context-sensitive launch of applications such as the HPOM Message Browser, and service tree.

— Proxy authentication in Java UI

— Verify Java Client Console Version Using CLI, see page 124

— Logging capability is added to the `ito_op_applet_cgi.ovpl` CGI script. Logging is enabled when the file `/var/opt/OV/log/ito_op_applet_cgi.log` exists. Logging information is then written to this file.

— The Java GUI connection algorithm has been extended so that it includes the connection over the `ovbbccb` communication broker. The main advantage of `ovbbccb` is that it offers an additional connection in case the HTTPS and plain socket connections fail.

The connection order is as follows:

1. The regular HTTPS port is used for the HTTPS connection.
2. In case of a failure, the socket fallback can be done.
3. In case the socket fallback fails as well, the fallback to `ovbbccb` (HTTPS) can be done.

If an operator cancels the socket fallback or the fallback to `ovbbccb`, an error window appears. After that the login window appears, which enables the operator to connect to another management server.

A new parameter has been added, `CB_PORT`. The default value, which is `383`, can be customized, for example, in `itooprc` and `ito_op_applet.htm`.

— Java GUI filtering now supports CMAs with HPOM style pattern matching.

Service Navigator

This section describes the new announcements and features available for Service Navigator.

Service Navigator Enhancements

Service Graph Navigation enhancements include:

- Navigation panel.
- Zooming.
- Service icon positioning and dragging.
- Service line selection marking.
- Lasso selection.
- Dynamic and multi-line service labels which can be set using the `opcsvcattr(1)` command line interface.
- Multi-line service labels that can also incorporate graphics.
- Auditing for Service Navigator

Figure 1-1 Service Navigator Screenshot

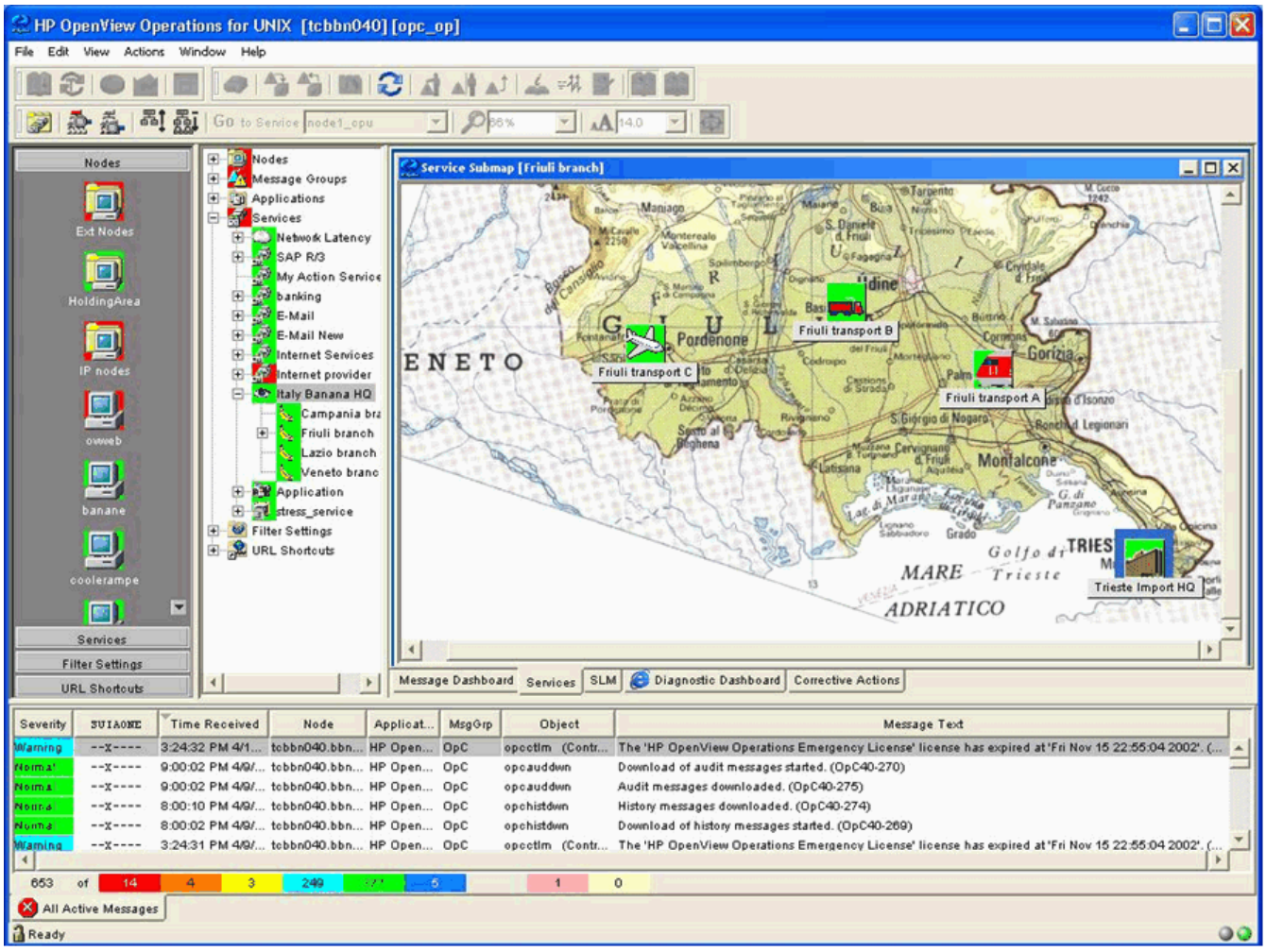
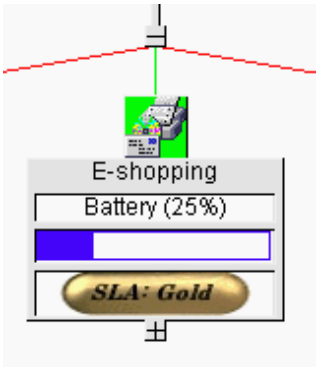


Figure 1-2 Multi-Line Service Label



Operational Service Views in the Java GUI

Service Navigator allows you to define dependencies among services. From the underlying messages in HPOM for UNIX, it establishes a service hierarchy and assigns responsibilities to operators. You can then see the current service status in the Java GUI.

Until HPOM for UNIX 8, each service in Service Navigator (SN) reflected only one status at a time. All messages in the active message browser were considered for the status calculation of services.

You can visualize more than one state per service and provide information to suit different users. For example:

- IT Managers may want to see service states which reflect the actual health of the managed environment including business services.
- Operators using Service Navigator Java GUIs may only want to see issues which are not already owned and being addressed by other operators.

With HPOM for UNIX 8, there is an additional status, `Operational`, for services calculated from a set of messages, based on a different set of rules. The calculation only considers active messages that are NOT currently owned by operators. This means that services can be simultaneously made to display two statuses, based on a different set of messages, and possibly reflecting two different severities.

You can monitor and work with services displayed in the following two status calculation views:

❏ **Overall**

The service status view based on all messages present in the active message browser.

The Overall status calculation view displays these services in the same way, irrespective of the targeting message ownership status. In this example, these services are colored red. You can observe this in the object pane, service graph or map, and in the shortcut bar. When you take the ownership of the message, the severity of the service does not change until the message is acknowledged.

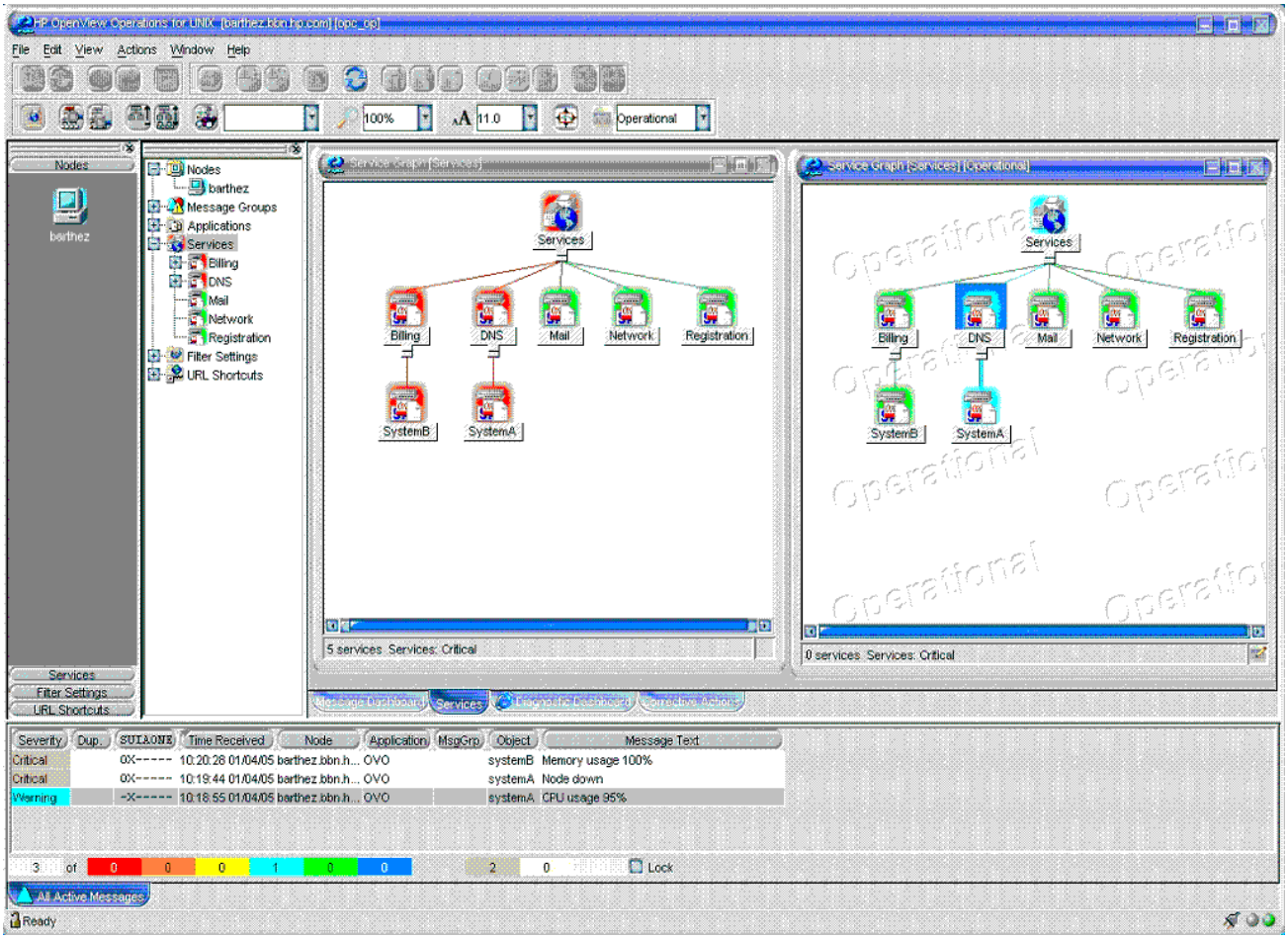
❏ **Operational**

The service status calculation view based on only non-owned messages present in the active message browser.

If your status calculation view is set to Operational and you take ownership of the message, the severities of the targeted service and all dependent services change back to the severity visible prior to the message arrival.

The benefit of the service operational view is that you can get an insight of how the service hierarchy would look if the message targeting a service is acknowledged, in other words, if the problem is solved. This is very useful, especially, if you monitor your services in both calculation views simultaneously as shown in Figure 1-3 on page 41.

Figure 1-3 Using Operational Service Views



For further information, refer to the HPOM Java GUI Operator's Guide available from the following location:

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

Allowing Dynamic Configuration Changes in Service Navigator

It is possible to program the HPOM for UNIX Service Engine to allow dynamic configuration changes, for example in Service Navigator.

For more information, refer to the *Getting Started with XML/Perl Programming for the HPOM Service Engine* whitepaper, available at the following location:

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

HPOM Target Connector License Check Utility

To help you assessing your actual HPOM Target Connector License needs, HP has developed a utility running on MS Windows. This tool evaluates the HPOM for UNIX Oracle database – by running a remote SQL query.

To conform with HP's license requirements, it is recommended to run this tool periodically. You can download the TC check utility from the following location:

`ftp://ovweb.external.hp.com/pub/cpe/ito/tcl`

The HPOM Target Connector license definition with a detailed description of use cases in which the LTU is required and which exceptions exist can be found in the *Additional License Restrictions for HP Operations Center Software Products* document. This document as well as the *Target Connector Check Utility User's Guide* can be downloaded from the following web site:

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

Select "Operations Manager for UNIX" and version 8.0.

Target Connector License Password Installation

To install the target connector license password using the `opclic` utility, choose either of the following options:

- *Option 1:*

  To install all license passwords contained in *<license_file>*, run the following command:

  `opclic -add <license_file>`

- *Option 2:*

  Enter `opclic -add` without specifying a file. The AutoPass GUI opens, which enables you to install license passwords. Perform the following steps:

  1. Click the `Browse` button and select the file containing the target connector license password or passwords.
  2. After you have selected the file containing the target connector license password or passwords, click the `View file contents` button.
  3. Browse for the passwords to be installed, and then choose them by selecting the check box of the list entry.
  4. Click the `Install` button.

Target Connector License Check

To check the installed target connector licenses, perform as follows:

1. Run the following command:

   `opclic -glist`

   This opens the AutoPass GUI showing a list of all installed license passwords. Search for the passwords with the `Annotation` containing `...Remote Management...`, and check the number of licenses in the password in the `LTU` column.

2. Summarize the LTUs for all target connector license passwords to get the number of installed target connector licenses.

NOTE `opclic -list` *does not* work for the target connector licenses.

Oracle Database

This section describes the features related to the HPOM database.

Table 1-8 presents the supported Oracle database versions for HP-UX Itanium:

Table 1-8 Supported Oracle Database Versions on HP-UX Itanium

Operating System	Oracle Database 10g Release 1 with 10.1.0.4 Patch Set	Oracle Database 10g Release 2 with 10.2.0.2 or Newer Patch Set	Oracle Database 11g Release 1 with 11.1.0.7 Patch Set
HP-UX 11.23 Itanium	✔	✔	✔
HP-UX 11.31		✔	✔

NOTE Oracle 9i became obsolete in July 2007 and is now in the Extended Support phase. Although HPOM still supports this version if a customer has signed up for Oracle Extended Support, it is strongly recommended to upgrade to supported Oracle 10g.

Oracle Database 11g Support on HP-UX 11.23 and 11.31 Itanium

HPOM for UNIX supports Oracle Database 11g (11.1.0.7 patch level or newer) with HP Operations management server 8.31 or higher. For more information, see "Oracle 11g Support-based Documentation Changes" on page 106.

Oracle Database 10g Release 1 Support on HP-UX 11.23 Itanium

HPOM for UNIX supports Oracle Database 10g Release 1 (10.1.0.4 patch level) Standard and Enterprise Edition. See the HPOM Installation Guide for the Management Server for more information on installing and using HPOM for UNIX with Oracle Database 10g. Previous versions of Oracle Database are not supported.

Oracle Database 10g Release 2 Support on HP-UX 11.23 and 11.31 Itanium

HPOM for UNIX supports Oracle Database 10g Release 2 (10.2.0.2 patch level or newer) with HPOM for UNIX Management Server 8.22 or higher. See "Upgrading to Oracle 10g Release 2" on page 131 and the HPOM Installation Guide for the Management Server for more information on installing and using HPOM for UNIX with Oracle Database 10g.

Independent Database Support

It is possible to install and configure the Oracle database used by the HPOM for UNIX management server in a cluster environment on a different node in the cluster, in a separate cluster, or on a remote system.

For more information about setting up HPOM for UNIX with an independent database server in a clustered or non-clustered environment, see also the *HPOM for UNIX Independent Database Server Whitepaper*.

There are three different installation possibilities:

- **Basic management server configuration**

  The HPOM for UNIX management server *and* the Oracle database server are installed on the *same system* or are part of the *same HA resource group* in a cluster environment.

❑ **Independent database server configuration**

HPOM for UNIX 8.31 patch introduces an Oracle 11g support. For Oracle 11g specifics, see the *HPOM for UNIX Independent Database Server Whitepaper* for HPOM for UNIX 8.31 patch, which will be released soon after the patch release.

The Oracle database server can be independently configured:

- On a remote system or on an different HA installation to the HPOM for UNIX cluster.
- On the same cluster as the HPOM for UNIX management server, but not configured as an HA resource group in HPOM for UNIX.

❑ **Decoupled (3-Tier) management server configuration**

The HPOM for UNIX management server and the Oracle database server are configured as separate HA resource groups in a single cluster environment.

Configuration Scenario	Basic		Independent		Decoupled
	Standard	**HA**	**Standard**	**HA**	**HA**
Database Installation	On HPOM for UNIX Management Server System	Part of the HPOM for UNIX Management Server HA resource group	On a dedicated remote system	On a dedicated remote system, preferably a remote cluster	As separate HA resource group on the HPOM for UNIX Management Server system

For more information about setting up the independent database, refer to the *HPOM Installation Guide for the Management Server*.

HPOM for UNIX 8 and Independent Database Server on Different Operating Systems

HP Operations can be set up with an independent Oracle Database so that the HPOM Management Server and the independent Oracle Database server systems run on different operating systems, as long as the Oracle Database version and the database server operating system are supported also by the HPOM for UNIX Management Server.

Both Oracle 9i and 10g are supported in this setup with limitations for certain operating system versions.

Since HPOM for UNIX 8 Management Server on HP-UX 11.23 and higher supports only Oracle 10g, the independent Oracle Database server version for HPOM for UNIX on HP-UX 11.23 and higher is limited to Oracle 10g. HPOM for UNIX Management Server on other supported HP-UX platforms supports both Oracle 9i and 10g in this setup.

For more information, refer to the *HPOM for UNIX Independent Database Server Whitepaper*, available from the following location:

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

Oracle Real Application Clusters (RAC) Support

HPOM for UNIX also offers support for Oracle Real Application Clusters (RAC) with Oracle 10g Release 2 (patch level 10.2.0.2 or newer) running as an independent database server.

Oracle RAC is a highly available, scalable and manageable solution for sharing access to a single database among managed nodes in a cluster environment.

For more information about using HPOM for UNIX with an independent database server on Oracle RAC, consult the *Oracle Real Application Clusters (RAC) Support Whitepaper*, available from the following location:

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

Oracle RAC server requirements are described in the Oracle RAC documentation available from the following location:

`http://www.oracle.com/technology/documentation/database10gR2.html`

HTTPS-Agents

With HPOM 8, the new HTTPS-Agent software is available for highly secure communication between HPOM for UNIX management servers and the managed nodes. HTTPS agent platforms and latest HTTPS agent patches are listed in Table 3-1, "HPOM 8 HTTPS Agent Versions from HPOM Media Kit and Latest," on page 86.

The HPOM HTTPS agents are developed on new and modern architecture, using several of the new HP Operations Common Management Environment (CME) components, including HTTPS communication, control and deployment, and the standardized logging and tracing module. For further details, refer to the new *HPOM HTTPS Agent Concepts and Configuration Guide*.

Common Agent

Manageability in heterogeneous environments with HPOM for UNIX and HPOM for Windows is achieved by introducing the common agent, which enables the same HP Operations agent to be deployed and managed seamlessly by multiple HPOM for UNIX as well as HPOM for Windows servers.

The minimum version of the HTTPS agent must be 8.53. The version of the HPOM for UNIX server must be 8.30 or higher, and the version of the HPOM for Windows server 8.10 or higher.

NOTE When purging policies in a MoM setup, all the policies on the node are purged, including the `mgrconf` policy. Because the HPOM for UNIX and the HPOM for Windows servers are in the MoM setup, you cannot switch the agent to the HPOM for UNIX server if the `mgrconf` policy is purged.

Single-Port Communication

HPOM for UNIX 8 allows a configurable, single-port, secure communication to and from the HTTPS agents. This restricts outside access to dedicated HTTP proxies and reduces port usage by multiplexing over HTTP proxies.

Outbound-Only Communication

HPOM for UNIX 8 can also be configured to use outbound-only communication with uni-directional secure communication between HPOM management servers and HPOM HTTPS agents through multiple firewalls and trust zones. With HPOM for UNIX 8.25, outbound-only communication can also be used between HPOM for UNIX management servers. For more information, refer to the *Configuring Outbound-Only Communication with HPOM for UNIX 8 Whitepaper* available from the following location:

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

Windows Installation Server

Windows installation server for HPOM HTTPS Windows agents is supported.

NOTE The agent must run as a domain administrator to allow access to the installation server functionality.

This is not as secure as running under the SYSTEM account.

Cluster Awareness for HTTPS Agents

The HPOM HTTPS agent supports the concept of virtual nodes and applications running in a high-availability environment. For more details, refer to the HPOM HTTPS Agent Concepts and Configuration Guide.

DHCP Support for HTTPS Agents

The HPOM HTTPS agent can be set up on managed nodes receiving dynamically assigned IP addresses using DHCP. For more details, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

SNMP Trap Interception for HTTPS Agents

Most currently available HTTPS agent platforms support SNMP trap interception, including Linux HTTPS agent platforms.

HTTPS Agents Running as "Non-Root"

HTTPS agents can be run under an alternative user to the privileged user.

NOTE This feature is not available for the Windows agent, which must always be run under the `SYSTEM` account, except for Installation Servers which must be run as a Domain Administrator.

NOTE The actual executing user for operator-launched applications will always be mapped to the current agent user in case the HTTPS agent runs as non-root.

Refer to the HP Operations Manager HTTPS Agent Concepts and Configuration Guide for further details.

Multiple HPOM for UNIX Configuration Servers

The HTTPS agents are able to intercept configuration data from multiple HPOM for UNIX 8 management servers. For example, a dedicated HPOM server acting as SAP competence center deploys *only* SAP-related policies and instrumentation, while another HPOM server is responsible for other tasks. For details refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

Common Criteria EAL-2 Certification

HPOM for UNIX is certified to comply with the Common Criteria EAL-2 guidelines. For an overview of the security aspects of HPOM, refer to Chapter 11, "About HPOM Security", in the HPOM Administrator's Reference and the HPOM Security Advisory Guide, available through

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

For more details about HPOM for UNIX and Common Criteria, refer to the following link:

http://www.niap-ccevs.org/cc-scheme/st/index.cfm/vid/10011

opcdelmsg Troubleshooting Utility

The opcdelmsg utility removes a single message out of the HPOM database without accessing the database directly.

The following is the opcdelmsg syntax:

```
opcdelmsg [ -help ] | [-o] [ -u <user_name> ] <msg_id> [<msg_id>...]
```

Where msg_id (message id) is used for message identification.

See opcdelmsg man page for more details on this utility.

To delete queue file entries, use the opcdelmsgs command line tool. Refer to the opcdelmsgs usage text for detailed information.

Handling IP node and non-IP node with the same node name

A new configuration parameter OPC_NEW_NAMERES has been introduced to handle IP nodes and non-IP nodes with the same name as a single node. If the parameter is set to TRUE, the following behavior is activated:

- HPOM treats the IP node and the non-IP nodes with the same name as a single node.
- Non-IP node names are also converted to lowercase if the OPC_USE_LOWERCASE parameter is set to TRUE.
- opcdbidx -lower converts non-IP nodes to lowercase.
- A new configuration parameter OPC_NEW_NAMERES_NO_LOOKUP : if set to TRUE, dblib (and opcmsgm) will not contact the name service for any node. The node name and IP address from the agent are taken as they are.

HP Operations Smart Plug-ins (SPIs) for HPOM for UNIX Update

October 2008 Release

The October 2008 release of the HP Operations Smart Plug-ins DVD contains a collection of Operations Smart Plug-ins (SPIs) and Operations supplementary management applications for use with HP Operations Manager for UNIX 8.2x and 8.30.

The SPIs contained on the DVD work with HPOM for UNIX to help you manage areas of:

- BEA WebLogic Server
- WebSphere Application Server
- IBM DB2
- Informix
- Microsoft® Exchange
- Microsoft SQL Server
- Oracle
- Oracle Application Server
- PeopleSoft
- Remedy Action Request System (ARS)

- SAP
- Sybase
- BEA Tuxedo
- Storage Essentials
- HP Systems Insight Manager Integration

November 2006 Release

The November 2006 collection of HP Operations Smart Plug-ins (SPIs) contains new and enhanced SPIs for version 8 of HP Operations Manager for UNIX. Note that the media format has changed to DVD - what has previously been available on three separate SPI CDs is now included in one DVD.

New Smart Plug-ins:

- Storage Essentials SPI
- HP Systems Insight Manager Integration

Updated Smart Plug-ins:

- Oracle Application Server SPI
- BEA Tuxedo SPI
- BEA WebLogic Server SPI
- Informix
- Oracle
- Microsoft SQL Server
- Sybase
- IBM DB2
- IBM WebSphere Application Server SPI
- Microsoft Exchange Server SPI
- PeopleSoft SPI
- Remedy SPI
- SPI for SAP

NOTE For more information, see the *Smart Plug-ins DVD for HPOM Installation Guide*, which is available from the following location:

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

Daylight Saving Time Operations Support

HP Software products support the DST change. Note that even though HP Software products may support the DST change, you still need to check that supporting software, such as Java, WebSphere, WebLogic and JBoss middleware and your systems' operating systems, supports the DST change as well.

Make sure that you have applied the necessary patches for your operating system to adjust to Daylight Saving Time changes.

For more information on other products' support for daylight saving time operations, refer to the following website:

`http://support.openview.hp.com/daylight_operations.jsp`

HP Performance Agent 4.70 Deployables

HP Performance Agent Deployables for HPOM for UNIX enable the central deployment and control of HP Performance Agent software on multiple managed systems by using HPOM for UNIX.

With HP Performance Agent 4.70, it is possible to log process command line string and manage log files based on number of days in addition to the size. It offers the ability to group applications based on zone id for better monitoring of Solaris Local Zones. Some of the new platforms supported with this release are RHEL 4, RHEL 5, SLES 10, Solaris 10, and Windows Vista.

Support for the RHEL 5.1 and RHEL 5.1 SELinux platforms is available with the HP Performance Agent 4.71 deployable patches.

HP Performance Agent 4.70 continues to support datacomm (same as HP Performance Agent 4.60), ARM, Tools (extract, utility, and so on), and the DSI interface. Refer to Release Notes and other HP Performance Agent documentation for a detailed list of the additional features and requirements of version 4.70, available in the `Performance Agent` directory at the following location:

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

Migration Aspects

The following migration paths to HPOM for UNIX 8.20 are supported:

- *From HPOM for UNIX 7.1x*
  - — on HP-UX (PA-RISC)
  - — on Solaris (SPARC)
- *From HPOM for UNIX 8.1x*
  - — on HP-UX (PA-RISC)
  - — on Solaris (SPARC)

NOTE Support for HPOM for UNIX 8.10 on HP-UX Itanium using Aries dynamic translation is discontinued.

Changed Features

This section lists existing functionality that has changed from HPOM 7.1x.

Installation of HPOM Management Server

It is much easier to install the HPOM management server. The `ovoinstall` utility guides you through the entire installation process.

NOTE Do *NOT* install HPOM using the Software Distributor UI or directly through the `swinstall` command line.

On HP-UX, the concept of a central depot server is no longer supported. However, you can use NFS-mounted file systems to install the HPOM for UNIX software, provided that your network has fast NFS response times.

Configuration Settings on the HPOM Management Server

The HPOM management server no longer uses the `opcsvinfo` configuration file.

Management server configuration is based on the new HP Operations Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`.

For example to set the limit of messages that are acknowledged directly to `1`, you use:

```
ovconfchg -ovrg server -ns opc -set OPC_DIRECT_ACKN_LIMIT 1
```

Configuration Settings on HTTPS Managed Nodes

The HTTPS agents no longer use the `opcinfo` and `nodeinfo` configuration files. The local HTTPS agent configuration is based on the new HP Operations Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`. For details, refer to the HP Operations Manager HTTPS Agent Concepts and Configuration Guide.

In case a variable is not explicitly set in a node's configuration, the command:

```
opcragt -get_config_var <name_space>:<variable_name> <node>
```

will return empty.

The node will still use default values if available.

If you want to set specific values for a selected process, use the following opcragt syntax:

```
opcragt -set_config_var eaagt.opcacta:MAX_NBR_PARALLEL_ACTIONS=100 <nodename>
```

This value is set for the action agent `opcacta` alone in namespace `eaagt.opcacta`.

HPOM Message Variables Passed into Instruction Text Parameter

The default behavior of the handling of message variables that are passed as parameters to an instruction interface has been changed.

The old behavior was that the variables were replaced by the attributes of the original message. For example, if you call:

```
opcmsg msg_t=hello
```

<$MSG_MSG> is replaced by the value that has been specified in the set area of the condition, for example, "This is a hello message."

The new behavior can be changed back to the old behavior by setting OPC_SET_MSGVARS_FROM_ORIGMSG to TRUE.

Examples

Change to the old behavior for all agent processes:

```
ovconfchg -ns eaagt -set OPC_SET_MSGVARS_FROM_ORIGMSG TRUE
```

Change to the old behavior for the opcmsgi process only:

```
ovconfchg -ns eaagt.opcmsgi -set OPC_SET_MSGVARS_FROM_ORIGMSG TRUE
```

Remote Actions Authorization

HPOM 8 has improved remote action execution authorization. By default, remote automatic actions from HTTPS nodes are allowed.

For details see the *Remote Action Authorization* section in the HPOM HTTPS Agent Concepts and Configuration Guide.

HTTPS Managed Nodes Policies

Policies are no longer encrypted, but signed. As superuser, you can read them directly. All templates of the same type are stored in one directory instead of one file.

There is a file for the policy header in XML (<UUID>_header.xml) and the policy body (<UUID>_data). The header basically contains information that is also in the body. To view the template as it would have been in HPOM 7, just view the UUID_data file. The policies are stored under following directories:

nodeinfo Templates	$OvDataDir/datafiles/policies/configsettings/
Logfile Templates	$OvDataDir/datafiles/policies/le/
MoM Templates	$OvDataDir/datafiles/policies/mgrconf/
Monitor Templates	$OvDataDir/datafiles/policies/monitor/
opcmsg Templates	$OvDataDir/datafiles/policies/msgi/
SNMP trap Templates	$OvDataDir/datafiles/policies/trapi/

No Remote Access to the Service Engine

By default, remote access to the service engine is disabled.

To allow the remote access to the service engine, make the following configuration changes:

1. Enter the following line in the /etc/services file:

   ```
   opcsvcterm  7278/tcp    # Service engine remote access
   ```

2. Enter the following line in the /etc/inetd.conf file:

   ```
   opcsvcterm  stream tcp nowait root /opt/OV/bin/OpC/opcsvcterm  opcsvcterm
   ```

3. Restart the `inetd` process:

```
inetd -c
```

Locally Managed Tablespaces

HPOM creates the database using Oracle locally managed tablespaces instead of dictionary managed tablespaces.

Error Logging

HPOM 8 uses the common HP Operations logging. The errors are no longer logged to the `opcerror` file, but to the following log files:

Binary `$OvDataDir/log/System.bin`

ASCII `$OvDataDir/log/System.txt`

The HTTPS agent and management server use the same location.

Tracing

HPOM 8 uses the common HP Operations tracing. For further information about common HP Operations tracing, refer to the *Tracing Concepts and User's Guide*. For HPOM-related tracing details, refer to the latest *HPOM HTTPS Agent Concepts and Configuration Guide*, which can be downloaded from the following website:

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

HPOM-SunMC Integration Kit

The HPOM/SunMC Integration Kit for HPOM for UNIX on HP-UX Itanium is available through a hotfix, which can be obtained from HP support.

Default Templates for AIX, HP-UX, Linux, Sun Solaris, Tru64, and Microsoft Windows

The default templates for AIX, HP-UX, Linux, Sun Solaris, Tru64, and Windows are no longer shipped with HPOM 8. This functionality is replaced by the Smart Plug-ins for Operating Systems, which are regularly updated and shipped on the frequently-released HP Operations Manager SPI DVD.

NOTE The OS-SPI includes a dedicated Release Notes document. Read this document before installing.

NOTE In cases where the OS-SPI has already provided similar functionality or a superset of the HPOM functionality, the existing OS-SPI version is used. In these cases, the actual template conditions, and command line parameters may not be 100% identical.

Table 1-9 maps the new OS-SPI instrumentation names to the names previously used by HPOM for UNIX 7.

Table 1-10 maps the new OS-SPI policy names to the template names previously used by HPOM for UNIX 7.

Table 1-11 maps the new OS-SPI application names to the names previously used by HPOM for UNIX 7.

Make sure that you change the names of your existing instrumentation and any copies of the original files on your system to match the names used by the OS-SPI as shown in Table 1-9, Table 1-10, and Table 1-11.

Table 1-9 OS-SPI Instrumentation Mapping

Platform	Type	Instrumentation Name used in HPOM for UNIX 7	OS-SPI Instrumentation Name
AIX	**Actions**	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opcps	osspi_ps.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		errpt_fmt.sh	osspi_errptfmt.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh
HP-UX	**Actions**	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df
		opclpst	osspi_lpst
		opcps	osspi_ps
	Performance Agent Commands	anycmd.sh	osspi_anycmd.sh
		perfcmd.sh	osspi_perfcmd.sh
		cfgfile.sh	osspi_cfgfile.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		opcnprcs	osspi_nprcs
		proc_mon.sh	osspi_pcntmon.sh
Linux	**Actions**	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opcps	osspi_ps.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh

Table 1-9 OS-SPI Instrumentation Mapping (Continued)

Platform	Type	Instrumentation Name used in HPOM for UNIX 7	OS-SPI Instrumentation Name
Solaris SPARC	**Actions**	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opcps	osspi_ps.sh
	Performance Agent Commands	anycmd.sh	osspi_anycmd.sh
		perfcmd.sh	osspi_perfcmd.sh
		cfgfile.sh	osspi_cfgfile.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh
		vcs_monitor.sh	osspi_vcsmon.sh
Tru64 UNIX	**Actions**	mailq_pr.sh	osspi_mailqpr.sh
		ana_disk.sh	osspi_anadisk.sh
		sh_procs.sh	osspi_shprocs.sh
	Commands	opcdf	osspi_df.sh
		opclpst	osspi_lpst.sh
		opcps	osspi_ps.sh
	Monitors	cpu_mon.sh	osspi_cpuutil.sh
		disk_mon.sh	osspi_diskutil.sh
		opcfwtmp	osspi_fwtmp
		proc_mon.sh	osspi_pcntmon.sh
Windows	**Actions**	None	
	Commands	itodiag.exe	winosspi_windiag.exe
		itoprocs.exe	winosspi_procs.exe
		itouser.exe	winosspi_winuser.exe
		itokill.exe	winosspi_prockill.exe
		itosdown.exe	winosspi_shutdown.exe
		itoreg.exe	winosspi_winreg.exe
		opcprfls.exe	winosspi_perfobj.exe
		itoreg.cfg	winosspi_winreg.cfg
		itomserv.exe	winosspi_confserv.exe
		mf_app.bat	winosspi_mf_app.bat
	Monitors	None	

Table 1-10 OS-SPI Template/Policy Mapping

Template Name	OS-SPI Policy Name
NOTE: To find the template groups which have a dedicated policy assigned, use the HPOM report `Template Summary` and search for the policy name in the report output. Most policies are assigned to more than one template group. This HPOM report can be found in the HPOM Administrator's GUI selecting: `Actions` -> `Utilities` -> `Reports...`	
AIX	
opcmsg(1|3)	OSSPI-opcmsg
Audit Log (AIX)	OSSPI-AIX-AuditLog
Bad Logs (AIX)	OSSPI-AIX-BadLogs
Kernel Logs (AIX)	OSSPI-AIX-KernelLogs
Logins (AIX)	OSSPI-AIX-Logins
Su (AIX)	OSSPI-AIX-Su
Syslog (AIX)	OSSPI-AIX-syslog
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
AIX with HACMP	
opcmsg(1|3)	OSSPI-opcmsg
Audit Log (AIX)	OSSPI-AIX-AuditLog
Bad Logs (AIX)	OSSPI-AIX-BadLogs
HACMP logfile (AIX)	OSSPI-HACMP_Log
Kernel Logs (AIX)	OSSPI-AIX-KernelLogs
Logins (AIX)	OSSPI-AIX-Logins
Su (AIX)	OSSPI-AIX-Su
Syslog (AIX)	OSSPI-AIX-syslog
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
Debian Linux	
opcmsg(1|3)	OSSPI-opcmsg
Auth (Debian Linux)	OSSPI-Linux-authlog
Kernel (Debian Linux)	OSSPI-linux-debian_kernellog
Logins (Linux)	OSSPI-Linux-Logins
Syslog (Debian Linux)	OSSPI-Linux-syslog
Inetd	OSSPI-Linux_inetdproc
MailQueueLength	OSSPI-mailqueue

Table 1-10 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
Debian Linux continued	
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
swap_util	OSSPI-swapmon
HP-UX	
opcmsg(1|3)	OSSPI-opcmsg
Bad Logs (10.x/11.x HP-UX)	OSSPI-HPUX-BadLogs
Boot (10.x/11.x HP-UX)	OSSPI-HPUX-Boot
Cron (10.x/11.x HP-UX)	OSSPI-HPUX-Cron
Kernel Logs (10.x/11.x HP-UX)	OSSPI-HPUX-Dmesg
Logins (10.x/11.x HP-UX)	OSSPI-HPUX-Logins
Mailqueue (10.x/11.x HP-UX)	OSSPI-mailqueue
Su (10.x/11.x HP-UX)	OSSPI-HPUX-Su
Syslog (10.x/11.x HP-UX)	OSSPI-HPUX-syslog
Syslog (ServiceGuard)	OSSPI-MCSG-Syslog
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
Management Server	
opcmsg(1|3)	OSSPI-opcmsg
Cron (10.x/11.x HP-UX)	OSSPI-HPUX-Cron
Su (10.x/11.x HP-UX)	OSSPI-HPUX-Su
disk_util	OSSPI-diskutil
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
SNMP Traps (NNM 7.01) SNMP ECS Traps	Replaced by corresponding versions for NNM 7.01. Provided by HPOM Platform.
Su (Solaris)	OSSPI-SOL-Su
Syslog (Solaris)	OSSPI-SOL-syslog
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
swap_util	OSSPI-swapmon

Table 1-10 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
MC/SG Physical Management Server	
opcmsg(1|3)	OSSPI-opcmsg
Cron (10.x/11.x HP-UX)	OSSPI-HPUX-Cron
Su (10.x/11.x HP-UX)	OSSPI-HPUX-Su
disk_util	OSSPI-diskutil
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
MetaFrame	
System Log (MetaFrame)	WINOSSPI-MF_FwdAllSysWarnError
MF_ICA_Browser	WINOSSPI-MF_ICA_Browser
MF_Prog_Neighborhood	WINOSSPI-MF_Prog_Neighbourhood
TS_Licensing	WINOSSPI-WTS_TermServLicensing
TS_Service	WINOSSPI-WTS_TermService
SC/HA Physical Management Server	
opcmsg(1|3)	OSSPI-opcmsg
Bad Logs (Solaris)	OSSPI-SOL-BadLogs
Cron (Solaris)	OSSPI-SOL-Cron
Logins (Solaris)	OSSPI-SOL-Logins
Su (Solaris)	OSSPI-SOL-Su
Syslog (Solaris)	OSSPI-SOL-syslog
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
Solaris SPARC	
opcmsg(1|3)	OSSPI-opcmsg
Bad Logs (Solaris)	OSSPI-SOL-BadLogs
Cron (Solaris)	OSSPI-SOL-Cron
Engine Log (SC)	OSSPI-SC-EngineLog
Engine Log (VCS)	OSSPI-VCS-EngineLog
Engine Notify Log (VCS)	OSSPI-VCS-EngineNotifyLog
Logins (Solaris)	OSSPI-SOL-Logins
Su (Solaris)	OSSPI-SOL-Su
Syslog (Solaris)	OSSPI-SOL-syslog
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil

Table 1-10 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
Solaris continued	
disk_util	OSSPI-diskutil
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
SuSE Linux	
opcmsg(1|3)	OSSPI-opcmsg
Kernel Messages (SuSE)	OSSPI-linux-suse_kernellog
Logins (Linux)	OSSPI-Linux-Logins
Messages (SuSE)	OSSPI-linux-suse_messages
Inetd	OSSPI-Linux_inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
swap_util	OSSPI-swapmon
Terminal Server	
System Log (Terminal Server)	WINOSSPI-WTS_FwdAllSysWarnError
TS_Licensing	WINOSSPI-WTS_TermServLicensing
TS_Service	WINOSSPI-WTS_TermService
Tru64 UNIX	
opcmsg(1|3)	OSSPI-opcmsg
Cron (Digital Unix)	OSSPI-cronproc
Logs (Digital Unix)	OSSPI-Tru64-Logins
Lplog (Digital Unix)	OSSPI-Tru64-printlog
OS Msgs (Digital Unix)	OSSPI-Tru64_messages
SIA Log (Digital Unix)	OSSPI-Tru64-BadLogs and OSSPI-Tru64-Su
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
swap_util	OSSPI-procutil
VCS Physical Management Server	
opcmsg(1|3)	OSSPI-opcmsg
Application (VCS)	OSSPI-VCS-ApplicationServiceLog
Bad Logs (Solaris)	OSSPI-SOL-BadLogs
Cron (Solaris)	OSSPI-SOL-Cron
Disk (VCS)	OSSPI-VCS-DiskServiceLog
DiskGroup (VCS)	OSSPI-VCS-DiskGroupLog
DiskReservation (VCS)	OSSPI-VCS-DiskReservationLog
ElifNone (VCS)	OSSPI-VCS-ElifNoneServiceLog

Table 1-10 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
VCS Physical Management Server continued	
Engine	OSSPI-VCS-EngineLog
Engine Shadow	OSSPI-VCS-EngineShadowLog
Engine Shadow Error	OSSPI-VCS-EngineShadowErrorLog
FileNone (VCS)	OSSPI-VCS-FileNoneServiceLog
FileOnOff (VCS)	OSSPI-VCS-FileOnOffServiceLog
FileOnOnly (VCS)	OSSPI-VCS-FileOnOnlyServiceLog
IP (VCS)	OSSPI-VCS-IPServiceLog
IPMultiNIC (VCS)	OSSPI-VCS-IPMultiNICServiceLog
Logins (Solaris)	OSSPI-SOL-Logins
Mount (VCS)	OSSPI-VCS-MountServiceLog
MultiNICA (VCS)	OSSPI-VCS-MultiNICAServiceLog
NFS (VCS)	OSSPI-VCS-NFSServiceLog
NIC (VCS)	OSSPI-VCS-NICServiceLog
Phantom (VCS)	OSSPI-VCS-PhantomServiceLog
Process (VCS)	OSSPI-VCS-ProcessServiceLog
Proxy (VCS)	OSSPI-VCS-ProxyServiceLog
ServiceGroupHB (VCS)	OSSPI-VCS-ServiceGroupHBServiceLog
Share (VCS)	OSSPI-VCS-ShareServiceLog
Su (Solaris)	OSSPI-SOL-Su
Syslog (Solaris)	OSSPI-SOL-syslog
Volume (VCS)	OSSPI-VCS-VolumeServiceLog
Inetd	OSSPI-inetdproc
MailQueueLength	OSSPI-mailqueue
Sendmail	OSSPI-mailproc
Syslogd	OSSPI-syslogproc
cpu_util	OSSPI-cpuutil
disk_util	OSSPI-diskutil
had	OSSPI-VCS-had
hashadow	OSSPI-VCS-Hashadow
proc_util	OSSPI-procutil
swap_util	OSSPI-swapmon
vmsa_server	OSSPI-vmsa-server
vxconfigd	OSSPI-vxconfigd
Windows 2000/2003	
opcmsg(1|3)	WINOSSPI-opcmsg
dflt_ApplEvLog (NT)	WINOSSPI-Logon_ApplInfo
	WINOSSPI-NetworkConfig_ApplInfo
	WINOSSPI-ADS_Replication_ApplInfo
dflt_DNSEvLog (2000)	WINOSSPI-ADS_DNSServ_FwdAllWarnError
dflt_DirectoryEvLog (2000)	WINOSSPI-ADS_FwdAllWarnErrorDS
	WINOSSPI-ADS_ReplcationActivites
dflt_FileReplicationEvLog (2000)	WINOSSPI-ADS_FwdAllWarnErrorFRS

Table 1-10 OS-SPI Template/Policy Mapping (Continued)

Template Name	OS-SPI Policy Name
dflt_SecEvLog (NT)	WINOSSPI-Logon_SecInfo
	WINOSSPI-Process_SecInfo
	WINOSSPI-SecEvLog_Operations
	WINOSSPI-ADS_PrivilegedObjects
dflt_SysEvLog (NT)	WINOSSPI-SCM_Sysinfo
	WINOSSPI-NetLogon_SysInfo
dflt_cpu_util_NT	WINOSSPI-SysMon_CpuSpikeCheck_Win2k_PrivilegedTime
	WINOSSPI-SysMon_CpuSpikeCheck_Win2k _ProcessorTime
	WINOSSPI-SysMon_CpuSpikeCheck_Win2k _UserTime
Windows NT[a]	
opcmsg(1|3)	WINOSSPI-opcmsg
dflt_ApplEvLog (NT)	WINOSSPI-Logon_ApplInfo WINOSSPI-NetworkConfig_ApplInfo WINOSSPI-ADS_Replication_ApplInfo
dflt_SecEvLog (NT)	WINOSSPI-Logon_SecInfo WINOSSPI-Process_SecInfo WINOSSPI-SecEvLog_Operations WINOSSPI-ADS_PrivilegedObjects
dflt_SysEvLog (NT)	WINOSSPI-SCM_Sysinfo WINOSSPI-NetLogon_SysInfo
dflt_cpu_util_NT	WINOSSPI-SysMon_CpuSpikeCheck_NT4_PrivilegedTime WINOSSPI-SysMon_CpuSpikeCheck_NT4 _ProcessorTime WINOSSPI-SysMon_CpuSpikeCheck_NT4 _UserTime
dflt_disk_util_NT	WINOSSPI-SysMon_DiskBusyCheck_AvgDiskQueue WINOSSPI-SysMon_DiskBusyCheck_DiskTIme WINOSSPI-SysMon_DiskFullCheck_FreeMB WINOSSPI-SysMon_DiskFullCheck_PercentageFreeSpace

a. Microsoft Windows NT operating system is no longer supported by Microsoft. The Windows OS-SPI currently delivers these policies with no further commitment to continue development.

Table 1-11 OS-SPI Application Mapping

HPOM for UNIX 7 Application Name	OS-SPI Application Group	OS-SPI Application Name
GlancePlus		
Start gpm	Unix OS SPI\HP Performance Products\HP Glance	GPM (Motif)
Start glance		Glance (Ascii)
List Processes	Unix OS SPI\HP Performance Products\ Common Applications	List processes
List Versions		List Versions
Tail Status Files		Tail Status Files
Config ttd.conf		Configure ttd.conf
MetaFrame Tools		
Sessions	Windows OS SPI\MetaFrame Tools	Sessions
Users		Users
Servers		Servers
Auditlog		Audit Log
ACL Info		ACL Info
Disconnect		Disconnect
Flush		Flush
Send Message		Send Message
Processes		Processes
License		License
NT Tools		
Cancel Reboot	Windows OS SPI\Microsoft Windows Core\System	Cancel Shutdown
CPU Load		CPU Load
LM Sessions		List Sessions
Process Kill		Kill Process
Reboot		Shutdown
Reg Viewer		Show Registry Key
Show Services		List Services
Start Service		Start Service
Stop Service		Stop Service
Diagnostics	Windows OS SPI\Microsoft Windows Core\ Information	Get System Overview
Installed Software		Installed Software
Job Status		Job Status
Local User		Local User
Memory Load		Memory Information
PerfMon Objs		Perfmon Objects
Shares		Shares
Server Config		Server Config
Server Stats		Server Stats
Show Drivers		Show Drivers
Show Users		User List
Used Shares		Used Shares
Workst Stats		Workst Stats

Table 1-11 OS-SPI Application Mapping (Continued)

HPOM for UNIX 7 Application Name	OS-SPI Application Group	OS-SPI Application Name
NetBios Sessions	Windows OS SPI\Microsoft Windows Core\ Networking	NetBios Sessions
TCP/IP Status		Show TCP/IP Connections
HP Performance Agent		
Start Perf Agt	Unix OS SPI\HP Performance Products\HP Performance Agent	Start HP Performance Agent
Stop Perf Agt		Stop HP Performance Agent
Restart Perf Agt		Restart Perf Agt
Restart PA Servers		Restart PA Servers
Reactivate alarmdef		Reactivate alarmdef
Config parm		Configure parm
Check parm		Check parm
Config perflbd.rc		Configure perflbd.rc
Config alarmdef		Configure alarmdef
Check alarmdef		Check alarmdef
Start extract		Start extract
Start utility		Start utility
Config ttd.conf	Unix OS SPI\HP Performance Products\ Common Applications	Configure ttd.conf
List Versions		List Versions
Tail Status Files		Tail Status Files
List Processes		List Processes
Start pv	Unix OS SPI\HP Performance Products\HP Performance	HP Performance Console
Start pvalarmd		Start pvalarmd
Stop pvalarmd		Stop pvalarmd
Tools		
Disk Space	"OS Tools" for every platform's Admin and Operator groups	Disk Space
Processes	"OS Tools" for every platform's Admin and Operator groups	Processes
UN*X Tools		
SMIT (AIX)	Unix OS SPI\AIX\AIX Admin Tools\OS Tools	SMIT (AIX)
ASCII SAM	Unix OS SPI\HPUX\HPUX Admin Tools\OS Tools	ASCII SAM
Motif SAM		Motif SAM
Print Status	"OS Tools" for every platform's Admin and Operator groups	Print Status
VERITAS		
VERITAS CSCM	Unix OS SPI\Veritas\Veritas Admin Tools	VERITAS CSCM
VERITAS VMSA		VERITAS VMSA

The following Application Groups have been replaced and are obsolete:

- GlancePlus
- Jovw
- MetaFrame Tools
- OV Performance
- Reports
- VERITAS

In addition to the applications in the obsolete application groups, the following applications are no longer provided:

```
Application                              Label
-----------------------------------------------------------
/Net Activity/Interface Statistics  : Interface Statistics
/OV Services/OV CDP View            : CDP View
```

The following applications are renamed and enhanced:

```
Application                              New Label
-----------------------------------------------------------
/Net Config/Addresses               : Addresses(Node)
                                      Addresses(Interface)
/Net Config/Routing Table           : Routing Table(Node)
                                      Routing Table(Interface)
/Net Config/ARP Cache               : ARP Cache(Node)
                                      ARP Cache(Interface)
```

Changed Features with HP Operations Manager for UNIX Developer's Toolkit

This section lists existing functionality that has changed from the HP Operations Manager for UNIX Developer's Toolkit version 7.1x.

Server API opcapp_start() Function Behavior Changed with HPOM 8

The function `opcapp_start()` is obsolete since VPO 6.0 and is only included for compatibility reasons. It is strongly recommended that you use the function `opcappl_start()` instead. Note the added 'l' in the function name.

The behavior of the function `opcapp_start()` has been changed and is forced to check the execution user name and password on the target node before the execution of the application. This is because execution user name could have been changed and is different from the execution user name of the application stored in the database. This was not the case with HPOM for UNIX 7 and earlier versions and has been changed to improve security.

This change also introduces a new configuration parameter:

`OPC_OMIT_PWD_CHECK_FOR_APP_START`

Setting this parameter to `TRUE` will switch the behavior back to the pre- HPOM for UNIX 8 and less secure model. This is NOT recommended, but implemented so that it is still possible to work with applications that require it.

To set the `OPC_OMIT_PWD_CHECK_FOR_APP_START` parameter only for the one application that needs it, enter the following command:

`ovconfchg -ovrg server -ns opc.<appl_name> -set OPC_OMIT_PWD_CHECK_FOR_APP_START TRUE`

Alternatively, use the function `opcappl_start()`, particularly for newer integrations.

In general it is NOT necessary to set the user name and password as long as it is not required to execute the application as different user. The execution user that is specified in the database will be used to execute applications on the target node, as long as the execution user in the `OPCDTYPE_APPL_CONFIG` structure is not changed. If it is changed, then the user will be checked and it is also necessary to specify the password.

Obsolete Features

This section lists the obsolete features of this release of HPOM:

- **Obsolete Management Server Platforms**
  - HP-UX 11.0
  - HP-UX 10.20
  - Sun Solaris 7
- **Obsolete HPOM Agent Platforms**
  - HP-UX 11.0
  - HP-UX 10.20
  - Linux Kernel 2.2 and 2.4 all derivatives
  - Novell NetWare 4.x
  - Tru64 UNIX 4.0x (excluding 4.0 F/G)
  - Microsoft Windows NT 4.0
  - HP MPE/iX
  - Microsoft Windows 2003 without SP
  - Microsoft Windows 2000 (all editions; unless there is an extended Microsoft support contract)
  - Microsoft Windows XP (SP1 and prior)
  - RedHat Enterprise Linux 2.1, 3.x
  - HP-UX 11.22 (Itanium)
  - Tru64 UNIX 4.x, 5.0A, 5.1, 5.1A
  - OpenVMS 7.3.1
- **Obsolete Java UI Platforms**
  - HP-UX 11.0
  - HP-UX 10.20
  - Sun Solaris 7
  - Microsoft Windows NT and 98
  - Microsoft Windows 2000
  - Microsoft Windows 2003 without SP
  - Microsoft Windows XP (SP1 and prior)
  - Linux Kernel 2.2 all derivatives

- **opcinfo and nodeinfo Configuration Files**

  The HPOM HTTPS agents no longer use the `opcinfo` and `nodeinfo` configuration files. The local HTTPS agent configuration is based on the new HP Operations Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`. For details, refer to the HP Operations Manager HTTPS Agent Concepts and Configuration Guide.

- **opcsvinfo Configuration File**

  The HPOM management server no longer uses the `opcsvinfo` configuration file. The management server configuration is based on the new HP Operations Common Management Environment (CME) components using `ovconfget(1)` and `ovconfchg(1)`.

- **opcerror**

  HPOM uses the common HP Operations Manager logging. The errors are no longer logged to the `opcerror` file, but to the `$OvDataDir/log/System.bin` (binary) and `$OvDataDir/log/System.txt` (ASCII) log files. The HTTPS agent and management server use the same location.

- **HP Advanced Security**

  The HP Advanced Security (HPAS) is not offered for this version of HPOM. HPOM for UNIX 8 itself provides most of the HPAS functionality, since HTTPS communication can be used for the HPOM agents and for the HPOM Java UI - HPOM for UNIX management server communication.

  Before migrating from HPOM for UNIX 7.1x, you must switch off the HPAS functionality completely for the Java UI.

- **opcdbreorg**

  The Oracle database maintenance program `opcdbreorg` is no longer necessary, since the `Database Extend Management` is switched to `local`.

- **Virtual Terminal Application to Connect to HTTPS Agent for Windows**

  There is no standard application delivered with HPOM for UNIX to provide a virtual terminal connection to the HTTPS Windows managed nodes.

  There are several 3rd party applications available designed specifically to achieve such connections.

What's Not Yet Supported

- **UTF8 Character Set**

  HPOM for UNIX 8 does not support UTF8 as the character set used for the Oracle database and the HPOM management server. The supported encoding and character sets are detailed in Table 2-5, "Certified Encoding and Character Sets," on page 81.

  However, UTF8 character set is supported for the HPOM Agent platforms. The supported encoding and character sets are detailed in Table 5-1, "OM Agent Platform Character Sets and Locales," on page 203.

- **User Provided Certificate Authority**

  HPOM for UNIX does not support the use of any external or custom Certificate Authority.

- **Hostnames Maximum Character Length is 256**

  HPOM for UNIX does not yet support hostnames longer than 256 characters.

What's Not Supported

- **HTTP Proxy Limitations**

  In case the HPOM for UNIX management server does not talk directly to an HTTPS agent, but by using an HTTP proxy, be aware of the following limitations:

  — **HTTP Proxy with USER/PASSWD Authorization**

  One of the following alternatives can be used:

  - HTTP Proxy must accept non-authorized requests from specific IP address or domain ranges with specified destination ports.
  - An additional HTTP Proxy must be used, which accepts non authorized requests from the HPOM Application but then contacts the main HTTP Proxy with USER/PASSWD.

  — **Fail-Over, Fallback, and Alternative HTTP Proxies**

  HPOM supports only one HTTP proxy per HTTPS agent, but different HTTP proxies can be specified for different HTTPS agents.

- **HTTPS to DCE Agent Conversion**

  HPOM 8 HTTPS agents cannot be directly downgraded to DCE agents. You must completely deinstall the HTTPS agent and install the DCE agent.

  Upgrading DCE agents to HTTPS agents, however, offers the following advantages:

  — The installation procedure automatically deinstalls the DCE agent.

  — `opcinfo` settings are rescued and converted automatically.

  — The Embedded Performance database settings are rescued and converted automatically.

  — ECS data and fact stores are rescued automatically.

- **ECS Designer**

  ECS Designer is not supported running on HP-UX 11.23 and 11.31 Itanium, HP-UX 11.23 and 11.31 PA-RISC, and on Solaris 10. If you would like to use ECS Designer in conjunction with HPOM for UNIX, you will have to create ECS circuits and data/fact stores on a operating system platform supported by ECS Designer, for example HP-UX 11.11, Solaris 8 or Solaris 9.

  After creating the circuits, data and fact stores on another system, transfer them to the HPOM for UNIX management server. Detailed instructions are available in the *Using ECS Designer Remotely* whitepaper that can be downloaded from the following location:

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

- **Service Navigator Value Pack (SNVP)**

  Due to changes in product strategy HP discontinued any further development and Operating System / Oracle database / JRE certification activities for the Service Navigator Value Packs (SNVP) versions 8 and 9. SNVP 8 and SNVP 9 are no longer supported as of June 30, 2009.

- **DCE- and NCS-based HPOM 7 Agents**

  DCE- and NCS-based HPOM 7 agents are obsolete since 2008. This also includes the HPOM 7 agents shipped with the HPOM for UNIX 8 media kit.

Obsolescence Announcements for the Next HPOM for UNIX Release

The following features may no longer be supported with the next release of HPOM for UNIX.
The next release of HPOM for UNIX is planned for the second half of 2009.

NOTE HP appreciates your feedback. Contact your HP sales or support representative if you would like HP to continue supporting the features listed in this section with the next release.

❑ **Management Server Platform**

HP plans to obsolete the following management server versions:

- HP-UX PA-RISC all versions
- HP-UX Itanium 11.23 (only HP-UX Itanium 11.31 will be supported)
- Sun Solaris 8 and 9 (only Solaris 10 will be supported)

❑ **Management Server Processes**

The following HPOM processes will become obsolete:

- `ovoareqhdlr`
- `opccmm`
- `opcctlm`
- `opcdistm`
- `opcmgrdist`
- `opcmsgrd`

libnspsv Library

The `libnspsv` library will be deprecated. However, it will be still present on the HP Operations management server for the backward compatibility. The integrations, applications or scripts linked to this library in the previous product versions will be also available for use.

Changing Control over HPOM Processes

The HPOM Control Manager (`opcctlm`) will become obsolete. The control over HPOM processes will be moved to the `OV Control` facility (the `ovcd` process). Some of Control Manager's functionality will be moved to the HPOM Request Sender (`ovoareqsdr`). The HPOM processes will be possible to control by the `ovc` and `opcsv` CLI, but no longer by `ovstart`, `ovstop` and `ovstatus` CLIs, because Network Node Manager will no longer be running on the same HPOM management server system.

❑ **NNM Local Integration**

NNM will be not possible to install on the same system as HPOM for UNIX, thus the local integration with NNM will become obsolete. However, an integration package will be provided with HPOM 9.0x to work remotely with NNM 7.xx and NNMi 8.xx.

❑ CLIs and CLI options

All CLIs provided by NNM will be no longer available on the HPOM for UNIX management server, such as `ovstart`, `ovstop`, `ovstatus`, `ovw`, and `ovaddobj`. Other CLIs that will become obsolete:

- `opc_backup`
- `opc_recover`
- `opcmgrdist`[a]
- `opctmplrpt`
- `opcauddwn`
- `opccfgupld`: the `-ascii` option
- `opccfgupld`: the `-deloldtempls` option
- `opcmomchk`: the `-escalation` option
- `opcpwd`
- `opclic`
- `opcsvreg`
- `opcsvskm`
- `opctranm`
- `ovbackup.ovpl`
- `ovrestore.ovpl`

a. Configuration synchronization of HPOM for UNIX servers can be accomplished by running standard CLIs, as described in "Synchronization of Configuration Data from One HPOM for UNIX Server to Another" on page 123.

❑ Configuration Variables

HP plans to obsolete the following configuration variables with the next release of HPOM for UNIX:

- `DCEMR_PROG`
- `DISTM_PROG`
- `OPC_CFG_KEY_TAB`
- `OPC_CFG_SEC_LEVEL`
- `OPC_COMM_PORT_DISTM`
- `OPC_DISABLE_EXT_DCE_SRV`
- `OPC_DOWNLOAD_TEMPL_INDIVIDUAL`
- `OPC_SKIP_DCE_FORWARDING`
- `OPC_FORWARD_MGR_DCE_QUEUE`
- `OPC_CHK_DCE_ADDR_MISMATCH`
- `OPC_FORWARD_MGR_DCE_PIPE`
- `OPC_COMM_LOOKUP_RPC_SRV`
- `OPC_COMM_PORT_RANGE`
- `OPC_HBP_USE_ALL_PROTOCOLS`
- `OPC_HPDCE_CLIENT_DISC_TIME`
- `OPC_OPCCTLM_KILL_OPCUIWWW`
- `OPC_OPCCTLM_START_OPCSVCAM`
- `OPC_RESTART_COUNT`
- `OPC_RESTART_DELAY`
- `OPC_RESTART_PROCESS`
- `OPC_RESTART_TIMEFRAME`
- `OPC_SKIP_DCE_FORWARDING`
- `OPC_USE_DCE_FORWM`
- `OPCTRANM_TIMEOUT`
- `OPC_MSGM_USE_GUI_THREAD`
- `OPC_COMM_REGISTER_RPC_SRV`
- `OPC_COMM_RPC_PORT_FILE`
- `OPC_DCE_TRC_OPTS`
- `OPC_MSG_FORW_CHECKALIVE_INTERVAL`
- `OPC_MSGFORW_BUFFERING`

❑ APIs

HP plans to obsolete the following APIs with the next release of HPOM for UNIX:

- `opcsync_inform_user()`
- `opcmsg_escalate()`

❑ HPOM Server to Server Forwarding

With the next release of HPOM for UNIX only HTTPS-based message forwarding from server A to server B will be available. DCE-based message forwarding will become obsolete.

❑ Backward Compatibility with Previous HPOM Agents

The next release of HPOM for UNIX will no longer support backward compatibility with HPOM 7 DCE agents. Only HTTPS agent versions 8.53 or higher will be supported.

❑ HPOM DCE and HTTPS Compatibility Wrappers

HP plans to obsolete the DCE compatibility wrappers on the HTTPS agents. These include:

- `opcagt` (to be replaced by `ovc`)
- `opctemplate` (to be replaced by `ovpolicy`)

In addition, wrappers on the HPOM management server, such as `opcdeploy`, will also become obsolete.

❏ **Java UI**

The Java UI will no longer be supported on the following platforms:

- HP-UX PA-RISC all versions
- HP-UX Itanium 11.23
- Sun Solaris 8 and 9
- Red Hat 8
- MacOS X 10.3 and lower versions

The next release of HPOM for UNIX Java GUI will no longer support the embedded browser capability for UNIX platforms.

❏ **Service Navigator Value Pack (SNVP)**

HP does not plan further updates of SNVP. No new version of SNVP will be available with the next release of HPOM for UNIX. Check the Dependency Mapping Automation product as a potential migration path.

❏ **Operator-initiated Message Escalation**

HP plans to obsolete the possibility to forward or escalate an HPOM message to another HPOM for UNIX server by pressing the escalate button in the HPOM operational UIs.

❏ **Motif UI**

Because the operational Motif UI will become obsolete, plan and execute the migration to the operational Java UI accordingly.

The administrative Motif UI will become obsolete with a future release of HPOM for UNIX, the Web-based Administration UI will be used instead.

❏ **Template Administrator**

The template administrator user will become obsolete as a part of a Motif UI functionality.

Instead of template administrator, the `ompolicy_adm` user will be used to log in to the HPOM Administration UI.

❏ **Miscellaneous**

HP plans to obsolete the following features:

- *CD-ROM as Installation Media*

  The next release of HPOM for UNIX may no longer be shipped on CD-ROMs as installation media, but on Digital Versatile Disks (DVDs).

- *Expressions <S> and <nS>*

  The pattern-matching expressions `<S>` and `<nS>` used in templates will become obsolete with future releases.

- The following `itooprc` parameters will beome obsolete:

  — `which_browser`

  - `auto` and `manual` values for `web_browser_type`
  - `ice_proxy*`
  - `web_browser_html_appl_result`
- The following values for configuration variable `OPC_JGUI_INTERNBRW_DISABLED` will be no longer supported:
  - `EMBEDDED`
  - `BOTH`

2 Management Server and Java UI Installation Requirements

Management Server Hardware and Software Requirements

IMPORTANT The HPOM for UNIX 8.20 software is intended for use only on HP-UX 11.23 Itanium systems. *Do not* attempt to install HPOM for UNIX 8.20 on PA-RISC systems, but only on HP Integrity Itanium-2 servers.

Make sure that you have the following Patch Bundle installed:

BUNDLE11i B.11.23.0409.3 Required Patch Bundle for HP-UX 11i v2 (B.11.23), September 2004

Table 2-1 Supported Management Server Platforms

Management Server Platform	Requirements
HP-UX 11.11	`ovo.info.HP-UX.B.11.11.txt`
	See "NNM 7.51 and NNM 7.53 CD-ROM/DVD-ROM Installation Important Update" on page 130.
HP-UX 11.23 PA-RISC	`ovo.info.HP-UX.B.11.23.txt`
	Requires NNM 7.51, recommended NNM 7.53; see HPOM Installation Guide for the Management Server.
HP-UX 11.23 Itanium	`ovo.info.HP-UX.B.11.23.txt`
	Requires NNM 7.51, recommended NNM 7.53
HP-UX 11.31 PA-RISC	`ovo.info.HP-UX.B.11.31.txt`
	Requires the `libil.2` library and the revised version of NNM 7.53
HP-UX 11.31 Itanium	`ovo.info.HP-UX.B.11.31.txt`
	Requires the `libil.2` library and the revised version of NNM 7.53
Solaris 8	`ovo.info.SunOS.5.8.txt`
Solaris 9	`ovo.info.SunOS.5.9.txt`
Solaris 10	`ovo.info.SunOS.5.10.txt`
	Requires NNM 7.51, recommended NNM 7.53, and the HPOM SD installer for Sun Solaris with added Solaris 10 support, which is included in the `tar.Z` file; see HPOM Installation Guide for the Management Server.

For more details on installation requirements, refer to the HPOM for UNIX installation requirements info file applicable to your operating system version. Installation requirements info files are located in the `Required_OS_Patch_Lists` directory on the HPOM for UNIX CD1. To install a management server, use the `ovoinstall` script located at: `ftp://ovweb.external.hp.com/pub/cpe/ito/latest_ovoinstall/`.

Before installing HPOM, make sure that the system you select as the management server meets the hardware and software requirements listed in Chapter 1 of the *HPOM Installation Guide for the Management Server*. In particular, make sure that all required additional software packages and operating system patches are installed.

Table 2-2 Management Server Patch 8.35

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
HPOM 8 consolidated server 8.35	PHSS_40357	PHSS_40355	ITOSOL_00715

IMPORTANT To detect whether a management server patch is installed, run the following command:

```
ovconfget -ovrg server opc.patches
```

Running this command gives you a list of all installed HPOM management server patches, where you can easily check which patch is installed and which is not.

IMPORTANT The consolidated HPOM for UNIX server patch must be installed before the database configuration section of the HPOM for UNIX Management Server installation. See HPOM Installation Guide for the Management Server for more information.

NOTE HPOM for UNIX 8.20 requires an updated version of Network Node Manager 7.5. The corresponding NNM7.5 CD set is part of the HPOM for UNIX 8 media kit update as of January 2006.

Refer to Chapter 2 of the *HPOM Installation Guide for the Management Server* for detailed instructions on how to install HPOM, as well as chapter 7 of this Release Notes document for known problems and their workarounds.

The following readme file describes the HPOM for UNIX media CD contents and layout and help you to locate products and documentation:

`/README_HPUX_Itanium.txt`

WARNING **An HTTPS agent must be installed on the HPOM for UNIX 8 management server system. Do not install a DCE/NCS agent on the HPOM for UNIX 8 management server system. Installing the DCE/NCS agent on the HPOM management server system could damage your installation!**

Do not install the HTTPS agent on an HPOM for UNIX 7 management server system. HPOM for UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE It can be very helpful to set the PATH variable to include the following HPOM for UNIX directories on the Management Server: `/opt/OV/bin`, `/opt/OV/bin/OpC`, `/opt/OV/bin/Perl/bin` and `/opt/OV/bin/OpC/utils`.

IMPORTANT HPOM installs the `opcuihttps` binary into the `/opt/OV/contrib/OpC` directory. However, to successfully use the HTTPS-based Java GUI, the binary must also be available in the `/opt/OV/bin/OpC` directory at runtime. Once the runtime binary is available in `/opt/OV/bin/OpC`, it is automatically updated when you install an HPOM patch.

In case you have management server in a cluster environment copy this file on each cluster node. For more details, refer to `/opt/OV/contrib/OpC/opcuihttps.readme` file located on the HPOM management server.

High Availability Environments

Table 2-3 lists the High Availability environments supported on the HPOM for UNIX management server.

Table 2-3 Supported High Availability Environments

Management Server Platform	High Availability Application	Supported Versions
HP-UX 11.11	HP Serviceguard	11.14, 11.15, 11.16
	Veritas Cluster Server	3.5
HP-UX 11.23 PA-RISC	HP Serviceguard	11.16, 11.17, 11.18
	Veritas Cluster Server	4.1, 5.0
HP-UX 11.23 Itanium	HP Serviceguard	11.16, 11.17, 11.18
	Veritas Cluster Server	4.1[a], 5.0
HP-UX 11.31 PA-RISC	HP Serviceguard	11.17, 11.18, 11.19
	Veritas Cluster Server	5.0
HP-UX 11.31 Itanium	HP Serviceguard	11.17, 11.18, 11.19
	Veritas Cluster Server	5.0
Solaris 8	Sun Cluster	3.0, 3.1, 3.2
	Veritas Cluster Server	3.5, 4.0
Solaris 9	Sun Cluster	3.0, 3.1, 3.2
	Veritas Cluster Server	3.5, 4.0, 4.1, 5.0
Solaris 10	Sun Cluster	3.1, 3.2
	Veritas Cluster Server	4.1, 5.0

a. See “Installing HPOM for UNIX on VERITAS Cluster Server 4.1 on HP-UX 11.23 Itanium” on page 135

HPOM for UNIX 8 Management Server installation as provided in the media kit supports only standard HP Serviceguard environments, not Campus (Far Distance) Clusters or MetroClusters. For more information about HP Serviceguard support, contact HP support. Serviceguard ContinentalClusters are not supported at this time.

HPOM for UNIX Product Support Matrix with the latest patch levels available for the supported platforms is available through:

`http://support.openview.hp.com/selfsolve/document/KM323488`

or by following the HP Operations Manager Support Matrix > HP Operations Manager Support Matrix - Part 1 - Operations and Service Navigator Value Pack links at:

`http://partners.openview.hp.com/ovcw/pricing/config_matrix.jsp`

Cluster Awareness Support

HTTPS agents can be used to run on and to manage High Availability environments.

Table 2-4 Cluster Awareness Supported Platforms (HP-UX Itanium)

Cluster Awareness Supported Platforms	Agent[a]	Server[b]	
		HP-UX 11.23 Itanium	HP-UX 11.31 Itanium
HP Serviceguard			
11.14	✔		
11.15	✔		
11.16	✔	✔	
11.17	✔	✔	✔
11.18	✔	✔	✔
11.19			✔
11.16 RHEL 4	✔		
Sun Cluster			
3.0	✔		
3.1	✔		
3.2	✔		
Veritas Cluster Server			
3.5	✔		
4.0	✔		
4.1	✔	✔	✔
5.0	✔	✔	✔
Microsoft Cluster			
2000	✔		
2003	✔		
2008	✔		

Table 2-4 Cluster Awareness Supported Platforms (HP-UX Itanium) (Continued)

Cluster Awareness Supported Platforms	Agent[a]	Server[b]	
		HP-UX 11.23 Itanium	HP-UX 11.31 Itanium
Red Hat Enterprise Linux			
AS 4.0	✔		
AS 5.0	✔		

a. Agent runs on each physical node in a cluster.
b. HPOM management server is able to switch as package.

NOTE *HPOM for UNIX Product Support Matrix* with the latest patch levels available for the supported platforms is available through:

`http://support.openview.hp.com/selfsolve/document/KM323488`

or by following the HP Operations Manager Support Matrix > HP Operations Manager Support Matrix - Part 1 - Operations and Service Navigator Value Pack links at:

`http://partners.openview.hp.com/ovcw/pricing/config_matrix.jsp`

Certified Encoding and Character Sets on HPOM for UNIX Management Servers

Table 2-5 details the certified encoding and character sets that need to be set for the HPOM for UNIX management server and Oracle database host systems.

Table 2-5 Certified Encoding and Character Sets

Language Variables / Character Sets	Encoding `HPOM for UNIX Node Character Set`	HP-UX Language Variable `LANG`	Solaris Language Variable `LANG` and `LC_ALL`	Oracle Database Code Set `NLS_LANG`
English	ISO-885915	C, en_US.iso88591, en_US.iso885915@euro, en_GB.iso88591, en_US.iso885915@euro	C, en_US.iso88591, en_US.iso885915@euro, en_GB.iso88591, en_US.iso885915@euro	WE8ISO8859P15
Spanish	ISO-885915	es_ES.iso885915@euro	es_ES.iso885915-euro	WE8ISO8859P15
Japanese	Shift-Jis	ja_JP.SJIS	ja_JP.PCK	JA16SJIS
Korean	EUC	ko_KR.eucKR	ko, korean, ko_KR.EUC	KO16KSC5601
Simplified Chinese	GB2312	zh_CN.hp15CN	zh, zh_CN.EUC	ZHS16CGB231280
Traditional Chinese	BIG5	zh_TW.big5	zh_TW.BIG5	ZHT16BIG5

Other locales are also supported, for example, German, and French.

NOTE HPOM for UNIX 8 is internationalized and supports most of the common languages. It has been explicitly certified for English, Japanese, Korean, Simplified Chinese, Traditional Chinese and Spanish. Check also the Oracle documentation, which character sets are available.

Note that the UTF-8 character set is NOT supported by HPOM for UNIX 8 as the Oracle database character set.

Java UI Supported Platforms

Table 2-6 Java GUI Client Patch 8.35

Patch Name	Management Server Platform		
	HP-UX PA-RISC	HP-UX Itanium	Solaris
Java GUI client 8.35	PHSS_40468	PHSS_40467	ITOSOL_00721

HPOM for UNIX bundles JRE for all MS Windows platforms. For all other platforms the required Java Runtime version must be available. Besides the versions listed in the table below, Java GUI also supports J2SE 6.

Table 2-7 Support Matrix - Java UI

Java Runtime	JRE	JRE Plug-in	JRE Plug-in	JRE Plug-in
TYPE	as Application	Internet Explorer 5.5, 6, 7	Safari 1.2.3	Mozilla 1.7
Red Hat Enterprise Linux 3	1.6.0_16	N/A	N/A	1.6.0_16
Windows 2000	1.6.0_16	1.6.0_16	N/A	1.6.0_16
Windows 2003	1.6.0_16	1.6.0_16	N/A	1.6.0_16
Windows 2003 for Itanium	N/A	1.6.0_16	N/A	1.6.0_16
Windows XP	1.6.0_16	1.6.0_16	N/A	1.6.0_16
Windows Vista	1.6.0_16	1.6.0_16	N/A	1.6.0_16
HP-UX 11.11, 11.23 (PA-RISC), 11.23 (IPF), 11.31	1.6.0_04	N/A	N/A	1.6.0_04
Solaris 8, 9, 10	1.6.0_16	N/A	N/A	1.6.0_16
MacOs	1.6.0_13	N/A	1.5.0_13	1.6.0_13

NOTE If the default JRE version installed with the operating system is not the same as the one required by HPOM for UNIX, install the supported Java Runtime Environment JRE from the following location:

`http://www.hp.com/products1/unix/java/`

Set the location of the installed JRE directory to the `JAVA_DIR` environment variable, for example.:

```
export JAVA_DIR=/opt/java1.6/jre
```

3 HTTPS Agent Requirements

This chapter provides prerequisite information for HTTPS agents:

- HTTPS Agent Hardware Requirements
- HTTPS Agent Software Requirements

Before installing HPOM, make sure the hardware appropriate for your HTTPS managed node platform is available. The hardware requirements are detailed in “HTTPS Agent Hardware Requirements” on page 89.

Before installing HPOM, make sure the software appropriate for your HTTPS managed node platform is installed. The software requirements are detailed in the following tables:

HTTPS Agent Supported Platforms

NOTE HPOM for UNIX Product Support Matrix with the latest patch levels available for the supported platforms is available through:

`http://support.openview.hp.com/selfsolve/document/KM323488`

Starting with the support matrix from October 2009, HP Operations Agent is available for selection as a separate product from the product drop-down list.

With HPOM 8, the new HTTPS-agent software is available for highly secure communication between HPOM management servers and the following managed nodes:

Table 3-1 HPOM 8 HTTPS Agent Versions from HPOM Media Kit and Latest

Managed Node Platform	HTTPS Agent Version							
	Core Agent		EventAction		Embedded Performance		HPOM Accessories	
	HPOM CD	Latest	HPOM CD	Latest	HPOM CD	Latest	HPOM CD	Latest
HP-UX PA-RISC 11.11, 11.23	8.13	8.60	8.13	8.60	8.10	8.60	05.06.013	8.60
HP-UX Itanium IA64 11.23	8.12	8.60	8.13	8.60	8.10	8.60	05.06.013	8.60
HP-UX Itanium IA64 11.31	N/A	8.60	N/A	8.60	N/A	8.60	N/A	8.60
HP-UX PA-RISC 11.31	N/A	8.60	N/A	8.60	N/A	8.60	N/A	8.60
Solaris 9, 10 for SPARC	8.13	8.60	8.13	8.60	8.10	8.60	05.06.013	8.60
Solaris 10 for x86/x64	N/A	8.60	N/A	8.60	N/A	8.60	N/A	8.60
Microsoft Windows 2000, XP Professional, 2003, 2003 R2, Vista, 2008, 2008 core(32-bit)[a]	8.12	8.60	8.13	8.60	8.10	8.60	05.06.013	8.60

Table 3-1 HPOM 8 HTTPS Agent Versions from HPOM Media Kit and Latest

Managed Node Platform	HTTPS Agent Version							
	Core Agent		EventAction		Embedded Performance		HPOM Accessories	
	HPOM CD	Latest	HPOM CD	Latest	HPOM CD	Latest	HPOM CD	Latest
Microsoft Windows XP Professional, 2003, 2003 R2, Vista, 2008, 2008 R2, 2008 core (64-bit)	N/A	8.60	N/A	8.60	N/A	8.60	N/A	8.60
Microsoft Windows 2003, 2003 R2, 2008, 2008 R2 (IA-64)[b]	N/A	8.60	N/A	8.60	N/A	8.60	N/A	8.60
Linux (Kernel2.6) Refer to Table 3-4.	N/A	8.60	N/A	8.60	N/A	8.60	N/A	8.60
Linux Kernel 2.6 zSeries[b]	N/A	8.17	N/A	8.17	N/A	8.17	N/A	8.17
IBM AIX 5.3	8.13	8.60	8.13	8.60	8.10	8.60	05.06.013	8.60
IBM AIX 6.1[c]	N/A	8.60	N/A	8.60	N/A	8.60	N/A	8.60
Tru64 HP/Alpha	N/A	8.53	N/A	8.53	N/A	8.53	N/A	8.53
OpenVMS for Alpha	N/A	8.0-1	N/A	N/A	N/A	N/A	N/A	N/A
OpenVMS for Integrity	N/A	8.0-1	N/A	N/A	N/A	N/A	N/A	N/A

a. Windows 2000 with SP4 supported *only*. No `dll` is required, since `vc redist` is installed by the agent.
b. Requires the HP Operations management server patch 8.27.
c. Supported with the HTTPS agent patch 8.53; requires the HP Operations management server patch 8.33.

NOTE The HP Operations management server patch 8.32 or higher is required for the HTTPS agent 8.53.

For detailed information about the supported HP Operations agent versions, platforms, known problems, and workarounds, see the *HP Operations Agent Release Notes* available for download in the Operations Manager for UNIX directory (Product version 8.0) at the following location:

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

The HP Operations HTTPS agent for Tru64 with Cluster Awareness, the HP Operations HTTPS agent for AIX, and the HP Operations HTTPS agent for Solaris x86/x64 are available. Although these are not included in the HPOM for UNIX media kit, the agents can be downloaded from the following site:

`http://support.openview.hp.com/patches/ito/ito.jsp`

The HP Operations HTTPS agent for Linux kernel 2.6 and the HP Operations HTTPS agent for zSeries can be downloaded from the following site:

`ftp://ovweb.external.hp.com/pub/cpe/ito/zSeries_HTTPS_agent/`

An update for the `ovprotect` security tool is also available for download from the following location:

`ftp://ovweb.external.hp.com/pub/ovprotect`

The HTTPS agent for Windows x64 is supported with the HP Operations management server patch 8.33.

HPOM Agent now also provides container support of Global and Local Zones for the HTTPS agents for Solaris 10.

The HPOM HTTPS Agent for OpenVMS can be downloaded from the following site:

`http://h71000.www7.hp.com/openvms/products/openvms_OVO_agent/INDEX_HTTPS.HTML`

NOTE It is strongly recommended that you download and apply the latest HP Operations Manager software patches after installing the HPOM for UNIX Management Server. The overview of the latest software patches is available at the following location:

`http://support.openview.hp.com/selfsolve/document/KM322544`

Check the above web location quartlery for the latest HPOM for UNIX software patches.

HTTPS Agent Hardware Requirements

Before installing HPOM, make sure the operating systems you select as managed nodes meet the following hardware requirements:

Disk Space

Up to 100 MB depending on platform.

(Up to 200 MB is required during the initial software installation).

HTTPS Agent Software Requirements

Before installing HPOM, make sure the software appropriate for your HTTPS managed node platform is installed. The requirements are detailed in the following tables:

- Table 3-2, “HP-UX HTTPS Agent Software, Settings and Operating System Patches,” on page 91
- Table 3-3, “Solaris HTTPS Agent Software, Settings and Operating System Patches,” on page 92
- Table 3-4, “Linux HTTPS Agent Software, Settings and Operating System Patches,” on page 93
- Table 3-5, “Microsoft Windows HTTPS Agent Software, Settings and Operating System Patches,” on page 95
- Table 3-6, “AIX HTTPS Agent Software, Settings and Operating System Patches,” on page 96
- Table 3-7, “OpenVMS HTTPS Agent Software, Settings and Operating System Patches,” on page 98

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.

Comparison Between New HTTPS Agents (8.51 and Higher) and Previous HTTPS Agents (8.17 and Lower)

Beginning with the HTTPS agent version 8.51, HTTPS agent patches have become consolidated agent patches that contain all the agent components (including the coda). Because of this, the installation time is longer than usual.

With 8.51 HTTPS agent patches, the following new components are added to HTTPS agents:

- Xalan (HPOvXalanA)
  Prerequisite for AgtRep component. Used for parsing XML files
- Xerces (HPOvXercesA)
  Prerequisite for AgtRep component. Used for parsing XML files
- AgtRep (HPOvAgtEx)
  Service discovery component used from HPOM for Windows 8.x server. Included in packages for all management servers.

Information used for component deployment is stored in the `OVO-Agent.xml` file.

The new components cannot be used directly by HPOM for UNIX so far. They can be used for mixed HPOM for Windows 8.10/HPOM for UNIX 8 installations from the HPOM for Windows 8.10 server.

With 8.51 HTTPS agent the HPOM for Windows 8.10 server cannot detect the installed HTTPS agent version correctly and therefore redeploys the HTTPS agent software before doing any policy deployment. This problem is fixed with 8.53 HTTPS agent patch.

HTTPS Windows Agent Installation Time

The installation of the new HTTPS Windows agent version may take approximately 2 to 2.5 times more time than the installation of the previous HTTPS agent versions.

Agent Patch Installation

Before installing the 8.51 or higher agent patch, verify whether the old (A.08.10.160) version of the zSeries agent software is installed on the server. You can do this by executing the following command:

```
swlist -l fileset OVO-CLT.OVO-ZLIN-CLT
```

If version A.08.10.160 is installed, implement the fix for QXCR1000815477 to prevent possible patch installation problems. For details about this fix, see “HTTPS Managed Nodes Installation” on page 171.

HP-UX HTTPS Agent Software Requirements

Table 3-2 HP-UX HTTPS Agent Software, Settings and Operating System Patches

HP-UX Supported Platforms

- HP-UX PA-RISC: 11.11, 11.23, 11.31
- HP-UX Itanium IA64: 11.23, 11.31

Required Software

❑ **Internet Services**
SD package: `InternetSrvcs.INETSRVCS-RUN`

❑ **LAN/9000**
SD package: `Networking.NET-RUN`

❑ **SNMP Agent for MIB Monitoring** (optional)
SD Package for HP-UX 11.x and higher: `OVSNMPAgent`

❑ **Native Language Support (NLS) Package** (optional)
SD package: `OS-Core.NLS-AUX`

❑ **MIB-I or MIB II**
The MIB monitoring functionality of HPOM requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.

Kernel Settings
No specific settings required; default settings are acceptable.

Supported High-Availability Environments

- HP Serviceguard 11.14, 11.15, 11.16, 11.17, 11.18
- Veritas Cluster 3.5, 4.0, 4.1, 5.0

Operating System Patches

HP-UX 11.11 PA-RISC	
HWEnable11i	Hardware Enablement version B.11.11.0306.4 (June 2003) or higher
GOLDBASE11i	Gold Base Patch for HP-UX 11.i version B.11.11.0306.4 (June 2003) or higher
PHSS_26946	HP aC++ -AA runtime libraries (aCC A.03.37)
PHSS_28871	ld(1) and linker tools cumulative patch.
PHNE_28568	s700_800 11.11 ONC/NFS General Release/Performance Patch
PHCO_27950	tbl(1) cumulative patch (optional in case of man page formatting issues)
PHSS_33945	HP aC++ -AA runtime libraries
HP-UX 11.23 PA-RISC	
PHSS_35978	HP aC++ -AA runtime libraries
HP-UX 11.23 IA64 The HP Operations HTTPS agent for HP-UX 11.23 runs as a native 32-bit application on IA64. There are no 64-bit APIs offered.	
PHSS_31086	libunwind Library Cumulative patch
HP-UX 11.31 PA-RISC	
PHSS_35981	HP aC++ -AA runtime libraries
HP-UX 11.31 PA-RISC and Itanium Before installing the Embedded Performance Agent, a hotfix must be applied to the management server (CODA-290), available from HP support.	

Solaris HTTPS Agent Software Requirements

Table 3-3 Solaris HTTPS Agent Software, Settings and Operating System Patches

Solaris SPARC Supported Platforms Solaris 9, 10 **Solaris x86/x64 Supported Platforms** Solaris 10	
Sun Solaris Required Software ❑ **MIB** The MIB monitoring functionality of HPOM requires the snmpd of the HP Operations Manager platform, or SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC1158) compliant agent software. ❑ **MIB-I or MIB II** The MIB monitoring functionality of HPOM requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software. ❑ **Solaris x86/x64** At least a minimal installation of HPOM for UNIX Management Server version 8.22 is required.	

Kernel Settings
Set the following minimum kernel parameter values for Solaris 9:
`semsys:seminfo_semmni=30`
`semsys:seminfo_semmns=200`
`semsys:seminfo_semmsl=100`	

Supported High-Availability Environments • Sun Cluster 3.0, 3.1,3.2 • Veritas Cluster 3.5, 4.0, 4.1, 5.0	
Operating System Patches	
Solaris 9 SPARC	
111712	SunOS 5.9 64-bit shared library patch for C++
112963	Linker Patch (32-bit)
111722	SunOS 5.9 Math Library libm patch
Solaris 9 x86/x64	
111711	SunOS 5.9 32-bit shared library patch for C++
112963	Linker Patch (32-bit)
111722	SunOS 5.9 Math Library libm patch
Solaris 10 SPARC	
117461	Linker
120753	libmtsk
119963	SunOS 5.10: Shared library patch for C++
Solaris 10 x86/x64	
118345	SunOS 5.10_x86: ld & libc.so.
119964	SunOS 5.10_x86 Shared library patch for C++_x86
120754	SunOS 5.10_x86 libmtsk

Linux HTTPS Agent Software Requirements

Table 3-4 Linux HTTPS Agent Software, Settings and Operating System Patches

Linux Supported Platforms (Intel)

- Debian: 4.0r1
- Novell OES/Linux 2.0 (Cyprus)
- RHEL[a]
- SuSE and SuSE Enterprise Server[a]

No patches are required for the supported distribution versions.

Linux Supported Platforms (zSeries)

- SuSE Linux Enterprise Server 9 and 10

Linux Required Software

❏ **Red Hat Package Manager (RPM)**

Must be installed on Debian systems.

❏ **SNMP Daemon (optional)**

Ensure that the SNMP daemon (`snmpd`) is running when you install the software remotely from the HPOM management server. This allows the HPOM management server to automatically determine the node type of the Linux managed node. The SNMP daemon must also be running if you want to use MIB variable monitoring.

❏ **MIB-I or MIB II**

The MIB monitoring functionality of HPOM requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.

Kernel Settings

No specific settings required; default settings are acceptable.

Supported High-Availability Environments

- *RedHat Enterprise Linux* 4
  - — MC Serviceguard 11.16
  - — RedHat Cluster Suite 4
  - — Veritas Cluster 4.1
- *RedHat Enterprise Linux* 5
  - — MC Serviceguard 11.18
- *RedHat Enterprise Linux* 5.1
  - — RedHat Cluster Suite 5
- *RedHat Enterprise Linux* 5.3
  - — Veritas Cluster 5.0
- *SuSE Linux Enterprise Server* 10
  - — MC Serviceguard 11.18
  - — Veritas Cluster 5.0

a. For detailed information about which Linux HTTPS agent to select for which Linux platform, refer to the Support Matrix (SUMA) interface, which is available for download form the following location:
`http://support.openview.hp.com/selfsolve/document/KM323488`

NOTE During the installation, make sure that you select the right machine type for Linux RedHat AS 4 64-bit operating systems (the agent from the `linux/x86/linux26` directory must be used):

Platform Selector	Machine Type	OS Name
linux/x86/linux26	Intel/AMD x86(HTTPS)	Linux 2.6

Microsoft Windows HTTPS Agent Software Requirements

Table 3-5 Microsoft Windows HTTPS Agent Software, Settings and Operating System Patches

Microsoft Windows Supported Platforms

Windows 2000 SP4 only (x86)

Windows Server 2003 including SP2 or higher (x64, x86, IA-64)

Windows Server 2003 R2 including SP2 or higher (x64, x86, IA-64)

Windows Server 2008 (x64, x86, and IA-64)

Windows Server 2008 Core (x64, x86)

W2K3 R2 including SP2

XP Professional including SP1 and SP2 (x86)

Windows Vista (x64, x86)

Software Requirements

- ❏ **FTP**

  FTP Service must be running (required during "FTP Agent Package" installation). The FTP service must have read/write permission for the FTP home directory and must not allow anonymous FTP access if the `Administrator` account is used.

- ❏ **SNMP Services**

  SNMP services must be running if you plan to use discovery and other SNMP features of HPOM.

- ❏ **MIB-I or MIB II**

  The MIB monitoring functionality of HPOM requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.

Supported High-Availability Environments

- Veritas Cluster 5.0 (Windows)
- MS Cluster Server 2000, 2003 and 2008 (Windows Server)

Operating System Patches

Windows 2000

Service Pack	Service Pack 4
`msvcp60.dll`	No `dll` is required, since `vc redist` is installed by the agent.

Windows XP Professional

No patches are required.

Windows 2003

No patches are required.

AIX HTTPS Agent Software Requirements

Table 3-6 AIX HTTPS Agent Software, Settings and Operating System Patches

AIX Supported Platforms

- ❏ AIX: 5.3, 6.1 English and Japanese Locales
- ❏ POWER 3-5, and 6 hardware with 32-bit Kernel running AIX 5.3 OS
- ❏ POWER 5-6 hardware with 64-bit Kernel running AIX 6.1 OS

Required Software

The HPOM HTTPS agent for AIX is available. Although it is not included in the HPOM for UNIX media kit, it can be downloaded from the following site:

`http://support.openview.hp.com/patches/ito/ito.jsp`

NOTE: Make sure you have installed a depot on the HPOM management server before you begin with the AIX HTTPS agent patch installation.

When installing the depot on HP-UX 11.23 PA-RISC and HP-UX 11.23 Itanium platforms, the `allow_incompatible` parameter must be set to `true`. For example,

```
swinstall -x allow_incompatible=true -s /tmp/AIX-HTTPS-Agent/OVO-AIX-CLT.depot \*

swconfig -x allow_incompatible=true OVO-CLT.OVO-AIX-CLT
```

- ❏ **SNMP Daemon (optional)**

  Ensure that the SNMP daemon (`snmpd`) is running when you install the software remotely from the HPOM management server. This allows the HPOM management server to automatically determine the node type of the managed node. The SNMP daemon must also be running if you want to use MIB variable monitoring.

- ❏ **MIB-I or MIB II**

  The MIB monitoring functionality of HPOM requires SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software.

Kernel Settings

No specific settings required; default settings are acceptable.

Supported High-Availability Environments

- HACMP 5.2, 5.3, 5.4, 5.4.1 and 5.5
- Veritas Cluster 4

OS-SPI Support	
Required patches	
Operating System Patches	
AIX 5.2	
Patch Level 4	
AIX 5.3	
Patch Level 2	

Table 3-6 AIX HTTPS Agent Software, Settings and Operating System Patches

Additional Requirements	
Performance Statistics filesets	bos.perf.libperfstat bos.perf.perfstat bos.perf.perfstat
POWER 5-6 with 64-bit Kernel running AIX 6.1	HP Operations agent 8.6 supports only the TL2 type of AIX 6.1 systems. To avoid memory leaks for different agent processes, make sure the following libraries are present on the AIX 6.1 node: • `xlC.aix61.rte` (version 10.1.0.2 or higher) • `xlC.rte` (version 10.1.0.2 or higher) If you want to use the HP Operations agent with a non-root user on the AIX 6.1 node, apply the TL3 for AIX 6.1 on the node.

OpenVMS HTTPS Agent Software Requirements

Table 3-7 OpenVMS HTTPS Agent Software, Settings and Operating System Patches

OpenVMS Supported Platforms

OpenVMS Alpha versions 7.3-2, 8.2, 8.3

OpenVMS Integrity versions 8.2-1, 8.3, 8.3-1H1

Software Requirements

❏ **OpenVMS Alpha Version 7.3-2**

- VMS732_SYS V8.0 or later
- VMS732_PTHREAD V3.0 or later
- VMS732_UPDATE V5.0 or later
- VMS732_RPC V4.0 or later

❏ **OpenVMS Alpha Version 8.2**

- VMS82A_UPDATE V7.0 or later
- VMS82A_SYS V7.0 or later

❏ **OpenVMS Alpha Version 8.3**

- VMS83A_UPDATE V3.0 or later

❏ **OpenVMS Integrity Version 8.2-1**

- VMS821I_UPDATE V5.0 or later
- HP I64VMS VMS821I_ICXXL V2.0 or later

❏ **OpenVMS Integrity Version 8.3**

- VMS83I_UPDATE V1.0 or later
- VMS83I_SYS V1.0 or later
- HP I64VMS VMS83I_ICXXL V2.0 or later

The patches are available at the following location:
`http://www2.itrc.hp.com/service/patch/mainPage.do`

❏ **SSL for OpenVMS**

You must have SSL version 1.2 or later installed and running on your OpenVMS system. The SSL kits are available at the following location:

`http://h71000.www7.hp.com/openvms/products/ssl/ssl.html`

Table 3-7 OpenVMS HTTPS Agent Software, Settings and Operating System Patches (Continued)

❑ **SNMP** SNMP must be enabled and started for the OpenVMS HTTPS Agents to recognize the operating system. You need to install the HTTPS Agent and SPI software on ODS-5 disk. OpenVMS agent depots are available at the following location: `http://h71000.www7.hp.com/openvms/products/openvms_OVO_agent/index.html`

4 Last-Minute Changes to Documentation

IMPORTANT Always check the latest available versions of HPOM for UNIX manuals, available from the following location:

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

Setting Up an Independent Database-Server System

The following changes must be made in the "Setting Up an Independent Database-Server System" section of the HPOM Installation Guide for the Management Server:

- The following text from step 4:

  When this message is displayed, leave the `ovoinstall` window open without answering the question and proceed with configuring the database-server system as described in the following procedure.

  must be changed to:

  When this message is displayed, leave the `ovoinstall` window open without answering the question. In a new terminal window, install the latest HP Operations management server. Proceed with configuring the database server system as described in the following procedure.

- Instead of editing the `/etc/exports` file, as described in step 5, the `/etc/dfs/dfstab` file must be edited and the following lines must be entered:

  ```
  share -F nfs -o rw=<DB_server> -d "home dirs" /home
  share -F nfs -o ro,rw=<DB_server>,root=<DB server> /opt/OV
  share -F nfs -o ro,rw=<DB_server>,root=<DB server> /var/opt/OV
  share -F nfs -o ro,rw=<DB_server>,root=<DB server> /etc/opt/OV
  ```

  For detailed information, see the *share* manpages.

- Note that it is not obligatory that the `ORACLE_SID` value mentioned in step 10 is `openview`.
- Adding the values for `ORACLE_HOME`, `ORACLE_SID`, and `NLS_LANG` to `/etc/rc.config.d/ovoracle` and exporting the Oracle variables, described in steps 10 and 11, should also be done on the database server.
- The following note should be removed from step 17 and included in step 12:

NOTE When prompted to enter the data and the index directories, accept the recommended value (the same one for both the data and index), for example:

`/opt/oradata/openview`

Do not specify any of the following locations for the data and index directory: `/opt/OV`, `/var/opt/OV`, and `/etc/opt/OV`. Also, the name of the directory must correspond to the `ORACLE_SID` value (`openview` is recommended).

- Step 18 should precede steps 14 and 15, so make sure that you do the following before unmounting the `/opt/OV`, `/etc/opt/OV`, and `/var/opt/OV` directories, and exiting the database server:

  Wait for the database server system configuration to complete, then press [`Enter`] in the `ovoinstall` window to continue with the HPOM installation.

HPOM Developer's Reference

The following must be added to the *HPOM Developer's Reference*:

- Page 98: The following description must be added beside the description of `OPCSVIF_MSG_EVENTS`:

  `OPCSVIF_MSG_EVENTS_ALL`

  This interface type is used to receive Message Events caused by changes to messages by other operators, in addition to new messages and a few formerly internal events (like duplicate received).

- Page 105: `OPCSVIF_MSG_EVENTS_ALL` must be added beside `OPCSVIF_MSG_EVENTS`.

- Page 467: The following must be added to the table describing `OPCDTYPE_MESSAGE_EVENT` (the `Description` column of the `OPCDATA_EVENT_FLAG` attribute):

  — `OPC_MSG_EVENT_CHGSEV`

  — `OPC_MSG_EVENT_MSGCHG`

  — `OPC_MSG_EVENT_CMA_UPDATE`

  — `OPC_MSG_EVENT_DEL`: Message was deleted.

  — `OPC_MSG_EVENT_ACTIVE_RECEIVED_MSG`[1]: New active message received. In case you registered for this event and if `OPCUIWWW_NEW_MSG_NO_DB` is `TRUE`, the new message is received instead of an event.

  — `OPC_MSG_EVENT_DUPL_RECEIVED`[1]: Duplicate of message received.

  — `OPC_MSG_EVENT_ANNO_ADD`[1]: Annotation added.

  — `OPC_MSG_EVENT_ANNO_SET`[1]: Annotation modified.

  — `OPC_MSG_EVENT_ANNO_DEL`[1]: Annotation deleted.

  — `OPC_MSG_EVENT_READONLY_MSG`[1]: Message became read-only.

  — `OPC_MSG_EVENT_CTRL_MSG`[1]: Message became a control switch message.

  — `OPC_MSG_EVENT_ACTIVE_RECEIVED`[1]: New active message received.

  — `OPC_MSG_EVENT_HISTORY_RECEIVED`[1]: New history message received.

1. This event occurs only if you open the Message Event Interface (MEI) with `OPCSVIF_MSG_EVENTS_ALL`.

Installing HPOM in a VERITAS Cluster Environment

The information describing installing HPOM in a VERITAS cluster environment in the HPOM Installation Guide for the Management Server must be changed on the following pages:

267:

`ovresore.ovpl` in the following sentence must be changed to `ovrestore.ovpl`:

But to restore a backup with `ovresore.ovpl` and to use the offline backup scripts, the OVO and Oracle HA resource groups must run on the same node.

280 and 287:

The comma at the end of the following command must be removed:

```
ifconfig <network_interface>:1 inet \
<IP> netmask 255.255.0.0 up,
```

293 and 297 (as well as 250 and 254):

The period at the end of the following link must be removed:

`/opt/OV/bin/OpC/utils/ha/ha_mon_ovserver_3tier.`

302:

The following must be added at the end of the “Installing the OVO Agent Software and Templates on Cluster Nodes” section:

IMPORTANT Make sure you have either `REXEC`, `RSHD`, or `SSH` services enabled on the remote agent before you start the HP Operations agent installation. Otherwise the agent installation will fail.

Installing Agent on the Cluster Physical Node

The following note must be added to the “About Managed Nodes” section in the HPOM Administrator’s Reference:

NOTE When installing agent on the cluster physical node, the same software requirements must be met as when installing the HP Operations agent on the non-cluster agent node.

opcmsg_set_owner()

The following API must be included in the “Server Message API” section of the HPOM Developer’s Reference:

opcmsg_set_owner()

```
#include opcsvapi.h

int opcmsg_set_owner (
             opc_connection     opc_conn,        /* in */
             const opcdata      message_id,      /* in */
             const char *       operator_name    /* in */
              );
```

Parameters

opc_conn	Connection to the HPOM database.
message_id	Message ID of the message to be owned; of type OPCDTYPE_MESSAGE_ID.
operator_name	Name of the operator who will become the owner of the message.

Description

Use the function opcmsg_set_owner() to set the owner of an active message to the specified operator. The specified operator must have permission to own messages.

To use this function, it is necessary to connect to the management server as an HPOM user with administrator rights, using the opc_connect() function.

A message event is sent to all running GUIs to update them with the new information. Applications can register with the Message Event Interface to get the event OPC_MSG_EVENT_OWN.

Return Values

OPC_ERR_OK	OK
OPC_ERR_INVALID_INPARAM	opc_conn is NULL; message_id is NULL; message_id is not of type OPCDTYPE_MESSAGE_ID.
OPC_ERR_INVALID_ID	Database contains no message with that ID, or the given ID is malformed.
OPC_ERR_DATABASE_ERROR	Cannot get operator/message capabilities, cannot get message details, cannot get database information for GUI change request.
OPC_ERR_ACCESS_DENIED	User is not allowed to own the message; user does not have administrative rights.
OPC_ERR_NO_MEMORY	Cannot reserve memory for ID, cannot allocate memory for GUI information request.
OPC_ERR_CANT_INFORM_UI	Cannot inform GUI.
OPC_ERR_MSG_OWNED_BY_ANOTHER_USER	Message is owned by another HPOM user.

Versions

8.25 and later

Location of Fact and Data Store Files

The location of the fact and data store files for an HTTPS agent described on page 88 of the *Configuring Circuits with ECS Designer for OVO/UNIX* document must be replaced with the following:

management server: `/var/opt/OV/conf/OpC/mgmt_sv/`

managed node (UNIX): `/var/opt/OV/conf/eaagt`

managed node (Windows): the default location: `C:\Program Files\HP OpenView\data\conf\eaagt`

Deinstalling HPOM from the Active Cluster Node

The following text must be added at the end of the "Deinstalling OVO from the Active Cluster Node" section in the HPOM Installation Guide for the Management Server:

After you deinstalled OVO from this cluster node, check whether the HA Resource group is still present by entering:

`/usr/sbin/cmviewcl -p ov-oracle`

If the HA Resource group is still present on the node, remove it by entering:

`/usr/sbin/cmdeleteconf -f -p ov-oracle`

opc_agent_status table

It should be documented that the database schema does not provide the information about the `opc_agent_status` table not being currently used.

The `opc_agent_status` table is empty, although according to the database schema this table contains the status of the agents on the managed nodes.

Consider that this table is not currently used and is meant to be used later.

Installing HPOM Agents on the Managed Nodes

`RSHD` should be changed to `RSH` in the following important notice in the "About Managed Nodes" section from the HPOM Administrator's Reference:

IMPORTANT Make sure you have either `REXEC`, `RSHD` or `SSH` services enabled on the remote agent (HTTPS-based) before you start the HPOM agent installation. Otherwise the agent installation will fail.

Oracle 11g Support-based Documentation Changes

IMPORTANT You need to install HPOM for UNIX 8.31 patch to use the Oracle 11g functionality.

Due to Oracle 11g support introduced with the HPOM for UNIX 8.31 patch, the following manuals must be updated:

- *"HPOM Installation Guide"*
- *"HPOM Administrator's Reference"*

NOTE Though HPOM for UNIX supports Oracle 10g and 11g, HPOM does not take advantage of the new features provided by these versions. HPOM uses the same approach to create the database for Oracle 9, Oracle 10, and Oracle 11. Thus, HPOM may use some settings that are different from those recommended by Oracle for newer versions, but are still fully supported by Oracle.

HPOM Installation Guide

- The software requirements for the management server should include the latest version of Oracle, namely Oracle 11g, whenever the older versions of Oracle are mentioned. These latest requirements are as follows:

  For database server:

  — Oracle 11g 11.1.0.6.0

  — Oracle Net Services 11.1.0.6.0

  For database client:

  — Oracle 11g 11.1.0.6.0

  — Oracle Net Services 11.1.0.6.0

  — SQL * Plus 11.1.0.6.0

NOTE For Itanium, 11.1.0.7.0 patch set is required.

- The “Starting and Stopping an Oracle Database Automatically” section should besides the older Oracle versions also mention Oracle 11g.
- For Oracle 11g only:

  The following link to Oracle client libraries must be entered for the decoupled HP Operations management server database installation, which is described in the “Installing the Oracle Database Server for HPOM in a Cluster Environment” section (step 4):

  ```
  rm -f /opt/OV/lib/hpux32/libclntsh.so.10.1
  ln -s <ORACLE_HOME>/lib32/libclntsh.so \
  /opt/OV/lib/hpux32/libclntsh.so.10.1
  ```

  ```
  rm -f /opt/OV/lib/hpux32/libclntsh.so.11.1
  ln -s <ORACLE_HOME>/lib32/libclntsh.so \
  /opt/OV/lib/hpux32/libclntsh.so.11.1
  ```

  ```
  rm -f /opt/OV/lib/hpux32/libnnz11.so
  ln -s <ORACLE_HOME>/lib32/libnnz11.so \
  /opt/OV/lib/hpux32/libnnz11.so
  ```
- The “Setting Up an Independent Database-Server System” procedure should contain the Oracle 11g specifics.

  Step 10 and 11:

  export ORACLE_HOME=/opt/oracle/product/*<version>*

  where *<version>* is the Oracle database version 11.1.0

  Step 16:

  Enter the following link for Oracle 11g:

  ```
  ln -s <ORACLE_HOME>/lib32/libclntsh.so \
  /opt/OV/lib/hpux32/libclntsh.so.10.1
  ```

  ```
  ln -s <ORACLE_HOME>/lib32/libclntsh.so \
  /opt/OV/lib/hpux32/libclntsh.so.11.1
  ```

  ```
  ln -s <ORACLE_HOME>/lib32/libnnz11.so \
  /opt/OV/lib/hpux32/libnnz11.so
  ```

  Some link pathnames in the *HPOM Installation Guide* for HP-UX Itanium are not correct. HP-UX Itanium libraries should be linked to the `/opt/OV/lib/hpux32` directory. Link to `/opt/OV/lib/hpux32` instead of `/opt/OV/lib`.

HPOM Administrator’s Reference

The “To Enable Archive Log Mode in Oracle” section should be updated as follows:

- The note on page 390 must besides Oracle 10 g also mention Oracle 11g.
- The `log_archive_dest_n` parameters can be used instead of the `log_archive_dest` parameter for Oracle 10g and 11g.

Upgrading to Oracle 11g

This section describes how to upgrade Oracle 9.2.0.6 or Oracle 10.1.0.4 to version 11g (11.1.0.6). After installing Oracle 11g (11.1.0.6), the 11.1.0.7 patch level is required. For more detailed information see the *Oracle Database Upgrade Guide 11g*.

NOTE After you have started up your database with ORACLE_HOME containing the new Oracle software, do not attempt to go back to the old version, as this could result in database files being corrupted.

Check the System Requirements

Make sure your system meets the requirements stated in the Oracle documentation. There might be a difference in required OS versions, patches, and kernel parameters for different Oracle versions (Oracle 9i, Oracle10g Release 1, and Oracle 10g Release 2, and Oracle 11g).

Check also requirements listed in the *Oracle Database Upgrade Guide 11g* as Oracle upgrade can require different Oracle patch levels. Oracle 11g is supported on HP-UX Itanium 11.23 and 11.31.

Prepare the Database for the Upgrade

Before upgrading the Oracle software, perform the following steps:

1. Exit the HPOM GUIs (motif and java) and stop the HP processes with **`ovstop -c`** and **`ovc -kill`**.
2. Stop all processes that access the Oracle database.
3. Shut down the database and, if necessary, the SQL*Net listener, as follows:
   a. Log in as user oracle or switch to user oracle:

      ```
      su - oracle
      ```

   b. If you are using SQL*Net, shut down the SQL*Net listener using the following command:

      ```
      $ORACLE_HOME/bin/lsnrctl stop
      ```

   c. Start the Oracle SQL*Plus tool and shut down the database as follows:

      ```
      $ORACLE_HOME/bin/sqlplus /nolog
      SQL> connect / as SYSDBA
      SQL> shutdown
      SQL> exit
      ```

4. Perform a full offline backup of the Oracle database or the complete system before you perform the upgrade. A full backup ensures that you can recover from errors encountered during the upgrade process.

Installation of Oracle 11g

Perform the following steps to install Oracle Database 11g software:

1. *If you are upgrading from Oracle 10g Release 1 or Release 2*:

Since user oracle, oinstall (primary) and dba (secondary) groups were already created as prerequisites for the Oracle 10g installation, there is no need to create them again.

If you are upgrading from Oracle 9:

Modify the user oracle with the following attributes:

a. Create a UNIX group named oinstall. The group ID should be greater than 100.

b. Make the user oracle a member of the group oinstall as the primary group, and dba as the secondary group.

Set umask to allow users to access the Oracle binaries:

```
umask 022
```

2. Create the Oracle home directory ORACLE_HOME:

```
mkdir /opt/oracle/product/11.1.0
```

You can also choose a different directory for ORACLE_HOME but you must use it consistently in all subsequent steps.

3. Change the ownership of the directories to oracle:oinstall by entering:

```
chown -R oracle:oinstall /opt/oracle/product/11.1.0
```

4. Change the following Oracle environment variables in the /home/oracle/.profile of user oracle:

```
export ORACLE_HOME=$ORACLE_BASE/product/11.1.0
```

This variable determines the location and the version of the Oracle installation. This is the recommended setting. You can choose a different setting, if needed.

5. Re-login as user oracle and start the Oracle Universal Installer.

6. After the Oracle Universal Installer is started, follow the instructions for installing the Oracle Database software provided by Oracle.

7. After exiting the Oracle Universal Installer, run the utlu111i.sql script as described in "Run the Pre-Upgrade Information Tool" chapter in the *Oracle Database Upgrade Guide 11g* and resolve all warnings.

8. Run the Oracle Database Upgrade Assistant to upgrade the database software. Be sure to carefully follow the *Oracle Database Upgrade Guide 11g*. When asked wether to use the Automatic Storage Management option, select Do Not Move Database Files as Part of Upgrade.

Configuring HP BTO Software Products to Use the New Oracle Version

Perform the following steps as user oracle:

1. Since the upgrade of Oracle database was done by Oracle Database Upgrade Assistant, there is no need to manually move the parameter file of the ORACLE_SID database instance to the new location. This is usually a symbolic link to /opt/oracle/admin/<ORACLE_SID>/pfile/init<ORACLE_SID>.ora.

2. Copy the SQL*Net files from the old ORACLE_HOME to the new location, for example:

```
cd  /opt/oracle/product/<old_version>/network/admin/
cp listener.ora /opt/oracle/product/11.1.0/network/admin/listener.ora
cp tnsnames.ora /opt/oracle/product/11.1.0/network/admin/tnsnames.ora
cp sqlnet.ora /opt/oracle/product/11.1.0/network/admin/sqlnet.ora
cp tnsnav.ora /opt/oracle/product/11.1.0/network/admin/tnsnav.ora
```

3. As user root, replace all occurrences of the old ORACLE_HOME value with the new value in the following files. You have to change variable assignments as well as directory names containing this value. Replace the following:

   -ORACLE_HOME in /etc/opt/OV/share/conf/ovdbconf
   -DB_RELEASE in /etc/opt/OV/share/conf/ovdbconf
   -ORACLE_HOME in /opt/oracle/product/11.1.0/network/admin/listener.ora
   -LOG_DIRECTORY_LISTENER in /opt/oracle/product/11.1.0/network/admin/listener.ora
   -TRACE_DIRECTORY_CLIENT in /opt/oracle/product/11.1.0/network/admin/sqlnet.ora
   -LOG_DIRECTORY_CLIENT in /opt/oracle/product/11.1.0/network/admin/sqlnet.ora
   -ORA_CRS_HOME in /sbin/init.d/init.cssd

4. Change the symbolic links used by HP Operations Manager. Change the following symbolic links:

   libclntsh.so, libclntsh.so.1.0, libclntsh.so.8.0, libclntsh.so.9.0, libclntsh.so.10.1, libopcora.so

   These point to the Oracle shared libraries. Remove them and recreate new links that point to the Oracle shared libraries in the new ORACLE_HOME, for example:

   ```
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libclntsh.so /opt/OV/lib/libclntsh.so
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libclntsh.so /opt/OV/lib/libclntsh.so.1.0
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libclntsh.so /opt/OV/lib/libclntsh.so.8.0
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libclntsh.so /opt/OV/lib/libclntsh.so.9.0
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libclntsh.so
   /opt/OV/lib/libclntsh.so.10.1
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libclntsh.so
   /opt/OV/lib/libclntsh.so.11.1
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libnnz11.so /opt/OV/lib/libnnz11.so
   ln -s /opt/oracle/product/11.1.0/lib32/hpux32/libclntsh.so libopcora.so
   ```

5. To find the missing files and to avoid starting the database with the wrong ORACLE_HOME value, it is recommended you rename the old ORACLE_HOME directory.

6. Start the database and the SQL*Net listener as follows:

   a. Log in as user oracle or switch to user oracle.

   b. If you are using SQL*Net, start up the SQL*Net listener:

      ```
      $ORACLE_HOME/bin/lsnrctl start
      ```

   c. Start the Oracle SQL*Plus tool and start the database, for example:

      ```
      $ORACLE_HOME/bin/sqlplus /nolog
      SQL> connect / as SYSDBA
      SQL> startup
      SQL> exit
      ```

7. If you no longer need the old Oracle version and after you verified that the new Oracle version works, you can remove the old Oracle version to gain disk space.

8. You can start the HPOM for UNIX Management Server and other HP component processes.

Tracing for the seadapter and for `cadmexport`

The "Tracing for the seadapter and for cadmexport" section of the *Service Configuration for Service Navigator Reference Guide* (Software Versions: 8.0 and 9.0) states that the following options accept `TRUE` and `FALSE` values:

- `SEADAPTER_MAIN_TRACE`
- `SEADAPTER_SOCKET_TRACE`
- `SEADAPTER_PARSER_TRACE`
- `SEADAPTER_MODEL_TRACE`

This is not true, as the above mentioned values should be entered in lower case, so the correct values are `true` and `false`, and not `TRUE` and `FALSE`.

Installing 10.2.0.2 Patch Set for Oracle Database Server

To install the 10.2.0.2 Patch Set for the Oracle Database Server, follow these steps:

1. Download the patch set installation archive to a directory.

NOTE	Make sure that this directory is not Oracle home directory, or under it in the filesystem structure.

2. Unzip and extract the installation files and start the Oracle Universal Installer as user `oracle`.Enter the following:

   `cd <patchset_directory>/Disk1`

   Where the *`<patchset_directory>`* is a directory where you have extracted the installation files.

   `./runInstaller`

3. In the Oracle Universal Installer `Welcome` window, click `[Next]`.

   The `Specify File Locations` window opens.

4. In the `Specify File Locations` window, click `[Next]`.

   Select the `products.xml` file from the stage directory where you unpacked the patch set files and click `[Next]`. For example:
   `<directory_path>``/stage/products.xml`

5. In the `Name` field of the `Destination` section, select the name of the Oracle home from the drop-down list, and click `[Next]`.

   The `Summary` window opens.

6. In the `Summary` window, click `[Install]` to start the installation.

7. When prompted, run the `$ORACLE_HOME/root.sh` script as the `root` user.

The following should be displayed:

```
The following environment variables are set as:
ORACLE_OWNER= oracle
ORACLE_HOME= /opt/oracle/product/<version>
```

Where the *<version>* is the Oracle database version, 10.2.0.

Enter the full pathname of the local bin directory [/usr/local/bin].

Enter: **/usr/lbin**

8. When the root.sh utility has finished, click [OK] in the Setup Privileges window.

NOTE If the Oracle Universal Installer warns you that some of the Oracle processes are still running and thus is impossible to proceed with the installation, stop the ocssd.bin Oracle daemon using the following command:

/sbin/init.d/init.cssd stop

After stopping the ocssd.bin daemon, continue with the installation.

Upgrading OVO 7 to Version 8.10 in a Cluster Environment

The procedure of upgrading OVO 7 to version 8.10 in a cluster environment is not described correctly in the *Basic Installation Scenario with Local Database for HP Serviceguard Cluster* and *Installation Guides*. These documents state the following:

To upgrade the HPOM management server running in a cluster environment from version A.07.1x to version A.08.10, you must first perform the upgrade procedure on all the passive nodes, and then on the active node.

This is not true, as to upgrade the HPOM management server running in a cluster environment from version A.07.1x to version A.08.10, you must first perform the upgrade procedure *on the active node*, and then *on the passive node(s)*.

Before Installing an Oracle Database

In the “Before You Install an Oracle Database” section of the *Installation Guide*, instead of “Run SAM as root” (step 2), the following should be written: Run SMH as root.

In the above mentioned section, add step f under step 2 with the following text:

The required shell for the oracle user is **POSIX shell (sh)**.

Add the following line to the /home/oracle/.profile directory:

SHELL=/sbin/sh

ha_mon_cb Cluster Monitor Script Change

The ha_mon_cb cluster monitor script (linked to M200_cb) has been changed to exit if ovbbccb is not running, which then causes failover.

Make sure that you disable the HARG monitoring before completely stopping the agent processes on the management server, for example:

```
/opt/OV/lbin/ovharg -monitor ov-server disable
ovc -kill
```

```
ovc -start
/opt/OV/lbin/ovharg -monitor ov-server enable
```

Shell Script for Uploading the Agent Information into the Database

Step 4 in the "Installing HTTPS Agent-Software Packages on the Management-Server System Manually" of the HPOM Installation Guide should be changed to:

Upload the agent information into the database by executing the following command:

```
for i in `find . -type f -name AgentPlatform` \
do j=`echo ${i} | sed -e 's|^./||' -e 's|\/AgentPlatform||'` \
/opt/OV/bin/OpC/opcagtdbcfg -p ${j} -d -f \
done
```

Independent Database Server Installation in a Cluster Environment

The following two commands are missing in the "Oracle Database Server on a Local Disk" and "Oracle Database Server on a Remote Filesystem" subsections of the "Installing the Oracle Database Server for HPOM in a Cluster Environment" section of the HPOM Installation Guide regardless of the platform and the cluster environment:

```
/opt/OV/bin/ovconfchg -ns opc -set OPC_HA TRUE
```

```
/opt/OV/bin/ovconfchg -ns opc -set OPC_MGMT_SERVER <SERVER_VIRTUAL_LONG_HOSTNAME>
```

They must be executed after setting an Oracle database hostname and before configuring the Oracle database to avoid the distribution failure.

NOTE Set OPC_MGMT_SERVER and OPC_HA with the **-ovrg server** option before calling opcdbsetup.

Decoupled HPOM Management Server Installation with Oracle Database Server on a Shared Disk (Exceptional)

In the *HPOM Installation Guide*, the subsection “Decoupled OVO management server database installation” of the “Oracle Database Server on a Shared Disk (Exceptional)” section, describing the decoupled cluster installation of the Oracle database server on a shared disk for the first cluster node, requires additional information.

In a decoupled cluster installation of the Oracle database server on a shared disk, you need to change `/etc/opt/OV/share/conf/ovdbconf` to use the `ORACLE_HOME` of the Oracle client installation as documented in the *HPOM Installation Guide*. However, this would mean that the `/sbin/init.d/ovoracle` script would also use these settings (if present), and fail if they are not set.

To make sure that the ovoracle script uses the Oracle server `ORACLE_HOME` while the HPOM binaries continue to use the Oracle client `ORACLE_HOME`, the following configuration information should be inserted directly after step2:

Edit the `/etc/rc.config.d/ovoracle` file by adding the following lines, using your specific settings:

```
ORACLE_HOME=<Oracle Server Home>
ORACLE_SID=<ORACLE_SID>
export ORACLE_HOME ORACLE_SID
```

This reflects the location of the Oracle client software. The `/etc/rc.config.d/ovoracle` file is used as a configuration file by the `/sbin/init.d/ovoracle` script. The script is used by the Oracle HARG to start the Oracle database.

Make sure that you use the latest version of the `/sbin/init.d/ovoracle` script. You need to copy the file from `newconfig` (on all the physical cluster nodes) by running this command:

```
cp /opt/OV/newconfig/OpC/sbin/init.d/ovoracle \
/sbin/init.d/ovoracle
```

PAM Failed Login Counter Functionality

The following subsection titled “PAM Failed Login Counter Functionality” should be added at the end of the “About PAM Authentication” section of the HPOM Administrator’s Reference:

With the PAM failed login counter functionality, the number of PAM authenticated failed logins to the Java and Motif GUIs can be counted.

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
   ```

PAM failed login counter is implemented for each operator in the corresponding namespace to reduce the number of attempts to use invalid/expired passwords.

For example, if the `opc_adm` operator fails to log in five times, the following config parameters are set in the corresponding `user.opc_adm` name space (`ovrg = server`):

```
[user.opc_adm]
FAILED_LOGIN_ATTEMPT_COUNTER=5
LAST_FAILED_LOGIN_ATTEMPT=1197550378
LOGIN_ATTEMPT_DELAY=240
```

Restricting Actions on the Management Server

In the “Security in Manager of Manager (MoM) Environments“ section on page 70 of the HPOM HTTPS Agent Concepts and Configuration Guide the following information about restricting actions on the management server should be added:

By default, in the merged MoM environment all automatic and operator initiated actions are allowed on both management servers because both management servers have root certificates installed and a trust relationship established. To restrict actions on management server A from agents belonging to other management servers, set the following configuration setting:

```
ovconfchg -ovrg server -ns opc -set \
OPC_RESTRICT_ACTIONS_WITH_FOREIGN_SIGNATURE TRUE
```

In case there are more than just two servers in the MoM environment and you want to allow actions from agents belonging to these servers, set the following configuration setting:

```
ovconfchg -ovrg server -ns opc -set \
OPC_ACCEPT_ACTION_SIGNATURES_FROM <List_of_allowed_srv_COREIDs>
```

where <List_of_allowed_srv_COREIDs> is a comma-separated list of other servers’ CORE IDs.

NOTE This action restriction cannot be configured by using the `remactconf.xml` file because a trust relationship is established between servers through installed root certificates.

Message Text Pattern in Java GUI Message Filters

With the Java GUI version 8.24 and later, the `With Message Text Pattern` field in the `General` tab of the `Filter Messages` dialog box is limited to 254 characters. This is not yet documented in the *HPOM Java GUI Operator’s Guide* and the Java GUI online help.

Java GUI Client Version Control

The Java GUI Client Version Control feature enables the HPOM for UNIX administrator to specify required and recommended Java GUI versions by using server configuration variables. This means that only the Java GUI client version specified by the HPOM for UNIX administrator is allowed to connect to the HPOM for UNIX management server.

NOTE The Java GUI Client Version Control feature is supported with Java GUI client 8.26 and management server 8.27 patch levels. Its functionalities with Java GUI client patch levels lower than 8.26 are limited. With Java GUI client patch level 8.21 and lower, this feature is not working properly.

The following server configuration variables are used for specifying the Java GUI client version:

- `OPC_JGUI_MINIMAL_VER` for specifying the minimum required Java GUI client version.
- `OPC_JGUI_RECOMMENDED_VER` for specifying the recommended Java GUI client version.

Examples of specifying the Java GUI client version:

Example 1:

```
ovconfchg -ovrg server -ns opc -set OPC_JGUI_MINIMAL_VER A.08.27
```

Java GUI clients with versions lower than A.08.27 are not allowed to connect to the management server.

Example 2:

```
ovconfchg -ovrg server -ns opc -set OPC_JGUI_RECOMMENDED_VER A.08.29
```

The recommended Java GUI client version specified by the administrator is A.08.29, but Java GUI clients with versions lower than the specified one can connect to the management server.

NOTE If you combine Example 2 with Example 1, that is if the recommended Java GUI client version is A.08.29 and the minimum required Java GUI client version is A.08.27 (both specified by the administrator), the A.08.27 Java GUI client can connect to the management server. Only a warning message is displayed, which alerts the operator that the recommended version for the management server is A.08.29.

On the other hand, the A.08.26 Java GUI client cannot connect to the management server.

Example 3:

```
ovconfchg -ovrg server -ns opc -set OPC_JGUI_MINIMAL_VER A.08.27,A.08.26.QXCR1000xxxxxx
```

Internal version awareness:
With the exception of A.08.26.QXCR1000xxxxxx, Java GUI clients with versions lower than A.08.27 are not allowed to connect to the management server.

NOTE The `listguis` command line interface has been extended to show the Java GUI client version as well.

HPOM Security Advisory: Protecting HPOM for UNIX Components

The *HPOM Security Advisory Guide*, chapter "Protecting HPOM for UNIX Components" does yet not contain the following information about securing the management server:

HTTPS-based HPOM Server-to-Server Communication

HPOM for UNIX uses HTTPS-based communication for forwarding events to other HPOM for UNIX management servers. The HTTPS protocol establishes a higher level of security for the communication between management servers. HTTPS-based message forwarding between management servers is enabled by default.

To successfully use HTTPS-based forwarding, a trust relationship must be established between all HPOM management servers that communicate with each other. For more information about setting up trust relationships, refer to the *HPOM HTTPS Agent Concepts and Configuration Guide*.

Securing the Java GUI

The *HPOM Security Advisory Guide*, chapter "Protecting HPOM for UNIX Components" does yet not contain the following information about securing the Java GUI:

Changing the Default Port of opcuiwww

Vulnerability	The default port number (2531) of the `opcuiwww` process is known and might therefore be a target of attack.
Impact	If `opcuiwww` is attacked through the default port, the system may stop responding.
Relevance	Medium
Risk Level	Medium

Solution	The configuration setting `OPCUIWWW_PORT` holds the `opcuiwww` port number as defined in `/etc/services` (`ito-e-gui` entry). It is used by `opcuihttps` to start `opcuiwww` processes. It is recommended to change the default port 2531 to another port: **`ovconfchg -ovrg server -ns opc.opcuihttps -set OPCUIWWW_PORT <new port>`** You can also use the `ovprotect` utility to change the default port. For more information about configuration variables for the management server, refer to the *HPOM Server Configuration Variables* guide.

Changing the Default Port of opcuihttps

Vulnerability	The default port number (35211) of the `opcuihttps` process is known and might therefore be a target of attack.
Impact	If `opcuihttps` is attacked through the default port, the system may stop responding.
Relevance	Medium
Risk Level	Medium
Solution	The default port number on which `opcuihttps` listens for incoming HTTPS connections from Java GUI clients is 35211. It is recommended to change the default port 35211 to another port: **`ovconfchg -ovrg server -ns opc.opcuihttps -set SERVER_PORT <new port>`** For more information about configuration variables for the management server, see the *HPOM Server Configuration Variables* guide.

Providing Certificates for Full Authentication Mode

Vulnerability	The `opcuihttps` server accepts anonymous connections from clients by default. Clients are usually HTTPS-based Java GUI consoles, but can also be web browsers.
Impact	If `opcuihttps` is attacked through anonymous connections, the system may stop responding.
Relevance	Medium
Risk Level	Medium

Solution	If `SSL_CLIENT_VERIFICATION_MODE` is set to `RequireCertificate`, clients require the certificate for (full) authentication. To provide the certificates for the full authentication mode, perform the following steps: 1. Enable full authentication mode for `opcuihttps`: a. Configure `opcuihttps`: **`ovconfchg -ovrg server -ns opc.opcuihttps -set SSL_CLIENT_VERIFICATION_MODE RequireCertificate`** b. Restart the `opcuihttps` process. For more information about configuring opcuihttps parameters, refer to the *HPOM Administrator's Reference*. 2. Ensure that the client certificate is installed on the client system. If an HP Operations agent is installed on the Java GUI client system, you can use its client certificate for authentication. If no agent is installed, install the client certificate manually as described in the *HPOM Java GUI Operator's Guide*. 3. Set the Java GUI startup parameter `lcore_defaults` to `yes`, so that Java GUI uses the default Core functionality. The Core functionality is installed with the HP Operations agent if it exists on the Java GUI client. If no agent is installed, install the Core functionality manually as described in the *HPOM Java GUI Operator's Guide*. For more information about configuration variables for the management server, refer to the *HPOM Server Configuration Variables* guide.

Protecting the Java GUI against Denial of Service Attacks

Denial of Service (DoS) functionality provides protection against attacks to the `opcuiwww` process. The protection includes:

- Limitation of the number of connections to the Java GUI
- Limitation of the number of connections from one system
- Limitation of input buffer size
- Time out of input stream inactivity before the first request is served

Vulnerability	Multiple Java GUIs may open too many sockets to `opcuiwww` and keep them open.

Impact	Such attack or situation may occupy all available memory after some time and the system may stop responding.
Relevance	Medium
Risk Level	Medium
Solution	1. Enable basic DoS protection for the `opcuiwww` process. Set the `DOS_ENABLED` configuration variable to `TRUE`: **`ovconfchg -ovrg server -ns opc -set DOS_ENABLED TRUE`** 2. *Optional.* Configure the following DoS settings according to your security needs: a. Set the size of the input buffer on the `opcuiwww` socket. If the size exceeds the buffer limit, an error is reported to `System.txt`, and the connection (the `opcuiwww` process) is closed. The default value is 4096. Example: **`ovconfchg -ovrg server -ns opc -set OPCUIWWW_INPUT_BUFFER_LIMIT 512`** b. Set the maximum number of simultaneous connections to `opcuiwww` (Java GUIs). The default value is 100. Example: **`ovconfchg -ovrg server -ns opc -set OPCUIWWW_MAX_CONNECTION 5`** c. Set the number of connections to `opcuiwww` from a single system. The default value is 30. Example: **`ovconfchg -ovrg server -ns opc -set OPCUIWWW_ONE_CONNECTION 2`** d. Set the time out for inactivity on the `opcuiwww` socket. A valid request must arrive at the socket within the specified time (measured from the initial connection), otherwise `opcuiwww` logs an error and exits. The default value is 5 (seconds). Example: **`ovconfchg -ovrg server -ns opc -set OPCUIWWW_TIMEOUT 3`** For more information about configuration variables for the management server, refer to the *HPOM Server Configuration Variables* guide.

Restricting the Number of Simultaneous Connections to opcuihttps

Vulnerability	Multiple Java GUIs may open too many sockets to `opcuihttps` and keep them open.
Impact	Such attack or situation may occupy all available memory after some time and the system may stop responding.
Relevance	Medium
Risk Level	Medium
Solution	Limit the maximum number of simultaneous connections to `opcuihttps`. Clients are usually HTTPS-based Java GUI consoles, but can also be web browsers. The default value is 100. Example: **`ovconfchg -ovrg server -ns opc.opcuihttps -set MAX_CONNECTIONS 10`** For more information about configuration variables for the management server, refer to the *HPOM Server Configuration Variables* guide.

Installing HPOM for UNIX on HP-UX PA-RISC 11.31 and HP-UX Itanium 11.31

HP-UX PA-RISC 11. 31 and HP-UX Itanium 11.31 platforms are supported with the following HPOM for UNIX configuration:

- HPOM for UNIX management server patch level 8.25 or higher
- Oracle 10gR2 (patch level 10.2.0.2 or newer)
- HPOM for UNIX HTTPS agent patch level 8.17 or higher
- NNM 7.53

HPOM Dependencies

Before installing HPOM, make sure that the `libil.2` library is on the system. To check whether the `libil.2` library is on the system, run the following command:

```
# swlist -l file | grep libil.2
```

If it is on the system, the command returns the following:

```
ImagingSubsystem.IMAGE-SHLIBS: /opt/image/lib/libil.2
ImagingSubsystem.IMAGE-SHLIBS: /usr/lib/libil.2
```

NOTE Make sure that the `ImagingSubsystem` product is also installed on the system before you install HPOM.

In addition, the following links must be created manually on the HP-UX 11.31 Itanium platform:

```
ln -s /opt/image/lib/hpux32/libil.so.1 /usr/lib/hpux32/libil.so.1
```

```
ln -s /opt/image/lib/hpux32/libilefs.so.1 /usr/lib/hpux32/libilefs.so.1
```

You cannot run HPOM without the CDE and the `ImagingSubsystem` product because HPOM requires runtime libraries that come with these products. In case these shared libraries are missing, the Motif GUI will not work.

For the HPOM Motif GUIs to work, at least the following SD products, which contain the necessary libraries, are required:

```
ImagingSubsystem.IMAGE-SHLIB-IA B.11.31 ImagingSubsystem
ImagingSubsystem.IMAGE-SHLIBS B.11.31 ImagingSubsystem
CDE.CDE-SHLIBS B.11.31 CDE Shared Libraries
CDE.CDE-SHLIBS-IA B.11.31 CDE IA Native Shared Libraries
```

In addition, if you want to use `dtterm` (for example, for the agent installation), you must install the following filesets:

```
CDE.CDE-DTTERM B.11.31 CDE Terminal Emulator
CDE.CDE-DTTERM-COM B.11.31 CDE Terminal Emulator
```

To use the online help in the Motif GUIs, you also need the following filesets:

```
CDE.CDE-HELP-RUN B.11.31 CDE Help Runtime
CDE.CDE-HLP-RUN-CM B.11.31 CDE Help Runtime
CDE.CDE-MIN B.11.31 CDE Minimum Runtime
CDE.CDE-MIN-COM B.11.31 CDE Minimum Runtime
CDE.CDE-TT B.11.31 CDE Messaging
```

Additional Installation Instructions

In case you want to use the embedded installation (`ovoinstall` automatically installs NNM, and then the HPOM server), follow these steps:

1. Log in as `root`.
2. Make sure the proper directory structure is at the depot location. This structure is as follows:

   `./OVNNMCD1 (NNM disk1)`

   `./OVNNMCD2 (NNM disk2)`

   `./OVNNMCD3 (NNM 7.53 upgrade disk)`

   `./OVOCD1`

   `./OVOCD2`
3. To copy the new `ovoinstall` script and `OVO.info.HP-UX.B.11.31.txt` into the depot, run the following commands:
   #cp <new_ovoinstall_dir>/ovoinstall <depot_dir>/OVOCD1/

```
#cp <new_ovoinstall_dir>/OVO.info.HP-UX.B.11.31.txt \
<depot_dir>/OVOCD1/Required_OS_Patch_Lists/
```

4. To run `ovoinstall`, type the following commands:
   ```
   #cd <depot_dir>/OVOCD1
   ```
   ```
   #./ovoinstall
   ```
5. Follow the installation procedure.

Upgrading Operating System with Existing HPOM for UNIX Installation

You can also upgrade the operating system of the HPOM for UNIX management server from HP-UX 11.23 to HP-UX 11.31 and keep the existing installation of HPOM for UNIX.

Synchronization of Configuration Data from One HPOM for UNIX Server to Another

To use HTTPS-based communication for the transfer, the following prerequisite must be met:

- ❏ The source HPOM for UNIX management server must be set up as an action-allowed manager on the target HPOM for UNIX server.

To allow synchronization of configuration data from one HPOM for UNIX server to another by using HTTPS-based communication, you must perform the following steps:

1. Create the appropriate configuration download information by running the `opccfgdwnld` CLI on the source HPOM for UNIX server.
2. Run the following commands on the source HPOM for UNIX server:
   ```
   #!/usr/bin/sh
   PATH=$PATH:/opt/OV/bin/OpC/install
   tar cvf - /var/opt/OV/share/tmp/OpC_appl/cfgdwn | gzip > /tmp/cfgdwn.tar.gz
   opcdeploy -deploy -file /tmp/cfgdwn.tar.gz -node mgmtsv2 -targetdir /tmp -trd absolute
   opcdeploy -cmd "rm -rf /var/opt/OV/share/tmp/OpC_appl/cfgdwn" -node mgmtsv2
   opcdeploy -cmd "gunzip < /tmp/cfgdwn.tar.gz| tar xvf - 2>&1" -node mgmtsv2
   ```
3. Upload the configuration on the target HPOM for UNIX server by running the `opccfgupld` CLI at a convenient time (for example, the planned maintenance window of the targeted HPOM for UNIX server).

Motif UI SSH-Based Virtual Terminal

The Secure Shell application type enables users to initiate secure terminal connections using an HPOM application. Users still cannot perform passwordless login (for example, using stored passwords) unless certain openssh features are used. However, you can define a user name with which a connection will be performed.

As a prerequisite, an ssh client must be installed on the management server and an ssh server must be installed on the target managed node.

Command Line Utility opcownmsg

A new utility has been introduced on the HPOM for UNIX Management Server. The command `opcownmsg` is used for setting, unsetting, and changing HPOM messages ownership. The utility can only be used by a superuser. For more information, see the `opcownmsg` man page.

New Java GUI Enhancements

The following HPOM for UNIX Java GUI enhancements are not documented, yet.

Save Service Graph Layout Feature

The service graph layout with the exception of the Root Cause and Impact Static Service graphs is now saved according to the operator's arrangement of the services. The saved information includes the position of the services and the expanded status of the services.

There are the two types of layout, the auto layout, which is the default layout, and the custom layout. A new toggle button is introduced, which allows you to switch between auto and custom layout on a currently selected service graph. If it is ON, the custom layout is enabled. If it is OFF, the auto layout is enabled.

Custom File Name for Configuration File

The `ito_op.bat` Java GUI startup script has been enhanced to accept a configuration file name and location for loading and saving Java GUI layout configuration as a command line option, for example

```
ito_op.bat -config=<path/filename>
```

Verify Java Client Console Version Using CLI

A new version parameter has been added to the `ito_op.bat` Java GUI startup script, enabling you to verify the Java Client console version without starting the Java GUI and checking by clicking Help -> About.

HTML Application Output as an Internal Webpage

Java GUI now supports application HTML output as an internal webpage. The output is controlled through the `web_browser_html_appl_result` parameter in `itooprc`.

To enable, use the following command:

```
ovconfchg -ovrg server -ns opc -set OPC_JGUI_WEBBRW_APPL_RESULT TRUE
```

To disable, use one of the following commands:

```
ovconfchg -ovrg server -ns opc -set OPC_JGUI_WEBBRW_APPL_RESULT FALSE
ovconfchg -ovrg server -ns opc -clear OPC_JGUI_WEBBRW_APPL_RESULT
```

Internet Explorer 7 Support for Java GUI Applet

A new launch HTML page for the Java GUI is provided to replace `ito_for_activator.html` which cannot be used with Microsoft Internet Explorer 7:

`http://<server>:3443/ITO_OP/ito_op_applet.html`

Java GUI Startup Options

Additional `ito_op` startup options for starting the HPOM for UNIX Java GUI in a custom state are available. These startup options can be used, for example, for CGI-Perl integration when running the Java GUI as an applet in a browser. Using CGI-Perl scripts, you can start the HPOM for UNIX Java GUI applet with custom parameters passed in the URL and open the GUI in a custom layout.

A CGI script that processes startup parameters is available at the following location:

`http://<server>:3443/Cgi-bin/ito_op_applet_cgi.ovpl`

A link to the script including examples for its usage are available at the following location:

`http://<server>:3443/ITO_OP`

For more information on starting the Java GUI with `ito_op` options, refer to the *About the ito_op Startup options* section of the HPOM Java GUI Operator's Guide.

Table 4-1 New attributes that control the layout and content of the Java GUI

Name	Value	Default	Overrides	Info
gui.dftllayout	boolean	false		Controls the base layout. See [a] for more details.
gui.objectpane	boolean			Show or hide Object Pane
gui.shortcutbar	boolean			Show or hide Shortcut Bar
gui.workspace	<name>	Default names as generated for new workspaces.		Create new workspaces
gui.msgbrw.type	active | history | pending	active		Opens a browser with active, history, or pending messages
gui.msgbrw.workspace	<name>	Default – first - workspace		Opens a browser in specified workspace.
gui.msgbrw.brwpane	<boolean>		gui.msgbrw.workspace	Opens a browser in browser pane
gui.msgbrw.filter.name	<name>		gui.msgbrw.filter.<ANY>	A saved filter name overrides all filter attribute values

Table 4-1 New attributes that control the layout and content of the Java GUI

Name	Value	Default	Overrides	Info
gui.msgbrw.filter .nodes	<name_list>			
gui.msgbrw.filter .services	<name_list>			
gui.msgbrw.filter .apps	<name_list>			
gui.msgbrw.filter .msggrps	<name_list>			
gui.msgbrw.filter .objects	<name_list>			
gui.msgbrw.filter .msgtext	<string>			
gui.msgbrw.filter .time.start	<date/time>	today 0:00:00		date / time format as specified by the system locale setting
gui.msgbrw.filter .time.end	<date/time>	today 23:59:59		date / time format as specified by the system locale setting
gui.msgbrw.filter .time.relative.start	<string>			the relative time syntax [+|-]<int>[d|h|m|s]
gui.msgbrw.filter .time.relative.end	<string>			the relative time syntax [+|-]<int>[d|h|m|s]
gui.msgbrw.filter .owned	not | me | others			
gui.msgbrw.filter .severity	<severity_list> enum {unknown, normal, warning minor, major, critical}			

Table 4-1 New attributes that control the layout and content of the Java GUI

Name	Value	Default	Overrides	Info
gui.svcgraph.name	<service_name>	top level service		All services assigned to operator.
gui.svcgraph.calcid	<calc_id> (0 | 1)	0		service status calculation id
gui.svcgraph.workspace	<name>	Default (first) workspace		opens a graph in specified workspace.
gui.svcmap.name	<service_name>	top level service		All services assigned to operator
gui.svcmap.calcid	<calc_id> (0 | 1)	0		service status calculation id
gui.svcmap.workspace	<name>	Default (first) workspace		opens a map in specified workspace.

a. The attribute controls the base layout of the JGUI on which the new objects, controlled by other attributes will be added. If set to:

- false (default): layout is blank. Additionally, if the message browser is opened on the browser pane, it will take 100% of the GUI (the horizontal splitter, dividing the workspace pane and browser pane will be on the top-most position). If also a service graph is opened in the workspace, then the GUI is spitted 50:50 between the workspace and browser pane.
- true: JGUI is opened as today: if session settings are found they are used, otherwise the defaults are used.

Introduction of R Flag for Read-Only Messages in Java UI Message Browser

HPOM for UNIX distinguishes between two subtypes of read-only messages:

- Notification

  In MoM environments, a message can be forwarded to or from management servers as a notification (as opposed to a controlled message)

- Read-Only

  Messages, that would normally not be shown to the operator because of their responsibility matrix settings if the service attribute of the message is a service that is assigned to that operator. The `OPCUIWWW_NORESP_SVCMSG` configuration variable on the management server must be set to `READONLY`.

HPOM for UNIX Java UI now also distinguishes between these two different read-only message types by setting the `S` flag to:

- N for NOTIFICATION messages (these messages can be (un)acknowledged and annotations can be added)
- R when message is operator level READ-ONLY (no operations are allowed on these messages)

Full Support for INFORM Own Mode in Java UI

The concept of ownership, as set by the HPOM for UNIX administrator by selecting one of the default ownership modes, 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`. Informational mode does not restrict or alter operations on the message.

Java GUI Time Zone Adjustments

Java GUI always uses the time zone of the local client. If the Java GUI runs in a time zone different from the mgmt sv time zone, the messages display a different time. You can force the Java GUI to use a specified time zone by editing the ito_op.bat script for Windows clients.

Time Zone Settings in ito_op.bat

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

For example, to use the Australia/Sydney time zone, add the text `-Duser.timezone=Australia/Sydney` to the `ito_op.bat` file (example extract):

```
:: Starting JavaGUI
for %%p in (true TRUE on ON yes YES) do if "%%p"=="%TRACE%" echo on
for %%p in (true TRUE on ON yes YES) do if "%%p"=="%PLUGIN%" goto :PLUGIN
%START% .\j2re1.4.2\bin\%JAVA% -Duser.timezone=Australia/Sydney -Xmx128m
com.hp.ov.it.ui.OvEmbApplet initial_node=%ITOSERVER% user=%USER% passwd=%PASSWD%
trace=%TRACE%
display=%DISPLAY% locale=%LOCALE% max_limited_messages=%MAX_LIMITED_MESSAGES%
refresh_interval=%
REFRESH_INTERVAL% apiport=%APIPORT% apisid=%APISID% https=%HTTPS% %BBCPARM%
goto END
```

Valid time zones are listed in the <JRE_HOME>\lib\zi directory, for example GMT, Asia/Singapore, or Europe/Warsaw. If you specify an invalid time zone, GMT is used.

Passing the Time Zone Information to the JAVA Web Client for HPOM

To pass the time zone information to the Java web client for HPOM, add user.timezone as a property to the resources group of /opt/OV/www/htdocs/ito_op /ito_op_ws.jnlp.

Customized Message Group Icons

Previously, the message groups icon with certain severity colors was hard to distinguish from the message group icon itself. Message group icons can now be customized through the OPC_JGUI_MSGGRP_ICON server-side variable in one of the following ways:

- the default icon can be set to be displayed in black and white:
  OPC_JGUI_MSGGRP_ICON=BW
- a custom image can be loaded (in the second example the image will be loaded from default HPOM image path /opt/OV/www/htdocs/ito_op/images):
  OPC_JGUI_MSGGRP_ICON=http://<server>:3443/ITO_OP/images/juke.32.gif
  OPC_JGUI_MSGGRP_ICON=africa.32.gif
- an empty image can be loaded, so only the severity color is visible:
  OPC_JGUI_MSGGRP_ICON=nonexisting_image

Java GUI Connection Port Setting

Beside setting the port for non-secure socket communication by using the itooprc file or directly editing the ito_op startup script, you can now also specify the port number as a parameter of the ito_op startup script or as part of the server name, passed as the parameter to the ito_op startup script or in the login dialog.

The port number can thus be set in one of the following ways:

- in itooprc: **port=*<port_number>***
- with **ito_op ... -port *<port_number>* ...**
- with **ito_op hostname:*<port_number>* ...** or **ito_op ... -server hostname:*<port_number>* ...**
- at login dialog in the management server field: **hostname:*<port_number>***
- in ito_for_activator.html: add **<PARAM NAME = port VALUE = port_number">**

Improved Cluster Error Handling and Logging

- When the HARG start, stop or monitor script returns an error and the HARG tracing was not switched on, it was extremely difficult to find out why the HARG script failed since the errors from these scripts were not logged anywhere.

  Errors from failed HARG scripts are now logged into the /var/opt/OV/hacluster/<HARG>/error.log file.
- HARG trace.log file size is limited. When the maximum file size is reached, trace.log is moved into trace.log.old and new information is written into a new trace.log file.

Max size of trace.log file can be changed by editing the following file:

`/var/opt/OV/hacluster/<HARG name>/settings`

and adding the following line:

`TRACING_FILE_MAX_SIZE=<maximum size in kBytes>`

Below is an example with a maximum size of7MB:

`TRACING_FILE_MAX_SIZE=7000`

NNM 7.51 and NNM 7.53 CD-ROM/DVD-ROM Installation Important Update

The NNM 7.5x media kit use a new format that is somewhat different from older formats.

As a result, HP UX 11.11 systems require a system patch to read the media kit properly. The media kits may appear to mount correctly on an unpatched HP UX 11.11 system. However, software installation will fail, because the system can not find certain files on the media kit.

Note that the issue is in reading the media kit, not in the NNM installation process. Therefore the solution is to patch the system where the media kit will be mounted, which is not necessarily where NNM is to be installed.

Visit `http://itrc.hp.com` and follow the "`patch database`" link to download the appropriate patches for your system.

HP-UX 11.11 Prerequisites

PHKL_28025 - s700_800 11.11 Rock Ridge extension for ISO-9660

Other Dependencies:

PHCO_25841 - s700_800 11.11 Add Rock Ridge extension to mount_cdfs(1M)

PHKL_26269 - s700_800 11.11 Rock Ridge extension for ISO-9660

Installation

Apply the patches on the system where the media kit will be mounted as follows:

1. Unpack the patch using this command:

   `sh <patchname>`

2. Apply the patch using this command:

   `swinstall -s <patchname>.depot`

NOTE This patch requires a system reboot.

IMPORTANT Long file names may be truncated when NNM media kits are mounted using the mount command as documented in the NNM CD/DVD insert and the *HP NNM Software Quick Start Guide*.

Use the following mount command with the Rock Ridge extension:

`mount -F cdfs -o rr,ro,cdcase <cd device> <mount destination>`

IMPORTANT NNM 7.53 installation may fail due to missing `libovextfmt.so` library. To solve this problem, before installing NNM, manually create symbolic link to the missing library:

```
ln -s /opt/OV/lib/hpux32/libovextfmt.so /opt/OV/lib/libovextfmt.so
```

Proceed with software installation as usual, according to the *HP NNM Software Release Notes* and *HP NNM Software Quick Start Guide*.

Upgrading to Oracle 10g Release 2

This section describes how to upgrade Oracle 9.2.0.6 or Oracle 10.1.0.4 to version 10.2.0.1 (Release 2). After 10.2.0.1 (Release 2), 10.2.0.2 patch level is required. For more detailed information see the O*racle Database Upgrade Guide 10g*.

The steps needed for a first-time installation of Oracle 10g are provided in the HPOM Installation Guide for the Management Server.

NOTE After you have started up your database with ORACLE_HOME containing the new Oracle software, do not attempt to go back to the old version, as this could result in database files being corrupted.

NOTE For the 10.2.0.2 or later Oracle patch set it is important to perform the optional step to run the changePerm.sh script as documented in the patch set readme to set the permissions correctly. Otherwise non-root users won't be able to start the Motif GUI.

Check the System Requirements

Make sure your system meets the requirements stated in the Oracle documentation. There might be a difference between Oracle 10g Release 1 and Oracle 10g Release 2 required OS patches and kernel parameters.

Prepare the Database for the Upgrade

Before upgrading the Oracle software, perform the following steps:

1. Exit the HPOM GUIs (motif and java) and stop the HP processes with **`ovstop -c`** and **`ovc -kill`**.
2. Stop all processes that access the Oracle database.
3. Shut down the database and, if necessary, the SQL*Net listener, as follows:
   a. Log in as user oracle or switch to user oracle:

      ```
      su - oracle
      ```

   b. If you are using SQL*Net, shut down the SQL*Net listener using the following command:

      ```
      $ORACLE_HOME/bin/lsnrctl stop
      ```

   c. Start the Oracle SQL*Plus tool and shut down the database as follows:

      ```
      $ORACLE_HOME/bin/sqlplus /nolog
      SQL> connect / as SYSDBA
      SQL> shutdown
      SQL> exit
      ```

4. Perform a full offline backup of the Oracle database or the complete system before you perform the upgrade. A full backup ensures that you can recover from errors encountered during the upgrade process.

Installation of Oracle 10.2.0.1 (Oracle 10g Release 2)

Perform the following steps to install Oracle Database 10.2.0.1 (Release 2) software:

1. *If you are upgrading from Oracle 10g Release 1*:

   Since user `oracle`, `oinstall` (primary) and `dba` (secondary) groups were already created as prerequisites for the Oracle 10.1.0.4 installation, there is no need to create them again.

   If you are upgrading from Oracle 9:

   Modify the user `oracle` with the following attributes:

   a. Create a UNIX group named `oinstall`. The group ID should be greater than 100.

   b. Make the user `oracle` a member of the group `oinstall` as the primary group, and `dba` as the secondary group.

   Set umask to allow users to access the Oracle binaries:

   ```
   umask 022
   ```

2. Create the Oracle home directory `ORACLE_HOME`:

   ```
   mkdir /opt/oracle/product/10.2.0
   ```

   You can also choose a different directory for `ORACLE_HOME` but you must use it consistently in all subsequent steps.

3. Change the ownership of the directories to `oracle:oinstall` by entering:

   ```
   chown -R oracle:oinstall /opt/oracle/product/10.2.0
   ```

4. Change the following Oracle environment variables in the `/home/oracle/.profile` of user `oracle`:

   ```
   export ORACLE_HOME=$ORACLE_BASE/product/10.2.0
   ```

This variable determines the location and the version of the Oracle installation. This is the recommended setting. You can choose a different setting, if needed.

5. As user `oracle`, start the Oracle Universal Installer.
6. After the Oracle Universal Installer is started, follow the instructions for installing the Oracle Database software provided by Oracle. After exiting the Oracle Universal Installer, run the Oracle Database Upgrade Assistant to upgrade the database software.

Configuring HP BTO Software Products to Use the New Oracle Version

Perform the following steps as user `oracle`:

1. Since the upgrade of Oracle database was done by Oracle Database Upgrade Assistant, there is no need to manually move the parameter file of the `ORACLE_SID` database instance to the new location. This is usually a symbolic link to `/opt/oracle/admin/<ORACLE_SID>/pfile/init<ORACLE_SID>.ora`.
2. Copy the SQL*Net files from the old `ORACLE_HOME` to the new location, for example:

```
cd  /opt/oracle/product/9.2.0/network/admin/
cp listener.ora /opt/oracle/product/10.2.0/network/admin/listener.ora
cp tnsnames.ora /opt/oracle/product/10.2.0/network/admin/tnsnames.ora
cp sqlnet.ora /opt/oracle/product/10.2.0/network/admin/sqlnet.ora
cp tnsnav.ora /opt/oracle/product/10.2.0/network/admin/tnsnav.ora
```

3. As user root, replace all occurrences of the old `ORACLE_HOME` value with the new value in the following files. You have to change variable assignments as well as directory names containing this value. Replace the following:

   -`ORACLE_HOME` in `/etc/opt/OV/share/conf/ovdbconf`
   -`DB_RELEASE` in `/etc/opt/OV/share/conf/ovdbconf`
   -`ORACLE_HOME` in `/opt/oracle/product/10.2.0/network/admin/listener.ora`
   -`LOG_DIRECTORY_LISTENER` in `/opt/oracle/product/10.2.0/network/admin/listener.ora`
   -`TRACE_DIRECTORY_CLIENT` in `/opt/oracle/product/10.2.0/network/log/sqlnet.ora`
   -`LOG_DIRECTORY_CLIENT` in `/opt/oracle/product/10.2.0/network/log/sqlnet.ora`
   -`ORA_CRS_HOME` in `/sbin/init.d/init.cssd`

4. Change the symbolic links used by HP Operations Manager. Change the following symbolic links:

   `libclntsh.so, libclntsh.so.1.0, libclntsh.so.8.0, libclntsh.so.9.0, libclntsh.so.10.1, libopcora.so`

   These point to the Oracle shared libraries. Remove them and recreate new links that point to the Oracle shared libraries in the new `ORACLE_HOME`, for example:

```
ln –s /opt/oracle/product/10.2.0/lib32/hpux32/libclntsh.so libclntsh.so
ln –s /opt/oracle/product/10.2.0/lib32/hpux32/libclntsh.so libclntsh.so.1.0
ln –s /opt/oracle/product/10.2.0/lib32/hpux32/libclntsh.so libclntsh.so.8.0
ln –s /opt/oracle/product/10.2.0/lib32/hpux32/libclntsh.so libclntsh.so.9.0
ln –s /opt/oracle/product/10.2.0/lib32/hpux32/libclntsh.so libclntsh.so.10.1
ln –s /opt/oracle/product/10.2.0/lib32/hpux32/libclntsh.so libopcora.so
```

5. To find the missing files and to avoid starting the database with the wrong `ORACLE_HOME` value, it is recommended you rename the old `ORACLE_HOME` directory.
6. Start the database and the SQL*Net listener as follows:
   a. Log in as user oracle or switch to user oracle.
   b. If you are using SQL*Net, start up the SQL*Net listener:

```
$ORACLE_HOME/bin/lsnrctl start
```

c. Start the Oracle SQL*Plus tool and start the database, for example:

```
$ORACLE_HOME/bin/sqlplus /nolog
SQL> connect / as SYSDBA
SQL> startup
SQL> exit
```

7. If you no longer need the old Oracle version and after you verified that the new Oracle version works, you can remove the old Oracle version to gain disk space.
8. You can start the HPOM for UNIX Management Server and other HP component processes.

Assessing Your System Vulnerability with ovprotect

HPOM for UNIX provides a new utility, called `ovprotect`, that helps you to determine and minimize the vulnerability risks of your systems from the HP Operations Manager perspective. It tests and disables unused services on the HPOM for UNIX management server or on the HPOM HTTPS agent platforms. In addition, it checks local file permissions, and can perform some corrective actions on the local systems.

The `ovprotect` tool is modular. More extensions, as well as modules for other HP BTO software products, are expected to be released on a regular basis. You can always download the latest version of the `ovprotect` tool from the HPOM for UNIX web site:

`ftp://ovweb.external.hp.com/pub/ovprotect`

For details and usage options, refer to the ovprotect(1m) man page and the HPOM Security Advisory Guide.

Message Counter Feature: Severity and Message Text Updates

When suppressing/counting duplicate messages, the severity and the message text of the message that has first arrived to the browser was retained. When the new incoming HPOM message has a different severity or message text, these new values can be displayed instead of the previous data.

Two new variables have been introduced to facilitate updating message text and severity:

`OPC_UPDATE_DUPLICATED_SEVERITY`

`OPC_UPDATE_DUPLICATED_MSGTEXT`

If these variables are set to `LAST_MESSAGE`, the appropriate value will be changed in the browser.

To test these two variables, use the following commands:

```
ovconfchg -ovrg server -ns opc -set OPC_UPDATE_DUPLICATED_SEVERITY LAST_MESSAGE
ovconfchg -ovrg server -ns opc -set OPC_UPDATE_DUPLICATED_MSGTEXT LAST_MESSAGE
```

If you prefer the current behavior (no update of severity and message text fields), do not set these two variables or set them explicitly to `FIRST_MESSAGE` using the following commands:

```
ovconfchg -ovrg server -ns opc -set OPC_UPDATE_DUPLICATED_SEVERITY FIRST_MESSAGE
```

```
ovconfchg -ovrg server -ns opc -set OPC_UPDATE_DUPLICATED_MSGTEXT FIRST_MESSAGE
```

Installing HPOM for UNIX on VERITAS Cluster Server 4.1 on HP-UX 11.23 Itanium

During the HPOM Management Server installation, the `ov-server` HA resource group is not started. To start the HPOM Management Server as an HA resource group manually, execute the following commands immediately after the installation:

```
/opt/OV/bin/ovharg_config ov-server -add_node <local hostname>
```

```
/opt/OV/bin/ovharg_config ov-server -start <local hostname>
```

Command Line Utilities opcinstrumdwn and opcpkgdwn

Two new utilities have been introduced on the HPOM for UNIX Management Server:

- `opcpkgdwn` is an HPOM for UNIX Management Server utility that copies all software packages together which are needed to install an HPOM HTTPS agent.

  Utility location: `/opt/OV/bin/OpC/opcpkgdwn`

- `opcinstrumdwn` is an HPOM for UNIX Management Server utility that copies all instrumentation files together which would be deployed to an HPOM HTTPS agent.

  Utility location: `/opt/OV/bin/OpC/opcinstrumdwn`

These tools are helpful for generating the generic HTTPS agent packages, which allow you easy mass deployments. For further details refer to the *HTTPS Agent Clone Imaging* whitepaper available for download from the following website:

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

opcdelmsg Troubleshooting Utility

`opcdelmsg` utility removes a single message out of the HPOM database without accessing the database directly.

The following is the `opcdelmsg` syntax:

```
opcdelmsg [ -help ] | [-o] [ -u <user_name> ] <msg_id> [<msg_id>...]
```

Where `msg_id` (message id) is used for message identification.

See `opcdelmsg` man page for more details on this utility.

dtterm Default for Agent Installation

`hpterm` is replaced with `dtterm` as the default terminal for the installation of the HPOM Agent. However, if you prefer to use `hpterm`, you can change the default installation window to `hpterm` using the following command:

```
# ovconfchg -ovrg server -ns opc -set OPC_TERMINAL /usr/bin/X11/hpterm
```

For more information about the default window for the agent installation, refer to the README file provided with the 8.21 server patch.

Message Attribute Synchronization between HPOM Management Servers in MoM Environments

Changes of HPOM message attributes, for example message severity, message text, and custom message attributes can be synchronized with other HPOM management servers.

Separating Message Fields with Tabs

With Java GUI 7.20 and later, when copying one or more messages using `Ctrl+C` and `Ctrl+V` commands, message fields were separated using a space as a separator, which commonly happens with `Edit -> Copy to clipboard` functionality.

The old functionality is restored, where the fields of the message are separated with tabs. This makes possible organizing messages into Excel spreadsheets, where each field of each message is a separate column in the row.

New Configuration Variables for opcuiwww

It is no longer required for `opcuiwww` to query the database when a new active message arrives. Set the following configuration variables for `opcuiwww` to receive the complete messages:

```
OPCMSGM_USE_GUI_THREAD=NO_RPC
```

```
OPCUIWWW_NEW_MSG_NO_DB=TRUE
```

Command Line Utility opccfguser

A new utility has been introduced on the HPOM for UNIX Management Server. The command opccfguser configures HPOM for UNIX operators and is used for assigning user profiles, unassigning user profiles and configuring the responsibility matrix. For more information, see the `opccfguser` man page.

Changed Behavior of the Java GUI 'Lock' Feature

When viewing old messages in the Java GUI, the arrival of new messages may cause that the messages you are currently viewing become invisible in the message browser.

To make sure that the messages you currently work on remain visible in the message browser while new messages are arriving, you can disable an autoscroll feature by clicking the `Lock` checkbox placed at the bottom of message browser. For more information, refer to the HPOM Java GUI Operator's Guide.

According to the old behavior of this feature, disabling an autoscroll feature resulted also in not being able to see any changes to the messages in the browser while it is locked.

The message browser shows the changes in the messages that are already visible and the acknowledged messages disappear from the browser, while the new messages are still stopped from showing. Changing sorting, clicking on the column header, or moving scroll slider unlocks the message browser while scrolling inside the message browser with keys does not unlock it, which makes possible to navigate through messages while the message browser is locked.

Moreover, an appropriate information is displayed in a locked message browser' status bar to indicate its status.

Auditing for Service Navigator

The auditing for Service Navigator (`opcsvcm`) should be documented in the HPOM Administrator's Reference. In the "Table 12-1: Audit Areas of the Administrator Audit Level" on page 505, a new table row should be added with the following details:

Service Navigator

- ❏ Add, remove, replace operations
- ❏ Assign, deassign operations

NOTE HPOM creates an audit entry when the action is carried out in the Service Navigator (`opcsvcm`)

Interoperability with HPOM for Windows

HPOM Server to Server Forwarding

On page 207 of the HPOM Administrator's Reference, information about the new server-based message forwarding capabilities of HPOM for WINDOWS version 7.50 and higher is not available. To learn more about the improved interoperability with HPOM for WINDOWS, refer to the HPOM for WINDOWS 7.50 online help:

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

HTTPS Agent Support in Mixed HPOM for UNIX and HPOM for WINDOWS Environments

Because HPOM for UNIX and HPOM for WINDOWS support different kinds of the HTTPS agent, you should be aware of the use case restrictions summarized in the following table:

Table 4-2 HTTPS Agent Support in Mixed HPOM for UNIX and HPOM for WINDOWS Environments

HTTPS Agent HPOM Server	8.1x	8.50	8.51
HPOM for UNIX 8.2x (x<9)	✔	✔[1]	✔[1]
HPOM for UNIX 8.29+	✔	✔[1]	✔
HPOM for WINDOWS 8.0		✔	

[1]operational and policy deployment only: HPOM message sending to HPOM server, action launch, action response, policy deployment, and so on, but *not* HTTPS agent software installation

NOTE At least the HPOM for UNIX 8.29 server patch level is required to install the 8.51 HTTPS agent patches on the HPOM for UNIX server.

Problems with Database Startup After Oracle 10.2.0.2 Patch Installation

The following note should be added in the HPOM Installation Guide, in the "Installing an Oracle Database" section:

NOTE If you encounter problems with starting the database after the Oracle 10.2.0.2.0 patch installation, check the upgrade information in the 10.2.0.2 `patchnote.htm` file located on the Oracle patch depot (under `doc`). Additionally check the Oracle documentation.

Enhanced Auditing for the Java GUI

When logging into the HPOM Java GUI, multiple records are recorded in the audit report because the Java GUI uses three connections for each session. This makes the audit reports difficult to read and understand.

Auditing for the Java GUI has now been enhanced such that each connection from the Java GUI to the HPOM management server is clearly marked with the acronym `JUI`. In addition, the hostname of the Java GUI client, the process ID of the connected Java GUI console, and the session ID of the currently connecting Java GUI console are listed.

Disabling Data Collection for the Embedded Performance Component

You may want to disable metric collection for the embedded performance component if you have HP Performance Agent on the same node, since OVPA collects a superset of the metrics available through the embedded performance component data source.

With data collection disabled, the process `coda` continues to run and remains under HPOM control. It then acts as a data communication layer for OVPA.

To disable data collection for the embedded performance component on HTTPS-based managed nodes with OVPA 4.5 installed, use the following command:

```
ovconfchg -ns coda -set DISABLE_PROSPECTOR false
```

Set the parameter `DISABLE_PROSPECTOR` to true to enable data collection again.

SQL *Plus Missing for Independent Database Server Installation

In HPOM Installation Guide, in the “Setting Up an Independent Database-Server System” section, the following bullet should be added in the step 2 (Install the following Oracle products on the HPOM management server):

- SQL *Plus 9.2.0.2 or SQL *Plus 10g (10.1.0.2.0 or 10.2.0.1.0)

Missing ip_flags Field in the opc_node_names Table

In the *HP OVO Reporting and Database Schema* document (software versions 8.10 and 8.20), the "opc_node_names Table" in the chapter "Node Tables" is missing a row with the information for the `ip_flags` field.

The information for the `ip_flags` field is given in the following table extract:

Table 4-3 Missing ip_flags Field for opc_node_names Table

Column Name	Constraint	Column Type	Description
ip_flags	N	int2	This field contains the IP settings flag which determines whether a node is static or DHCP-derived. The possible values are: 0 None 1 IP obsolete 2 Static IP (not added if the IP address is set by DHCP) 16 IP received by agent 32 IP set on server 256 Alternate IP addresses available 512 Alternate IP names available 64 "On" if IPv6 is active

The actual value in the table is the sum of the values of the desired flags. For example:

- A value of 32 represents a DHCP node (32 for IP set on server).
- A value of 34 represents a static, non-DHCP node (32 for IP set on server plus 2 for static IP).

heartbeat_flag Description in opc_nodes Table

In the *HP OVO Reporting and Database Schema* document (software versions 8.10 and 8.20), the "opc_nodes Table" in the chapter "Node Tables" contains the following incorrect description for the `heartbeat_flag` field:

0...Heartbeat polling on
1...Heartbeat polling off

The correct description is given in the following table extract:

Column Name	Constraint	Column Type	Description
heartbeat_flag	N	number(3)	Switches heartbeat polling on or off. Possible values are: 1 Heartbeat polling on 0 Heartbeat polling off

comm_type HTTPS Option in opc_comm_type and opc_nodes Tables

In the *HP OVO Reporting and Database Schema* document, the sections “opc_comm_type Table” and “opc_nodes Table” in the chapter “Node Tables” do not contain a value for the communication type HTTPS.

The following table extract contains the complete list for both tables:

Column Name	Constraint	Column Type	Description
comm_type	N	number(3)	Communication method. Possible values are: 0…Unspecified communication type 1…NCS 2…DCE TCP 3…DCE UDP 4…Sun RPC, TCP 5…SUN RPC, UDP 6…TCP Socket 7…UDP Socket 8…OPC Interface 9…RPC Local 10…HTTPS

Default Login Shell of opc_op User on HTTPS Agents

In the HPOM HTTPS Agent Concepts and Configuration Guide, the default login shell of the user `opc_op` is incorrect. The correct default shell is POSIX Shell (`/bin/sh`).

Wrong Character Set in the Administrator's Reference

The HPOM Administrator's Reference lists `ZHSI6CGB23128` as a character set for Simplified Chinese (on page 254). This is incorrect. The correct character set is `ZHS16CGB23128`.

Reduced Packet Size in Agent Installation Script

The HPOM Administrator's Reference, section "Installing or Updating HPOM Software Automatically" does yet not contain the following information about the agent installation 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
```

Number of Annotations Added for Duplicate Messages

The HPOM Concepts Guide, section "Suppressing Duplicate Messages on the Management Server" does yet not contain the following information about limiting the number of annotations added for duplicate messages:

If suppression is enabled, HPOM stores information about suppressed duplicate messages in annotations to the first message. Use the `OPC_MAX_DUPL_ANNO` configuration variable to limit the number of duplicate messages for which annotations are added.

Monitoring an Oracle Database in a Decoupled Management Server Configuration

The *HPOM Administrator's Reference*, section "Manual Operations for Starting, Stopping, and Monitoring HP Operations Management Server in a Cluster Environment" does yet not contain the following information about monitoring an Oracle database:

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`.

Load Balancing Software Incorrectly Mentioned in High Availability Through HPOM Server Pooling White Paper

The *High Availability Through HPOM Server Pooling* white paper incorrectly mentions the term load balancing software. This invokes wrong expectations. HPOM does not support load balancing software. The term load balancing software has been removed from the white paper and the following text has been added to clarify the situation:

Every physical server can have more than one virtual interface at once, which allows the implementation of load balancing. **Load balancing** in general terms refers to spreading a workload among multiple computers. Load balancing is often achieved by a load balancing software or hardware device.

In the context of HPOM for UNIX, load balancing refers to the concept of switching the responsibility for a group of managed nodes from one management server to another; for example, in the following situations:

- The load from incoming messages is too high.
- The number of managed nodes is too high for one management server. With a second management server added, you can split the load by directing half of the managed nodes to the second management server.

NOTE Server pooling is not designed for dynamic, short term load balancing. This is because the agent may run into a timeout and may start buffering messages. Eventually, it will establish a new connection after a successful switchover. It can be used, however, for longer term, manual load balancing.

HPOM for UNIX does not support load balancing software. To move some of the virtual interfaces to other, less used physical servers, you use commands such as `ovbbccb`, `netstat`, and `ifconfig`.

Non-root HTTPS Agents and Cluster Awareness

The *HPOM HTTPS Agent Concepts and Configuration Guide* does not yet contain the following information about managing HPOM agents running under alternative users in a cluster-aware environment:

Configuring Agents Running under Alternative Users

HPOM agents running under alternative users do not by default have the correct permissions to issue cluster commands such as HP Serviceguard's `cmviewcl` or `cmgetconf`. To grant non-root agents the required permissions, configure them to use a security program such as `sudo` or `.do` when issuing cluster commands.

For example, use the following command to configure HP Operations agents running under alternative users to use the `.do` tool when issuing cluster commands:

```
ovconfchg -ns ctrl.sudo -set OV_SUDO /usr/local/bin/.do
```

If you are using a configuration file to specify which users can run which commands, add the cluster commands listed in Table 4-4 to this file.

Table 4-4 Cluster Commands Used by ClAw

Cluster Application	Cluster Command
AIX Cluster (HACMP	`/usr/es/sbin/cluster/clstat`
	`/usr/es/sbin/cluster/utilities/clRGinfo`
	`/usr/es/sbin/cluster/utilities/clgetip`
HP Serviceguard	`/usr/sbin/cmviewcl`
	`/usr/sbin/cmgetconf`
Microsoft Cluster Server	ClAw uses APIs instead of command-line tools.
Red Hat Cluster Suite (Red Hat Enterprise Linux 4)	`/sbin/cman_tool`
	`/usr/sbin/clustat`
Red Hat Cluster Suite (Red Hat Enterprise Linux 5)	`/usr/sbin/cman_tool`
	`/usr/sbin/clustat`
Sun Cluster	`/usr/cluster/bin/scha_cluster_get`
	`/usr/cluster/bin/scha_resource_get`
	`/usr/cluster/bin/scha_resourcegroup_get`
TruCluster	`/usr/sbin/clu_get_info`
Veritas Cluster Server (VCS)	`/opt/VRTSvcs/bin/haclus`
	`/opt/VRTSvcs/bin/hasys`
	`/opt/VRTSvcs/bin/hagrp`
	`/opt/VRTSvcs/bin/hares`

The seldist.tmpl file Updates for New SPIs

The *HPOM Administrator's Reference*, section "Example of a policy configuration file" does yet not contain the following updates:

- The example of the `seldist.tmpl` file with 2004 and 2008 SPI changes should look like follows:

```
# This is the sample 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 ora_metrics     # catalog 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
# Added 2004
DBSPI spi_db
DBSPI spi_migrate
# end of section Database SPI

# SPI for SAP
sap r3                # general prefix for most files
sap OvSAP             # prefix used for ServiceDiscovery
sap spi_mysap         # prefix used for SelfHealingServices
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 OvReadConfig.dll  # used for SAP on Windows
sap OvSpiAseR3.dll    # used for SAP on Windows
sap librfc32.dll      # used for SAP on Windows
sap librfccm.so       # used for SAP on Linux
sap sap_mode.sh       # used for SAP on AIX/Solaris
```

```
# Added 2008
sap ovosysdetect_SAPspi # general prefix for many files
sap SAPNetWeaverTestRemoteConnection.pl
sap castor.jar
sap xalan.jar
sap xerces.jar
sap libsapspi_xerces-c.so.25
sap log4j-1.2.15.jar
sap SvcDisc.pm
sap xerces-c_2_7.dll
sap OvSetR3Configuration.dll
sap OvDPQueueCheck.dll
# end of section SPI for SAP

# PeopleSoft SPI
# This is partitioned into 10 node groups.
# Note that in order to distribute the files for the according SPI for Databases,
# the nodes need to be assigned to the DBSPI related node groups, too.
PSORAServer psspi
PSAppServer psspi
PSBatchServer psspi
PSWebServer psspi
PSDB2Server psspi
PSWinMSSServer psspi
PSWinAppServer psspi
PSWinBatchServer psspi
PSWinDB2Server psspi
PSWinORAServer psspi
# end of section PeopleSoft SPI
```

- The `sap-mode.sh` file name should be changed to `sap_mode.sh` in the following text:

  "... and `sap-mode.sh` are individual files."

- The text `PS_DB_Server dbspi` should replace the text `PSDB2Server psspi`. Likewise, `PS DB Server` in the following sentence should also be replaced with `PSDB2Server`:

  "... node belongs to either of the node groups `DBSPI` or `PS DB Server`."

Updates for Manually Installing the Performance Agent 4.x

The *HPOM Administrator's Reference* does not yet contain the correct paths and filenames for manually installing the versions 4.x of the Performance Agent. The existing instructions are correct for the Performance Agent versions 3.x.

The following directories for the Performance Agent 4.x should be added in the section "Manual Installation of HP Performance Agent" on pages 193-194 (HPOM Administrator's Reference, 8.10 and 8.20, Edition 15):

- *On HP-UX*
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/ia64/hp-ux11_32/`
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/ipf32/hpux1122/`
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/hp/pa-risc/`
- *On Solaris*
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/sun/sparc`
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/sun/x86/solaris10`
- *On AIX*
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/ibm/rs6000`
- *On Windows*
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/ms/x86/winnt/`
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/ms/x64/winxp/`
  - `/var/opt/OV/share/databases/subagent/VP_Perf_Agt/ms/intel/nt/`

Connecting with opcuihttps through the BBC Port 383

The *HPOM Administrator's Reference* does not yet contain the information about how to connect with secure JGUI (`opcuihttps`) through the BBC port (port 383).

The following prerequisites have to be met:

- Use a full authentication mode (not `anonymous`). On the HPOM management server, set an XPL variable as follows:

  ```
  ovconfchg -ovrg server -ns opc.opcuihttps -set SSL_CLIENT_VERIFICATION_MODE \
  RequireCertificate
  ```

- Install a client certificate, or an HTTPS agent from the management server on the system that is hosting Java GUI.
- On the Java GUI client, add the following settings to either `itooprc` or `ito_op.bat` file:
  - `https true`
  - `lcore_defaults true`

```
— https_port 383
```

5 Known Problems and Workarounds

This section describes problems with the HPOM software that are already known and could *not* be fixed until now. Where necessary, recommended workarounds are provided.

IMPORTANT The workarounds documented in these Release Notes reflect the status of the latest patch level. It is strongly recommended to install the most recent patches to ensure that you have the latest functionality and fixes.

It is also recommended to review the following sections before searching for a specific problem workaround:

- “Changed Features” on page 50.
- “What’s Not Yet Supported” on page 68.
- “What’s Not Supported” on page 69
- “Obsolete Features” on page 66.

NOTE **Before you install HPOM for UNIX, read this section in its entirety.**

NOTE The latest HPOM for UNIX known problems and workarounds are accessible from the following location:

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

Oracle Database Installation and Configuration

1. **Symptom QXCR1000425427**
   ovoinstall fails when Oracle is installed on a shared file system

   `opcconfig` might fail in a cluster environment if Oracle 10 is used, if Oracle is shared, and if it fails to determine the Oracle version correctly.

   Solution

   When using shared Oracle 10, use the `/bin/ksh` shell as root user.

2. **Symptom**
   opc Aborts with an Oracle Library Not Found Error

   If opc or another program is called as non-root user, it aborts with an Oracle library not found error, for example:

   ```
   pc
   /usr/lib/dld.sl: Can't find path for shared library: libclntsh.sl.9.0
   /usr/lib/dld.sl: No such file or directory
   Abort
   ```

   Solution

   During the 9.2.0.8 or later patchset installation, all new files and directories are created with restricted access, by default. That means that non-root users have do not have sufficient permissions to see and execute the Oracle binaries and libraries.

   Run the `$ORACLE_HOME/install/changePerm.sh` script as documented in the Patch Set Installation Instructions to change the permissions.

Management Server Upgrade/Migration

WARNING **An HTTPS agent must be installed on the HPOM for UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the HPOM for UNIX 8 management server system. Installing the DCE/NCS agent on the HPOM for UNIX 8 management server system could damage your installation!**

Do not install the HTTPS agent on an HPOM for UNIX 7 management server system. HPOM for UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE When installing HPOM for UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

Supported Migration Paths to HPOM for UNIX 8.20

The following migration paths are supported to HPOM for UNIX 8.20:

- *From HPOM for UNIX 7.1x*
  - on HP-UX (PA-RISC)
  - on Solaris (SPARC)
- *From HPOM for UNIX 8.1x*
  - on HP-UX (PA-RISC)
  - on Solaris (SPARC)

Uploading Upgrade Data

The handling of uploading the upgrade data has changed significantly from HPOM for UNIX 7 to HPOM for UNIX 8. With HPOM for UNIX 7, after loading the initial defaults, the customer data was uploaded with the command:

```
opccfgupld -replace -subentity
```

The HPOM for UNIX 8 upgrade procedure now documents to upload the downloaded data with the command:

```
opccfgupld -add -subentity.
```

This means, that for some configurations, the HPOM for UNIX 8 defaults are not be replaced by the previously downloaded configuration, but only not previously existing subentities are added.

This means, that the following configuration that was changed in HPOM for UNIX 7 will be present with the HPOM for UNIX 8 default and not the downloaded customer data:

- Application Group data (label and description - assignments are preserved).
- The management server managed node (this is by intention, since it is now an HTTPS agent).

- Message groups (label and description).
- Node defaults.
- Node Group data (only the label and descriptions).
- NodeBank Node Hierarchy. Note, that the command `opccfgupld add -subentity` will upload all nodes that are not yet in the node bank into the correct node layout group. So the node bank hierarchy is retained except for the management server node.
- Template defaults and existing conditions.
- Core data of the default users (`opc_adm`, `opc_op`, `netop` and `itop`).

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

- Database maintenance settings are reset (no audit and history download).
- Management Server Configuration is reset (audit settings, duplicate suppression settings, Server MSI settings and parallel distributions).
- Trouble Ticket Call is reset to no trouble tickets.

The Required Approach

The data that would cause problems when uploaded with the `-replace` option is the management server node and all cluster nodes. Therefore, after uploading the data with `-add -subentity`, you can upload the data with `-replace -subentity` if you exclude the managed nodes:

1. Copy the index file of the download (download-directory /$LANG/*.idx). For example:

   ```
   cp /tmp/cfgdwn/C/cfgdwn.idx /tmp/cfgdwn/C/nonodes.idx
   ```

2. Modify the copied index file. Remove the node bank section from the index file. This is everything from the line:

   ```
   ENTITY NODE_BANK
   ```

   To the semi colon (';') before the node defaults:

   ```
   ;
   ENTITY NODE_DEFAULTS *
   ```

   and the `CONTENTS *` line if it exists.

3. Now upload your configuration data using the command:

   `opccfgupld -replace -subentity with the -index option`

   For example:

   ```
   opccfgupld -replace -subentity -configured -index \
   /tmp/cfgdwn/C/nonodes.idx /tmp/cfgdwn
   ```

Workarounds

1. **Symptom QXCR1000196910**
   MoM: respmgrs File Must be Updated After HPOM for UNIX Server and Agent Upgrade to HPOM for UNIX 8

   After upgrading a MoM environment from HPOM for UNIX 7 to HPOM for UNIX 8 and converting some agents to HTTPS, the following must be taken into consideration. HPOM for UNIX 8 managed nodes cannot communicate with an HPOM for UNIX 7 management server and therefore you might get errors.

   Solution

   If you have a mixed environment with HPOM for UNIX 7 and HPOM for UNIX 8 servers, you may need to deploy two flavors of `allnodes` files:

   - The `allnodes` file that contains HPOM for UNIX 7 and HPOM for UNIX 8 management servers.
   - The `allnodes.bbc` file that contains only HPOM for UNIX 8 management servers.

   The essential thing is that no HPOM for UNIX 7 management servers are mentioned in a responsible-manager file which is deployed to an HTTPS agent, because the HPOM for UNIX 7 server cannot handle HTTPS traffic from the agent.

   In addition, all management servers that are mentioned in responsible-manager templates, for example:

   `/etc/op/OV/share/conf/OpC/mgmt_sv/respmgrs/allnodes.bbc`

   a. Must be added to the Node Bank
   b. Must be HTTPS-capable (not HPOM for UNIX 7 or lower)
   c. Their core ID must be present in the node bank

   For more information, check for term `allnodes.bbc` in the *HPOM HTTPS Agent Concepts and Configuration Guide*.

2. **Symptom QXCR1000200001**
   ovoremove does not Remove Some Filesets on Upgraded Systems

   After running `ovoremove` on a system which was upgraded from HPOM for UNIX 7.xx to 8.00 some filesets are still present.

   Solution

   Perform deinstallation using the command `ovoremove -f`. If you already encountered this problem use `ovoremove -f` from HPOM CD1.

   To remove left-over from HPOM for UNIX 7.10 system run the following commands:

   ```
   swlist -l | grep -i -e ITO -e OVO
   ```

   ```
   swremove <product1> <product2> ...
   ```

3. **Symptom**
   Nodes with Unknown Agent Type Skipped During Configuration Upload

   When uploading configuration data to an HPOM for UNIX management server, errors are displayed for managed nodes with agent platforms types that are not installed on the management server, for example, DCE agents.

   Solution

   This is the intended behavior.

However, to avoid losing node configurations of these managed node platforms, make sure that you have the corresponding HPOM agent fileset installed on the HPOM for UNIX management server before running `opccfgupld(1m)` again. The current DCE agent platforms can be found on CD2:

`/OV_DEPOT/HPOvOrpcClients.depot`

To install the depot, mount CD2 and enter the following command as user `root`:

```
swinstall -x mount_all_filesystems=false -s <mount point>/\
OV_DEPOT/HPOvOrpcClients.depot \*
```

4. **Symptom NSMbb70296**
   Obsolete Application Groups Still Visible After Upgrading from HPOM for UNIX 7.1x to HPOM for UNIX 8

   After the upgrade from HPOM 7.10 to HPOM 8, some obsolete application groups are still visible in the Application Bank. For example `MetaFrame Tools`. In general, these application groups have been replaced with new ones. The HPOM applications in these obsolete groups might not work. If no customizations have been made, these application groups can be removed. However, if you have added applications to these groups, move them to an appropriate HPOM 8 application group before deleting the obsolete groups.

   For a detailed mapping of the new application groups used by the OS-SPIs, refer to Table 1-11, “OS-SPI Application Mapping,” on page 62.

   The following Application Groups have been replaced and are obsolete:

   - `GlancePlus`
   - `Jovw`
   - `MetaFrame Tools`
   - `OV Performance`
   - `Reports`
   - `VERITAS`

   The following applications are also no longer provided:

```
Application                            Label
------------------------------------------------------------
/Net Activity/Interface Statistics  : Interface Statistics
/OV Services/OV CDP View            : CDP View
```

   Solution

   To remove an application, execute the following steps:

   a. Right-click the application or application group.

   b. Select `Delete...`

5. **Symptom NSMbb70285**
   VPO Status Application Visible After Upgrading from HPOM for UNIX 7.1x to HPOM for UNIX 8

   After the upgrade from HPOM for UNIX 7.1x to HPOM for UNIX 8, in the Application Bank you see one `OVO Status` application and one `VPO Status` application.

   Solution

To remove the VPO Status application, execute the following steps:

a. Right-click the VPO Status application.

b. Select Delete.

6. **Symptom QXCR1000196891**
Service Navigator Value Pack Requirements for Migration from HPOM for UNIX 7 to HPOM for UNIX 8

The listed parameters in the opcsvinfo file of an HPOM for UNIX 7.xx installation are used by the Service Navigator Value Pack and must be migrated to OVconf, ovrg server, namespace opc for HPOM for UNIX 8.00.

Solution

Recreate the two required parameters:

OPCSVCM_MSGSVSNAME_DEFAULT

OPCSVCM_FILESYSTEM_SOCKET

using the following commands:

```
cadmactivate -d
```

```
cadmactivate
```

7. **Symptom QXCR1000139398**
OVwModifySubmap: Submap Permission Denied

After the upgrade from HPOM for UNIX 7.1x to HPOM for UNIX 8, when you start the Motif GUI for the first time, the following error message is displayed on stderr of the shell from which you started the Motif GUI:

```
OVwModifySubmap: Submap permission denied.
```

Solution

This error message can be safely ignored.

New Installation of the HPOM for UNIX Management Server

WARNING **An HTTPS agent must be installed on the HPOM for UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the HPOM for UNIX 8 management server system. Installing the DCE/NCS agent on the HPOM management server system could damage your installation!**

Do not install the HTTPS agent on an HPOM 7 management server system. HPOM 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE DO NOT run `ovoinstall` from the CD mount point.

NOTE Before migrating from HPOM for UNIX 7.1x to HPOM for UNIX 8, you must switch off the OVAS functionality completely for the Java UI.

NOTE When installing HPOM for UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

NOTE If you are using Hummingbird Exceed, XDMCP should be set to `Exceed XDMCP Query`.

Installation Workarounds

1. **Symptom QXCR1000376614**
   ovoinstall fails because newer versions of components are already on the system

   The installation of some of the components fails because newer versions of the components are already installed.

   Solution

   A new `ovoinstall` script, which fixes this symptom, is available for download. For more information about the `ovoinstall` script location, see Table 2-1 on page 75.

2. **Symptom QCCR1A93841**
   ovoinstall script for 11.31 leaves allow_incompatible flag set to true

   The `ovoinstall` and `ovoremove` scripts temporarily change the system-wide SD defaults (`/var/adm/sw/defaults`) to add the following lines on HP-UX 11.31 (since the depot is not compatible with 11.31):

- mount_all_filesystems=false
- enforce_dependencies=false
- allow_incompatible=true

In case the scripts exit unexpectedly, these settings remain in the SD defaults file and consenquently cause problems.

Solution

The ovoinstall and ovoremove scripts were changed to allow you to specify the flags directly in the command-line interface, instead of modifying the system-wide SD defaults file. A new ovoremove script is available as part of the HPOM 8.35 patch, and a new ovoinstall script is available for download from the location stated in the Table 2-1 on page 75.

3. **Symptom QXCR1000363029**
   ovoinstall Hangs if NNM 7.5x is Installed

   ovoinstall hangs at the point where ovoinstall.log says it is entering the PostM10iPatch function.

   Solution

   A new ovoinstall script, which fixes this symptom, is available for download. For more information about the ovoinstall script location, see Table 2-1 on page 75.

4. **Symptom QXCR1000288952**
   Error During Database Configuration - ORA-00942: table or view does not exist

   During the database configuration section of the installation of the HPOM for UNIX management server the following error is written into System.txt:

   ```
   ORA-00942: table or view does not exist
   ```

   Solution

   You can safely ignore this error.

5. **Symptom QXCR1000294562**
   Errors During when Deinstalling HPOM for UNIX with a Remote Database

   When deinstalling the HPOM management server using a remote database server with ovoremove, the following errors and warnings are displayed:

   ```
   ERROR:   Error occurred calling sqlplus.
   ERROR:   Error occurred while trying to get ORACLE tablespaces and data files
   WARNING: Couldn't remove the opc tablespaces.
   WARNING: Please remove these files manually in the index and data directory.
   WARNING: If these files aren't removed a later installation can fail.

   WARNING: Net listener configuration files left untouched
   WARNING: Please remove the entries for ov_net/openview manually.
   ```

   Solution

   You can safely ignore these errors and warnings. After ovoremove has finished, remove the database on the remote database server manually. As user oracle execute the following commands:

   ```
   sqlplus /nolog
   SQL> connect system/manager
   SQL> shutdown abort
   SQL> quit
   ```

Manually delete all files in the Oracle index and data directory on the database server, for example `/u01/oradata/openview/`.

Remove SID (for example, HP Operations Manager) entries on both the management server and the database server from the following configuration files:

`/etc/oratab`
`<ORACLE_HOME>/network/admin/listener.ora`
`<ORACLE_HOME>/network/admin/sqlnet.ora`
`<ORACLE_HOME>/network/admin/tnsnames.ora`
`<ORACLE_HOME>/network/admin/tnsnav.ora`

Delete the following files on the management server:

/etc/opt/OV/share/conf/ovdbconf
/opt/OV/conf/ovdbora (on HPOM server)

Delete the following files on the database server:

`<ORACLE_HOME>/dbs/init<SID>.ora`
`<ORACLE_HOME>/dbs/spfile<SID>.ora`

6. **Symptom QXCR1000289820**
   ovcs Aborts after Deinstalling and Installing HPOM for UNIX

   After de-installing HPOM and installing it again with ovoinstall, `ovcs` keeps aborting, even after stopping and starting all processes.

   Solution

   The deinstallation of HPOM for UNIX also removed the certificate server (CS) including the root CA, but could not remove the certificate client (CC) with old certificates if other installed HP Operations Manager products use the CC component. The old certificates are now not accepted by the new C

   First, remove the old certificates. Here is an example of commands used:

   ```
   COREID=`ovcoreid`
   ovcert -remove $COREID
   ovcert -remove $COREID -ovrg server
   ```

   You also have to remove the old CA certificate in the agent section:

   ```
   ovcert -remove CA_${COREID}
   ```

   Now export the trusted CA certificate (the CA certificate that was created during the installation):

   ```
   ovcert -exporttrusted -file /tmp/trustedcertif -ovrg server
   ovcert -importtrusted -file /tmp/trustedcertif
   ```

   Issue a new certificate:

   ```
   ovcm -issue -file /tmp/certif -name $(hostname) -pass mypwd -coreid $(ovcoreid)
   ```

   Import the new certificate for the local agent:

   ```
   ovcert -importcert -file /tmp/certif -pass mypwd
   ```

   Import the new certificate for the management server. The needed steps depend on wether you use a cluster or not.

   a. Non-clustered environment:

      ```
      ovcert -importcert -file /tmp/certif -pass mypwd -ovrg server
      ```

   b. Clustered environment:

```
rm -f /tmp/certif
ovcm -issue -file /tmp/certif -name $(hostname) -pass mypwd -coreid \
$(ovcoreid -ovrg server)
ovcert -importcert -file /tmp/certif -pass mypwd -ovrg server
```

Remove the temporary files:

```
rm -f /tmp/trustedcertif /tmp/certif
```

Remove the templates in the HPOM template cache that were signed with the old certificate:

```
find /etc/opt/OV/share/conf/OpC/mgmt_sv/templates -type f -exec rm -f {} \;
```

7. **Symptom QXCR1000213326**
   ovoinstall: wrong text for NLS proposal for Taiwanese

   During the installation of the HPOM for UNIX management server in Taiwanese, the proposed `NLS_LANG` is `traditional chinese_taiwan.ZHS16GBK` but the message text recommends using `traditional chinese_taiwan.ZHT16BIG5`.

   Solution

   Use the proposed `NLS_LANG` of **`traditional chinese_taiwan.ZHS16GBK`** and ignore the message text.

8. **Symptom QXCR1000202026**
   expr Error During ovoinstall with CC Mounts

   During disk space check of ovoinstall `expr` error is displayed.

   Solution

   This problem is caused by local filesystem mounts (lofs). Except bad disk space calculation for the file systems in questions and aesthetic problems this error output can be safely ignored.

9. **Symptom QXCR1000195500**
   HPOM for UNIX Management Server Installation Fails if /var/opt is a Symbol Link

   If the directory `/var/opt/OV` or `/var/opt` is a symbolic link, the HPOM for UNIX management server installation fails.

   Solution

   `/var/opt/OV` and `/var/opt` must be local directories.

10. **Symptom QXCR1000135085**
    swverify Error Messages

    `swverify` reports many errors about the existing installation.

    Solution

    These error messages can be safely ignored.

11. **Symptom QXCR1000199175**
    HPOM for UNIX Installation Fails in NIS Environments

    It is possible that when `ypbind` (NIS binder process) is running but the NIS environment is not configured, the `opcgrp` group is not created and HPOM for UNIX server installation fails.

    Solution

    If you are using NIS or NIS+, make sure that the NIS or NIS+ environment is correctly configured and all NIS or NIS+ processes are running on the system where HPOM for UNIX server is to be installed. Otherwise, all NIS or NIS+ processes, for example, `ypbind` or `rpc.nisd`, must be stopped before starting the HPOM for UNIX management server installation.

New HA Installation of the HPOM for UNIX Management Server

TIP Before installing the HPOM for UNIX management server in a cluster environment, refer to the chapter titled *Administration of the HPOM Management Server in a Cluster Environment* in the *HPOM Administrator's Reference Guide* for information on cluster concepts, and how to use and troubleshoot HPOM for UNIX installed in cluster environments.

For detailed information refer to the *HPOM Installation Guide* or one of the dedicated installation guides for installing HPOM for UNIX in an HP Serviceguard environment using a local database available from:

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

NOTE HPOM for UNIX 8 can only be installed on clean systems or migrated from HPOM for UNIX 7.1x and later versions. If any other previous version of HPOM for UNIX was installed on the system chosen to host the HPOM for UNIX 8 management server, ensure that this installation is completely removed and that the HP Operations Manager database instance is also removed.

NOTE DO NOT run `ovoinstall` from the CD mount point.

WARNING **An HTTPS agent must be installed on the HPOM for UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the HPOM for UNIX 8 management server system. Installing the DCE/NCS agent on the HPOM management server system could damage your installation!**

Do not install the HTTPS agent on an HPOM for UNIX 7 management server system. HPOM for UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE Before migrating from HPOM for UNIX 7.1x to HPOM for UNIX 8, you must switch off the OVAS functionality completely for the Java UI.

NOTE When installing HPOM for UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

1. **Symptom AutoPass License Password Installation in Server HA Environments**

   The HPOM AutoPass component is integrated into HPOM for UNIX 8 to manage its licenses. This component installs, checks and manages the license passwords and stores the passwords in a location that is typically not shared in HA environments. In addition, AutoPass uses the local IP-Address and not on the virtual IP-Address. This makes it necessary to get HPOM license passwords for all cluster nodes and install them on each cluster node.

   Solution

   Request your HPOM license passwords for all cluster nodes in a HA environment with its physical IP-Address and install these passwords on the according cluster nodes.

Upgrade of the HPOM for UNIX Management Server Running in an HA Environment

TIP Before installing the HPOM for UNIX management server in a cluster environment, refer to the chapter titled *Administration of the HPOM Management Server in a Cluster Environment* in the *HPOM Administrator's Reference Guide* for information on cluster concepts, and how to use and troubleshoot HPOM for UNIX installed in cluster environments.

NOTE HPOM for UNIX 8 can be installed *only* on clean systems or migrated from HPOM for UNIX 7.1x and later patch versions. If any other previous version of HPOM for UNIX was installed on the system chosen to host the HPOM for UNIX 8 management server, ensure that this installation is completely removed and that the HP Operations Manager database instance is also removed.

WARNING **An HTTPS agent must be installed on the HPOM for UNIX 8 management-server system. Do not attempt to install a DCE/NCS agent on the HPOM for UNIX 8 management server system. Installing the DCE/NCS agent on the HPOM management server system could damage your installation!**

Do not install the HTTPS agent on an HPOM for UNIX 7 management server system. HPOM for UNIX 7 cannot communicate with the HTTPS agent and attempting to install the HTTPS agent could damage your installation!

NOTE DO NOT run `ovoinstall` from the CD mount point.

NOTE Before migrating from HPOM for UNIX 7.1x to HPOM for UNIX 8, you must switch off the OVAS functionality completely for the Java UI.

NOTE When installing HPOM for UNIX in a Japanese environment, the underlying Network Node Manager installation and UNIX OS-SPI installation dialogues are in English.

1. **Symptom QXCR1000139026**
   Node Type (HTTPS) Must be Changed on All Cluster Nodes

   Using virtual nodes in HPOM for UNIX 8 requires that all nodes (physical and virtual) are of the same platform type (HTTPS).

   Changing the agent type when upgrading from DCE to HTTPS must be done in a very short time frame for all nodes (minutes!).

NOTE All agent types must be of the same type also after the migration.

Management Server Runtime

1. **Symptom QXCR1000753602**
   HPOM message processing may become slow due to slow name resolution

   If the name resolution is slow, `opcmsgm` cannot process messages as fast as it normally does.

   Solution

   To improve HPOM name resolution and consequently message processing speed, do the following:

   a. Make sure the reverse lookup works well.

   b. Make sure unknown hosts and IP addresses resolve in a reasonable time.

   c. If DNS works well, use DNS first and then fallback to `/etc/hosts` in `/etc/nsswitch.conf`:

   ```
   hosts:        dns [NOTFOUND=continue] files
   ```

NOTE `opcmsgm` processes messages immediately after the server restart even if the name service is slow. This is due to the fact that the IP mapping table is created in a separate thread.

It is also possible to disable the IP mapping table. You can do this by entering the following:

```
ovconfchg -ovrg server -ns opc -set OPC_DISABLE_IP_MAPPING_TABLE TRUE
```

---

   d. Change HPOM retries to 1 by entering the following command:

   ```
   ovconfchg -ovrg server -ns opc -set OPC_NAMESRV_RETRIES 1
   ```

   e. Cache name service results either by setting up the caching DNS server on the management server or by increasing the size of the HPOM name service cache. In the latter case, the size of the HPOM name service cache should be set so that it can hold all node bank nodes and some additional ones. For example:

   ```
   ovconfchg -ovrg server -ns opc -set OPC_NAMESRV_CACHE_SIZE 10000
   ```

   f. Measure name resolution time, and generate a warning if the threshold is exceeded (for example, 200 milliseconds) by entering the following:

   ```
   ovconfchg -ovrg server -ns opc -set OPC_NAMESRV_MAX_TIME 200
   ```

   g. Within DNS, define timeouts for resolver functions to limit the time that a name service call takes if there are problems with DNS. This is done differently on different platforms:

   - HP-UX:

     You can modify two settings on HP-UX:

     `retrans`: retransmission timeout with the default value being 5000 milliseconds

     `retry`: number of retries with the default value being 4

     There are two ways in which this can be done, either by using `/etc/resolv.conf` (system wide) or the `RES_RETRY` and `RES_RETRANS` configuration variables (only for those processes).

For example, to set the timeout to 1 second and retries to 2, add the following lines to `/etc/resolv.conf`:

```
retrans 1000
retry 2
```

NOTE With Core Agent patch A.08.13 and later, it is possible to set the configuration variables for `ovcd` (and its children) in the `ctrl.env` name space, for example:

```
ovconfchg -ns ctrl.env -set RES_RETRY 2 -set RES_RETRANS 1000
```

After doing that you must restart the agent.

With management server patch A.08.33 and later, it is possible to set the configuration variables for the server processes in the `opc` name space, for example:

```
ovconfchg -ovrg server -ns opc -set RES_RETRY 2 -set RES_RETRANS 1000
```

After doing that you must restart the management server processes.

- Solaris:

  You can modify several settings on Solaris, including the same two as on HP-UX:

  `retrans`: retransmission timeout with the default value being 5 seconds

  `retry`: number of retries with the default value being 4

  The ways in which this can be done are the same as for HP-UX.

  `retrans` and `retry` must be set as options on Solaris. For example,

  ```
  options retrans:1
  options retry:2
  ```

2. **Symptom QXCR1000103169**
   Escalated Messages with CMAs not Displayed

   Escalated messages with added custom message attributes are not displayed in the message properties in the Java GUI.

   Solution

   Currently, CMAs cannot be escalated yet.

3. **Symptom QXCM1000412508**
   opcforwm Performance Degrade and Abort

   Bulk message forwarding loses items on bulk tag change, opcforwm performance degrades aborts on forward loops when using HPOM for Windows.

   Solution

   A solution for this symptom is not included yet in the HPOM for UNIX 8.25 management server patch but is available as a 8.25 patch based hotfix from HP support and will be included in the next HPOM for UNIX management server patch.

4. **Symptom QXCR1000361388**
   Inaccessible HPOM URLs When NNM 7.5x Installed

   Management Server URLs are inaccessible when NNM 7.5x patch is installed.

Solution

a. Stop all HPOM processes including `httpd`. Enter the following:

`ovstop`

b. Modify `/opt/OV/httpd/conf/httpd.conf` file on your management server. Add the following lines:

```
<Directory /opt/OV/www/htdocs/ito_doc>Options Indexes FollowSymLinks
AllowOverride None
order allow,deny
allow from all
</Directory>

<Directory /opt/OV/www/htdocs/ito_op>
 Options +MultiViews
 Options +MultiViews
 Options +MultiViews
 Options +MultiViews
</Directory>
<Directory /opt/OV/www/htdocs/ito_op/>
 ErrorDocument 404 /ITO_MAN/itoman_error.htm
</Directory>

Alias   /ITO_OP /opt/OV/www/htdocs/ito_op/
Alias   /ITO    /opt/OV/www/htdocs/ito/
Alias   /ITO_DOC        /opt/OV/www/htdocs/ito_doc/
Alias   /ITO_JDOC_AGT   /opt/OV/www/htdocs/jdoc_agent/
Alias   /ITO_MAN        /opt/OV/www/htdocs/ito_man/
ScriptAlias     /ITO_SVC        /opt/OV/www/htdocs/ito_svc/opcsvcweb
```

c. Start all HPOM processes. Enter the following:

`ovstart`

5. **Symptom QXCR1000291336**
Templates are not distributed to the Managed Nodes

Templates for the HPOM managed node are not successfully distributed after changing the communication port ranges for the HPOM managed node.

Solution

Before distributing the templates to the HPOM managed node after the communication ports for it had been changed, create a symbolic link on the HPOM management server using the following command:

```
ln -s /opt/OV/bin/OpC/utils/opcsv_reinit /opt/OV/lbin/xpl/config/update/opcsv_reinit
```

6. **Symptom QXCR1000289933**
Error in System.txt: Cannot open pipe svcengmsgadptp

When restarting the management server using `opcsv -stop` and `opcsv -start`, the following error is logged in `System.txt`:

```
Cannot open pipe svcengmsgadptp
```

Solution

This error message can safely be ignored.

7. **Symptom QXCR1000289718**
   Critical Errors in Message Browser and System.txt after Disabling OvoDceDistmMsgrd

   If the `OvoDceDistmMsgrd` service is disabled with `ovprotect`, critical messages and errors occur in the Message browser and `System.txt`.

   Solution

   Do not disable the `OvoDceDistmMsgrd` service. If the service is already disabled, enabled it using ovprotect.

8. **Symptom QXCR1000289120**
   Deleting a Node with Software Already Deinstalled

   When deleting a node within the HPOM GUI, from which HPOM software has already been deinstalled, the following question is displayed nonetheless:

   ```
   Do you want to automatically deinstall software from managed nodes?
   ```

   Solution

   If the HPOM software has already been removed from the specified node, you can safely ignore this question.

9. **Symptom QXCR1000200633**
   Logfile Entries Cannot be converted from eucJP to SJIS

   The following message appears in the HPOM Message Browser:

   (OpC30-138)
   Can't convert logfile entry.
   (OpC20-274)
   Bad input character converting string from "eucJP" to "SJIS".
   Incorrect byte sequence.

   Solution

   The character set for all Logfile Templates must be changed to reflect the current locale character set. This can be done using `Message Source Templates` window from the Motif GUI. Redistribute modified templates, if they were previously distributed.

10. **Symptom QXCR1000138782**
    Identical Cron Messages Are Generated From Two Templates

    Two identical Cron messages are generated each time, (one in English and the other Japanese) from the following message source templates:

    Message in Japanese:

    `Cron (Solaris)` under `Default: Solaris` template group:

    ```
    fetch 'cron|at|batch command failed
    ```

    Message in English:

OSSPI-SOL-Cron_1 under "Operating System SPIs: SOLARIS: QuickStart Solaris Policies template group:

```
fetch 'cron|at|batch command failed.
```

Solution

Write a multiple-source ECS correlator such that only one of these messages hits the browser.

Or,

Suppress the conditions from either template, if both templates are deployed to all nodes.

11. **Symptom QXCR1000287349**
After Enabling Tracing for opcctlm process the HPOM for UNIX Management Server cannot be Started

After enabling remote tracing for server's opcctlm process, the HPOM for UNIX management server cannot start.

Solution

Do *not* use remote tracing for opcctlm process, use local tracing instead. You can set local tracing for opcctlm on management server by entering the following:

```
ovconfchg -ovrg server -ns opc -set OPC_TRACE TRUE
ovconfchg -ovrg server -ns opc -set OPC_TRC_AREA DEBUG
ovconfchg -ovrg server -ns opc -set OPC_TRC_PROCS opcctlm
```

The trace file should be generated at the following location:

```
/var/opt/OV/share/tmp/OpC/mgmt_sv/trace
```

12. **Symptom QCCR1A98561**
The server processes cannot be started because the password of the Oracle user opc_op expired

With Oracle 11g, password aging is enabled by default and passwords expire in six months. If the password of the Oracle user opc_op expires, the HPOM processes are no longer able to connect to Oracle.

Solution

a. Change the password in the database and in the HPOM password file using the following command:

```
# /opt/OV/bin/OpC/opcdbpwd -set
```

b. Because of an Oracle defect (Bug 7462851) set the opc_op password manually.

IMPORTANT Be sure to use the same password as for the `/opt/OV/bin/OpC/opcdbpwd -set` command:

```
# su - oracle
$ sqlplus /nolog
SQL> connect / as sysdba
SQL> alter user opc_op identified by <password>;
SQL> exit
```

c. Update the Admin UI with the changed password using the following commands:

```
# /opt/OV/OMU/adminUI/adminui clean
# /opt/OV/OMU/adminUI/adminui password -u ovodb -a -p <password>
```

Now you should be able to start the processes again.

d. Make sure that the processes that were started before changing the password can be restarted. Restart the processes using the following commands:

```
# ovc -kill
# ovc -start
```

e. Change other Oracle passwords, for example, `opc_report`, `sys`, and `system` as follows:

```
# su - oracle
$ sqlplus /nolog
SQL> connect / as sysdba
SQL> alter user opc_report identified by <new-password>;
SQL> alter user system identified by <new-password>;
SQL> alter user sys identified by <new-password>;
SQL> exit
```

If you want to disable password aging, do the following:

```
# su - oracle
$ sqlplus /nolog
SQL> connect / as sysdba
SQL> ALTER PROFILE default LIMIT PASSWORD_LIFE_TIME UNLIMITED;
SQL> exit
```

For more information about Oracle password aging and password complexity, see the Oracle documentation.

Management Server Deinstallation

1. **Symptom QXCR1000195544**
   Error During Removal of HPOvXpl Package

   After running `ovoremove` including deinstallation of NNM, the `HPOvXpl` package remains on the disk and can be verified by using `pkginfo` or `swlist`.

   Solution

   Remove the file manually as user root by entering the following command:

   ```
   swremove HPOvXpl
   ```

2. **Symptom QXCR1000138928**
   OS-SPI Scripts Remain after ovoremove

   After removal of the OS-SPI, many OS-SPI scripts remain in the directory tree:

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

   Solution

   Execute the following command to remove all OS-SPI related programs:

   ```
   find /var/opt/OV/share/databases/OpC/mgd_node/customer -name \
   osspi_* -type f | xargs rm
   ```

HTTPS Managed Nodes Installation

NOTE If you are using the 'certificate installation using install-key' method (refer to the *HPOM HTTPS Agent Concepts and Configuration Guide* for details about this method), always use a new installation key for each new managed node installation. Reuse of a previously used installation keys can result in lack of connection to the managed node without any error messages being displayed.

1. **Symptom QCCR1A90854**
   Installing agent patches during the first pause of the ovoinstall script causes the postinstall script of the agent patch to fail

   If you install the agent patches during the first pause of the `ovoinstall` script, which pauses twice to allow the installation of the patches, the `postinstall` script of the agent patch will fail because the database is not yet configured and the Oracle library symbolic links are missing.

   NOTE The `ovoinstall` script pauses twice to allow the installation of the patches:

   - Before `opcconfig`/`opcdbsetup` is called: this allows you to install the server patch and optionally the Java GUI patch. After that `ovoinstall` runs `opcconfig`/`opcdbsetup` to configure the database.
   - After `opcconfig`/`opcdbsetup` is called: this allows you to install the agent patch(es). After that `ovoinstall` installs the local agent, which means that the patched agent will be used.

   Solution

   If you installed the agent patches during the first pause, run `opcagtutil` once again, for example:

   ```
   /opt/OV/bin/OpC/install/opcagtutil -p hp/ipf32/hpux1122 -require
   ```

   IMPORTANT To avoid this problem, it is important that you install the agent patches during the second pause of the `ovoinstall` script.

2. **Symptom QXCR1000815477**
   Agent patch installation fails after OVO-CLT.OVO-ZLIN-CLT is installed

   After installing Linux zSeries depots (version A.08.10.160) on the HPOM for UNIX server, you can receive an error when installing EventAction/Core HPOM for UNIX Agent patches.

   Solution

   To avoid this problem, perform as follows:

   a. Deinstall all old Linux zSeries depots:

```
swremove OVO-CLT.OVO-ZLIN-CLT
swremove OVO-CLT-NLS.OVO-ZLIN-JPN
swremove OVO-CLT-NLS.OVO-ZLIN-KOR
swremove OVO-CLT-NLS.OVO-ZLIN-SCH
swremove OVO-CLT-NLS.OVO-ZLIN-SPA
```

NOTE Deinstalling old Linux zSeries depots does not affect managed nodes with the already installed zSeries agent software, as well as customizations stored in the customer directory tree.

b. Reinstall the affected patch by executing the following command:

```
swinstall -x reinstall=true -x reinstall_files=true -x \
autoreboot=true -x patch_match_target=true -s <full_path_of_affected_patch_depot>
```

c. Install a new Linux zSeries depot.

For detailed information about the installation process, refer to the updated Release Notes for “OMU A.08.17 AGENT FOR SLES9/SLES10”.

The new depot and Release Notes are available at the following location:

`ftp://ovweb.external.hp.com/pub/cpe/ito/zSeries_HTTPS_agent/`

3. **Symptom QXCR1000381360**
Cannot install 8.10.160 AIX Agent on HP-UX 11.23 PA-RISC

The installation of the HP Operations Manager HPOM A.08.10.160 AIX Agent on HPOM Management Server for HP-UX 11.23 PA-RISC fails.

Solution

Install the agent using the allow_incompatible=true option:

```
swinstall -x allow_incompatible=true
```

4. **Symptom QXCR1000344595**
Windows agent installation unregisters RegObj.dll

The installation of the HTTPS agent software unregisters the shared library RegObj.dll. This causes problems with other applications that use this DLL.

Solution

Reregister RegObj.dll using the following command:

```
C:\WINDOWS\system32\regsvr32.exe  /s "<path_to_regobj>\regobj.dll"
```

5. **Symptom QXCR1000306217**
HPOM for UNIX Perl Modules Cannot be Found

The Perl installed with the HPOM agent fails to find the HPOM for UNIX Perl modules if another application sets the PERL5LIB to point to locations that do not include the HPOM for UNIX Perl lib location.

Solution

Prepend the ovo perl lib path to the PERL5LIB system environment variable using the following commands

```
PERL5LIB=C:\Program Files\HP OpenView\nonOV\perl\a\lib;c:\OR..
```

Restart the agent processes using the following commands:

```
opcagt -kill
opcagt -start
```

Check the ovo environment:

```
ovdeploy -cmd set
```

Reboot the system, if the PERL5LIB variable is not set correctly and the system variable is correct.

6. **Symptom QXCR1000301123**
   Installation and Deinstallation Times of the HTTPS Agent on an AIX System

   The installation of the HTTPS agent on an AIX system takes considerably longer than on other platforms.

   Solution

   Read the Known problems and Limitations sections of the Readme file provided with the HTTPS agent for AIX patch.

7. **Symptom QXCR1000300781**
   Embedded Performance Agent Aborts on an AIX System

   The embedded performance agent (CODA) daemon may abort on AIX systems.

   Solution

   Apply the latest available HPOM HTTPS Core agent and Embedded Performance patches.

8. **Symptom QXCR1000284265**
   Disk Space Error when Installing the HTTPS Agent on an AIX System

   The installation of the HTTPS agent on an AIX system fails due to insufficient available disk space.

   Solution

   Make sure that there is at least 120 MB of free disk space available in the `/tmp` partition or the partition that contains this directory.

9. **Symptom QXCR1000286867**
   Building Example Programs for HP-UX 11.23 IPF fails

   Using `Makef.hpuxIA32` to build example programs on HP-UX 11.23 IPF returns errors.

   Solution

   To build the HPOM agent example program files, open the following file:

   ```
   /opt/OV/OpC/examples/progs/Makef.hpuxIA32
   ```

   and replace the following line:

   ```
   OPCLIB=-lopc_r -lnsp -lopcas
   ```

   with

   ```
   OPCLIB=-lopc_r -lnsp
   ```

10. **Symptom QXCR1000241952**
    HTTPS Agent Deinstallation Error with HP Performance 5.0 Installed on the same System

    HP Operations Manager HTTPS agent deinstallation returns an error if the HTTPS agent is being deinstalled from a system with HP Performance 5.0 installed.

Solution

Due to a dependency of HP Performance on the `HPOvPerf.HPOVPACC` fileset, the deinstallation of the HTTPS agent fails. This behavior is expected when the HPOM HTTPS agent installed on the same system as HP Performance 5.0 Nevertheless, the HPOM-specific part of the agent is deinstalled in any case.

11. **Symptom QXCR1000202565**
Modifying Type/Platform of a Node Retains Previous Parameters

After modifying the machine type/platform of a node in the Node Bank, parameters valid for the original type/platform remain. For example, `Interval` and `Installation user`. This can cause installations to fail, for example, when you modify from UNIX to WINDOWS node types and the `Installation user` field is not changed from `root` to `Administrator`.

Solution

After modifying Machine type/platform from UNIX to WINDOWS in the Motif GUI, modify the `Installation user` field from `root` to `Administrator`.

12. **Symptom QXCR1000204686**
Communication Broker does not Register with Windows Firewall on Windows XP SP2

When installing the HPOM HTTPS agent on a Windows XP SP 2 system, the certificate installation fails because the Communication Broker (`ovbbccb`) is not registered at the Windows Firewall. The result is that all HTTPS communication fails.

This can be verified by running the following command on the HPOM for UNIX Management Server system:

`bbcutil -ping <node>`

Solution

Register the Communication Broker (`ovbbccb`) manually:

a. Open the `Control Panel` -> `Windows Firewall`.

b. Open the `Exceptions` tab.

c. Click `Add Program ...`

Browse and select `<OV InstallDir>/bin/ovbbccb.exe`

d. Click `OK`.

The `bbcutil -ping <node>` command should now succeed.

NOTE If SNMP trap interception is desired and `SNMP_SESSION_MODE` is set to `NNM_LIBS`, SNMP trap reception must also be enabled in the firewall.

a. Select `<OVO installDir>/lbin/eaagt/opctrapi.exe` in the `Exceptions` tab.

b. Click `OK`.

---

13. **Symptom QXCR1000135982**
Windows Agent Install using an Installation Server Completes Asynchronously

When installing an HTTPS agent to a Windows system by using an installation server, the installation window on the HPOM for UNIX Management Server shows the following output:

```
[...]
PHASE III: (de)-installing Agent Packages to Managed Nodes.
============================================================

---- <Name of target node> ----
```

After this, no progress is visible to the installing user but the installation is actually running in the background. The installation script on the HPOM for UNIX Management Server will eventually either successfully contact the HPOM Agent after being started on the target system or time out.

Solution

Wait until either of these two events occurs. Additionally, you may check the installation progress on the target node by watching for `msiexec` processes or viewing the HPOM Agent installation log file in `%SystemRoot%\Temp\opc_inst.log`.

14. **Symptom QXCR1000135861**
Path Problem in New Shell after Windows Agent Install using an Installation Server

    After installing a Windows agent using an Installation Server, there is a path-related problem when opening a new shell, and none of the HP commands are found.

    During the installation, the system environment is extended by `<InstDir>/bin` and `<InstDir>/bin/OpC`.

    When opening the `Control Panel` -> `System` -> `Advanced` -> `Environment Variables...` these are present for the system variable PATH but due to a Windows problem, the modification of the PATH does not get propagated to other programs.

    To verify this particular behavior, open a new command shell and enter the command:

    ovc

    If this command is found and works normally, everything is OK. If the command is not found, verify the system PATH in the control panel, follow the described workaround and try again.

    Solution

    Open the `Control Panel` -> `System` -> `Advanced` -> `Environment Variables...` and modify the system path to include `<InstDir>/bin` and `<InstDir>/bin/OpC` and click `OK`.

    This will trigger the propagation of the PATH change to other programs. If the HPOM for UNIX path components are already in place, perform some other minor modification, for example, add a semicolon.

15. **Symptom QXCR1000134895**
Unexpected Pop Up Window During HTTPS Agent Installation (opcnode -timestamp)

    After distributing a new agent to a remote machine, a message window displays the following message:

    `The configuration of the Node Bank has changed. Please restart your session.`

    Solution

    This message can be safely ignored. There are no changes in the `Node Bank` to refresh.

16. **Symptom QXCR1000131758 and 1000132001**
Manual Installation of HTTPS Agents: Agent is not Activated if HPOM for UNIX Management Server is not Reachable

    During manual agent installation, the following lines are displayed:

    ```
    NOTE:    Starting opcactivate utility
    ERROR:   Server ... and/or BBC CB on server not reachable
    ```

Solution

The management server to which the agent should report must be running when making either of the following calls:

- `opc_inst -s <mgmt server>`
- `opcactivate -s <mgmt server>`

17. **Symptom QXCR1000139502**
Problems While Running the OS-SPI Service Discovery on Non-Root Agents

The directory `/var/opt/OV/SPISvcDisc` is not present when a SPI is distributed to the agent and, as a result, the permissions of this directory are not changed when `ovswitchuser.sh` is called. This can cause problems while running the SPI Service Discovery on non root https agents.

Solution

A script is provided to solve this problem and must be called before `ovswitchuser.sh` is used to change the user under which the HTTPS agent runs. Before `ovswitchuser.sh` is called on an HP-UX, Solaris or Linux HTTPS managed node, enter the command:

`/var/opt/OV/bin/instrumentation/ovcreatedirs.sh`

It is not necessary to call that script more than once on a node, even when `ovswitchuser.sh` is used to subsequently switch the agent to another user.

18. **Symptom QXCR1000136922**
Agent Installation Fails on Turbolinux ES 8J

Agent installation fails on Turbolinux ES 8J systems because only manual installation is supported.

Solution

Copy packages, package descriptors, and the `opc_inst` script to the managed node.

Execute the following commands:

`chmod +x opc_inst`
`opc_inst -s <mgmt_server>`

`HPOvXpl` package is installed but postinstall script fails.

`opc_inst -s <mgmt_server>`

`HPOvCtrl` package is installed but postinstall script fails.

`cp <inst_dir>/HPOvCtrl.xml /var/opt/OV/installation/inventor`

`opc_inst -s <mgmt_server>`

19. **Symptom QXCR1000103186**
Error OpC60-800 Displayed After Agent Deinstallation Using Motif GUI

After deinstallation of an agent from the Motif GUI, the following error message maybe displayed:

`Can't deinstall Agent Software on Node <node> (OpC60-0800)`

Solution

Provided that no other errors were reported during deinstallation, this message can safely be ignored.

20. **Symptom QXCR1000133707**
Removing Physical Nodes from Virtual Node Does Not Remove Its Policies

When removing a node from the list of physical nodes belonging to a virtual node, the policies assigned to the virtual node are not removed with the next deployment to the virtual node. After removing the physical node from this list, information about the linked (virtual) policies in the database is also removed from the configuration stored on the management server, but requires an explicit deployment to the physical node.

Solution

You must redistribute the policies to the physical node itself to enforce an update of all policies on the managed node.

21. **Symptom QXCR1000103060**
Agent Upgrade or Patch Installation and Deinstallation

Agent upgrade (patch installation) and deinstallation is performed using the deployment component and no password is required. As a result, when HP Operations Manager core components are stopped during deinstallation or when upgrading core components, the connection to the remote node is lost.

Agent Deinstallation

It is reported that deinstallation was started, then the connection is lost and status of deinstallation is not known.

Agent Upgrade

If an error is encountered during the upgrade, processes do not start and errors are reported.

Solution

Agent Deinstallation

To check if deinstallation was successful, login to remote node and check the log file:

`$Datadir/log/opc_inst.log`

Agent Upgrade

If an error was reported during upgrade, open the log file `$DataDir/log/opc_inst.log` on the managed node and check whether the packages were correctly installed.

If the packages were properly installed but there was a problem with the starting of components, try to start the processes with the command:

`opcagt -start`

Check if all processes were started with the command:

`ovc -status`

If there is a problem with installation of upgraded components, reinstall the agent using the `force` mode.

HTTPS Managed Nodes Runtime

1. **Symptom QXCR1000352852**
   BBC Message Receiver process (opcmsgrb) aborts because it runs out of memory

   Because different threads use different memory arenas, the way threaded programs on the HP-UX allocate memory cause the BBC Message Receiver process (`opcmsgrb`) to grow and eventually abort.

   Solution

   An enhancement has been made to allow the setting of the `_M_ARENA_OPTS` and `_M_SBA_OPTS` configuration variables before starting a controlled process by `ovoareqsdr` and `opcctlm`.

   `opcmsgrb` will use only one memory arena by setting the following:

   ```
   ovconfchg -ovrg server -ns opc.opcmsgrb -set _M_ARENA_OPTS 1:128
   ```

   after which you must restart the server processes.

   For more information about the `_M_ARENA_OPTS` and `_M_SBA_OPTS` configuration variables, refer to the *malloc(3)* manpage.

2. **Symptom QCCR1A57578**
   After executing ovswitchuser, ovcd does not start when OS rebooted

   On Solaris 8 agents, if you set up new users using the administration tools of the operating system, and then run `ovswitchuser` to switch the agent to the new user, the agent processes may not start automatically after the system has been rebooted.

   Solution

   To enable the agent processes to start automatically after rebooting, change the default profile of the user so that the `exit` command is not executed. Alternatively, use `ovconfchg` to set the `RUN_PROFILE` attribute to `false`:

   ```
   ovconfchg -ns ctrl -set RUN_PROFILE false
   ```

3. **Symptom QXCR1000283571**
   Message Browser does not Show Internal Messages

   Internal message filtering does not work if the HPOM Message Interceptor (opcmsgi) is not running.

   Solution

   Check whether the HP process `opcmsgi` is running using the ovstatus(1m) utility. If necessary, restart this service using the following command:

   ```
   ovc -start opcmsgi
   ```

4. **Symptom QXCR1000217165**
   Cannot Change Root Directories After ovswitchuser is Run

   When `ovswitchuser` is run on a UNIX managed node where the `suid-bit` is not set for `ovbbccb` the following error might be entered in the `System.txt` file and the HPOM message browser at each startup of `ovbbccb`:

   ```
   ovbbccb (16577/1): (bbc-188) Cannot change the root directory for the current process.
   See chroot man page for additional detail.
   ```

   Solution

   Enter the following configuration command on any UNIX managed node that exhibits this behavior:

```
ovconfchg -ns bbc.cb -set CHROOT_PATH /
```

5. **Symptom QXCR1000189469**
   opcmsg and opcmon Java API Wrappers do not work on Linux Platforms

   The opcmsg and opcmon Java API wrappers do not work on Linux platforms.

   Solution

   No workaround is currently available.

6. **Symptom QXCR1000103564**
   ovconfd Sends Error Regular Message When Veritas Cluster Server is Down

   `ovconfd` continuously sends error messages when the Veritas Cluster server is down on a cluster node.

   Solution

   a. Create a message interceptor template with a suppress-condition for:

      ```
      application = "OpenView", message group = "OpenView", object = "ovconfd"
      ```

      The message text must contain the string "`(conf-336)`".

   b. Deploy this template to the concerned Veritas cluster node(s).

7. **Symptom QXCR1000197215**
   Applications do Not Work if Executed as opc_op User on Windows

   If applications, for example `Broadcast`, are started under the user `opc_op` on a Windows system, the following error is displayed:

   ```
   Application started, please wait.
   Error: Process could not be started in the specified user account.
   Please check the agent's logfile for more information.
   ```

   The HTTPS Windows agent does not create the `opc_op` user. Recommending administrator is somewhat different, because `opc_op` used to be a non-admin user.

   Solution

   Configure `$AGENT_USER` or administrator or any other existing user account and execute applications on Windows systems under this account.

8. **Symptom QXCR1000138209**
   Control Kills ovconfd if the Initialization Hook Times Out

   On slow or busy systems, `ovconfd` may take longer than 30 seconds to initialize. In such cases it is not possible to start `ovconfd` using `ovctrl` because any processes that `ovctrl` has invoked which do not initialize within the configured time period are killed by `ovctrl`. In such a situation, the HPOM HTTPS agent is NOT started at all. For example, this problem may be experienced if tracing is activated.

   Solution

   Increase the `ACTION_TIMEOUT` parameter of `ctrl.ovcd` namespace in the configuration settings, for example to 120 seconds, with the command:

   ```
   ovconfchg -ns ctrl.ovcd -set ACTION_TIMEOUT 120
   ```

9. **Symptom QXCR1000203203**
   Remote Action Security Rule is Still Provided for Deleted Node Group

   If you delete a node group that is under the control of remote action authorization rules from the `OVO Node Group Bank`, those rules will still applied to the nodes which were in this group.

Remote action authorization rules are defined in the configuration file:

`/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml`

Solution

Do not delete the node group. Only remove nodes from this node group. Now, rules which applied to nodes in this node group will have no effect on the nodes deleted from this node group.

10. **Symptom QXCR1000197467**
ComponentMatrix.cfg & DependenciesMatrix.cfg Contain OvDepl After Deinstalling Agent

    Files `/var/opt/OV/conf/ComponentMatrix.cfg` and `/var/opt/OV/conf/DependencyMatrix.cfg` still contain an entry for `OvDepl` after deinstallation of an HPOM HTTPS agent from the HPOM for UNIX management server system using the Administrator's GUI.

    Solution

    This situation can be safely ignored.

11. **Symptom QXCR1000285220**
coda Daemon Stops on an HTTPS HPOM for UNIX 8.10.160 Agent on AIX 5.1

    The coda daemon stops on an HTTPS HPOM for UNIX 8.10.160 agent on AIX 5.1.

    Solution

    No workaround is currently available.

12. **Symptom QXCR1000284323**
T-Chinese HTTPS Agent on Windows has Wrong Default Charset: UTF-8 Instead of big5

    Traditional Chinese message which is generated by `opcmsg` on an HTTPS agent, on Traditional Chinese Win2003 managed node, is garbled.

    This problem exists for all locales on Windows managed by the HPOM HTTPS agent.

    Solution

    The codeset used by the HPOM HTTPS agent running on the MS Windows managed node must be adjusted adequately to the HPOM for UNIX management server charset. Perform the following:

    a. Change `OPC_NODE_CHARSET` to `big5` using the `ovconfchg` command-line tool:

       ```
       ovconfchg -ns eaagt -set OPC_NODE_CHARSET big5
       ```

    b. Restart the agent using the following commands:

       ```
       opcagt -stop
       opcagt -start
       ```

HTTPS Managed Nodes and Proxies

1. **Symptom QXCR1000133276**
   Change in ovconf: PROXY Setting is Not Processed without Restart

   Changing of PROXY settings takes no effect on the management server system or on a managed node system.

   Solution

   If you changed the PROXY configuration settings, all processes must be restarted with the following commands:

   On managed node:
   ```
   ovc -kill
   ovc -start
   ```
   On management server:
   ```
   ovstop ovoacomm
   opcsv -start
   ```

HTTPS Managed Nodes and NAT Environments

1. **Symptom QXCR1000136801**
   NAT (Server IP Address): Windows Agent Installation Hangs

   In a NAT environment (server IP address is translated on agent side) the HTTPS agent installation may hang. This is caused by ftp which is used during installation. The ftp connection to Windows 2000 itself hangs.

   Solution

   Install the HTTPS Agent software manually. It is very likely that FTP does not work, so another file transport mechanism must be used.

2. **Symptom QXCR1000136802**
   NAT (Node IP Address): Broadcast Application does Not Start on HP-UX Agent

   In a NAT Environment (node system IP addresses translated on the HPOM for UNIX management server side), the execution of applications and actions may immediately return a communication error.

   Solution

   Check if the corresponding agent is reachable using `ping` and other commands. For help on how to do this, refer to *Troubleshooting HTTPS-based Communication* in the *HPOM HTTPS Agent Concepts and Configuration Guide*.

   If it is reachable the communication error message is obviously wrong. Restart the server processes and retry.

   This behavior is seen very infrequently after adding and installing a Node in an NAT environment. If an application can be executed, the error message will not be displayed again, as long as the agent remains reachable.

Embedded Performance Component (EPC, also known as CODA)

1. **Symptom QXCR1000139054**
   HP Performance 4.05 and HP Reporter 3.5 Require that EPC Runs in HTTP Mode

   If the Embedded Performance Component (EPC) is configured to use the HTTPS protocol, HP Performance Manager 4.05 (HPPM) and HP Reporter 3.5 (HP Reporter) fail to make a connection to the Embedded Performance Component on HPOM HTTPS agents and are unable to collect performance metrics.

   However, these applications can connect to and collect performance metrics, if the Embedded Performance Component is configured to use the HTTP protocol.

   To determine if the EPC is configured to use the HTTP protocol or the HTTPS protocol, run the command:

   <OV_DIR>/bin/ovconfget coda SSL_SECURITY

   where <OV_DIR> is the directory where EPC is installed.

   If the output is ALL or REMOTE, then EPC is configured to use the HTTPS protocol.

   If the output is NONE, then EPC is configured to use the HTTP protocol.

   Solution

   To configure EPC to use the HTTP protocol, run the command:

   <OV_DIR>/bin/ovconfchg -ns coda -set SSL_SECURITY NONE

Deployable Performance Agent (HPPA)

1. **Symptom QXCR1000385683**
   All server processes should be restarted after HP Performance Agent is installed on a local node

   The agent starts buffering messages if all server processes are not restarted after the HP Performance Agent is installed on the local node.

   Solution

   You must restart all server processes after you install the HP Performance Agent on the local node. Run the `ovstop` and `ovstart` commands.

2. **Symptom QXCR1000280832**
   HP Performance Agent Processes not Running after the Installation on HP-UX 11.23 Itanium Node

   After installing HPOM for UNIX on HP-UX 11.23 Itanium nodes, the HP Performance Agent processes are not running.

   Solution

   Stop and restart the processes using the following commands:

   ```
   mwa stop
   ```

   ```
   mwa start
   ```

3. **Symptom QXCR1000314580**
   Deployment of HP Performance Agent fails on HPOM for UNIX 8.21

   Deployment of HP Performance Agent/HP-UX C.04.50.00 from a 8.21 HPOM for UNIX Management Server fails if higher versions of shared components (HPOvLcore.*, HPOvPerf.*) are already installed on the node.

   Solution

   As a higher version of shared components are already installed on the node, HP Performance Agent installation will complete, although the deployment reports that a failure has occurred. HP Performance Agent will not be running on the node after the deployment.

   To start the HP Performance Agent on node, execute the following command

   ```
   /opt/perf/bin/ovpa start
   ```

HP Performance Manager (PM)

1. **Symptom QXCR1000743584**
   HP Performance Manager 8.00 does not work after the HPOM for UNIX server deinstallation

   If HP Performance Manager 8.00 and HP Operations Manager for UNIX 8 are installed on the same system and if HP Operations Manager for UNIX is deinstalled using the `ovoremove` script, HP Performance Manager 8.00 stops working.

   Solution

   To resolve the issue, do the following:

   a. Copy all the contents of the `/var/opt/OV/shared/server/conf/perf` directory to a temporary location.

   b. Deinstall HP Operations Manager for UNIX by using the `ovoremove` script.

   c. Run the following command:

      `/opt/OV/lbin/xpl/ovinit.sh -dependencies OvGC -ovrg server`

   d. Copy the backed-up contents to the following location:

      `/var/opt/OV/shared/server/conf/perf`

2. **Symptom QXCR1000247176**
   After HP Performance 5.0 Deinstallation Core Agent Processes are Stopped

   After HP Performance deinstallation from HPOM for UNIX management server node, the local HPOM agent is stopped.

   The following is displayed when entering **`ovc -status`**:

   ```
   (ctrl-111) Ovcd is not yet started.
   ```

   Solution

   After HP Performance deinstallation start all Core Agent processes including local agent manually by entering:

   ```
   ovc -start
   ```

Motif UI

1. **Symptom QXCR1000413545, QXCR1000373878**
   If Oracle 10.2.0.2 is used as a database, the GUI cannot be opened by a non-root user

   If Oracle 10.2.0.2 is used as a database for HPOM 8.X server, non-root users cannot open the HPOM GUI, except for the `oracle` user.

   Solution

   Execute the following command to solve this problem:

   ```
   chmod a+rX $ORACLE_HOME
   ```

2. **Symptom QXCR1000136788**
   Changing IP Address Of Node Creates Errors When Starting Applications

   When a node in the Node Bank is changed to use a different IP-Address or Node Name, an error occurs when starting an application on that node using the Motif GUI. The error is:

   `Unable to get node information of <oldnodename>.`

   Solution

   Apply one of the following workarounds:

   - Do not use the `Modify Node` window to change the IP-Address or the node name of a node. Delete the node and add a new one instead.
   - When the IP-Address or the node name has been changed using the `Modify Node` window, restart the Motif GUI.

3. **Symptom QXCR1000144554 & QXCR1000211752**
   English OVw Starts When Starting OVw in X-OVw Application Group

   When starting the `Start OVw` application from the `X-OVw` application group, OVw is always started in locale C (English) even on a Japanese, Simplified Chinese or Korean system.

   Solution

   If you always want to start OVw in a language other than English, you can modify the `Start Ovw` application as follows:

   a. Right click the application symbol and select `Modify`.

   b. In the `Application Call` edit text, at the very beginning, add the required `LANG`:

HP-UX	Japanese:	**`LANG=ja_JP.SJIS`**
	Simplified Chinese:	**`LANG=zh_CN.hp15CN`**
	Korean:	**`LANG=ko_KR.eucKR`**
Solaris	Japanese:	**`LANG=ja_JP.PCK`**
	Simplified Chinese:	**`LANG=zh_CN.EUC`**
	Korean:	**`LANG=ko_KR.EUC`**

   c. Insert a space after the `LANG=*` entry and before `opcctrlovw`.

4. **Symptom QXCR1000139221**
   NNM-ET View Application IPv6 Network

Applications in application group `NNM-ET Views` do not work and a Java error message is displayed. Some of the NNM-ET views require additional configuration to work correctly.

Solution

For NNM-ET applications to work, you must run the `NNM-ET` setup script to enable NNM-ET on the management server system.

For more details on NNM Extended Topology and how to enable it, refer to the NNM release notes under:

`/opt/OV/www/htdocs/<language>/ReleaseNotes`

5. **Symptom QXCR1000113589**
   XmScrollBar Warning Opening Message Detail Window for Long Messages

   When a message detailed window containing a long message text is opened, a Motif warning message of the following form is displayed in the terminal window:

   ```
   &#129;@[W: X Toolkit Warning:
   \012
   Name: HorScrollBar\012
   Class: XmScrollBar\012
   The specified scrollbar value is greater than the maximum\012 scrollbar value minus the
   scrollbar slider size.\012].
   ```

   Solution

   This warning message can be safely ignored.

6. **Symptom QXCR1000287652**
   No Error Message if Templates are Distributed to the HTTPS Managed Node without Agent Installed

   No error message appear in the Motif GUI and neither in the `System.txt` file if templates are distributed to the HTTPS managed node without agent installed.

   Solution

   Make sure you first install HPOM for UNIX HTTPS agent on the managed node before you distribute templates or instrumentation to it.

7. **Symptom QXCR1000285182**
   MIB Application Builder Creates an Application on the HPOM for UNIX Management Server

   MIB Application Builder adds or creates an application on the HPOM for UNIX Management Server local node instead on the selected node.
   This happens with both Motif and Java UI.

   Solution

   No workaround is currently available.

Java UI

1. **Symptom QCCR1A94554**
   New Java GUI cannot read the old itoopbrw file (Version 3.0) correctly

   Because of the incompatibility, the new Java GUI cannot read the old `itoopbrw` file (Version 3.0) correctly.

   Solution

   For the `itoopbrw` file to be compatible with the new Java GUI, follow these steps:

   a. Change the version of the `itoopbrw` file from Version 3.0 to Version 4.0.

   b. Make sure that you use the double quotation marks with the filter names. For example, change `NAME:first filter` to `NAME:"first filter"`.

2. **Symptom QCCR1A91247**
   Some HPDMA tools do not run from the Java GUI

   Some HPDMA tools do not run when started from the Java GUI running as an application.

   Solution

   To ensure that the applets are correctly run from within the Java GUI, start the Java GUI as an applet.

3. **Symptom QCCR1A57494**
   Java GUI exits because it runs out of memory

   If the filtered history browser returns a lot of messages, the Java GUI exits because it runs out of memory.

   Solution

   To avoid this problem, increase the Java VM heap memory in the `ito_op.bat` file (if installed at the default location: `C:\Program Files\Hewlett-Packard\HP OVO Java Console\ito_op.bat`).

   For example, to change the Java VM heap memory from 128 MB to 512 MB, change the `%START% .\j2re1.4.2\bin\%JAVA% -Xmx128m com.hp.ov.it.ui.OvEmbApplet ...` line to the following:

   ```
   %START% .\j2re1.4.2\bin\%JAVA% -Xmx512m com.hp.ov.it.ui.OvEmbApplet ...
   ```

4. **Symptom QCCR1A58506**
   When a new node is added to the node layout group, the filter on the node layout group in the Java GUI is not updated

   If a filter is created in the Java GUI based on a node layout group, and a new node is added to the node layout group, the filter is not automatically updated to include the newly added node.

   Solution

   This is the intended behavior.

5. **Symptom QCCR1A58284**
   java.io.EOFException error message is displayed when exiting Java GUI

   When exiting the Java GUI, the following error message is displayed:

   ```
   ERROR MSG, 3:15:56 PM, com.hp.ov.it.ui.OvEmbApplet: java.io.EOFException
   There was a problem closing the communication link to the server.
   ```

   Solution

   This error message can be safely ignored.

6. **Symptom QXCR1000364133**
   Applet on JRE Version 1.5: JLabel and Separator Items Missing in the Popup Menus

   Note that JLabel and separator items are removed from the top of popup menus when you run an applet on JRE version 1.5:

   - in the Status Calculation popup in service graphs
   - in the Object pane (services)
   - in service graphs (on icons and zoom settings)
   - in the Navigation panel

7. **Symptom QXCR1000443919**
   Only service names are shown in the Message Browser

   The Java GUI Message Browser shows only service names, but it should also show service labels.

   Solution

   The Java GUI message structure was extended with the Service Label attribute.

   Note that service labels are empty by default. To enable the loading of labels, select the **Show Service Label in Messages** checkbox of the Services tab in the Preferences window.

NOTE If the Service Load on Demand (SLOD) feature is enabled, only the service labels of the loaded services are shown.

If the Service Load on Demand caching is enabled, deleting a service results in the service label disappearance.

---

8. **Symptom QXCR1000103169**
   Escalated Messages with CMAs not Displayed

   Escalated messages with added custom message attributes are not displayed in the message properties in the Java GUI.

   Solution

   Currently, CMAs cannot be escalated yet.

9. **Symptom QXCR1000226646**
   Internet Explorer stops responding when logging off with JRE 1.5

   The Java GUI applet may cause Internet Explorer web browser to stop responding when exiting or logging off and using Java Runtime Environment (JRE) version 1.5.

   Solution:

   Disable caching of downloaded content for the Java plugin. In the `Java Plug-in Control Panel` click the `Settings` button in the `Temporary Internet Files` section of the `General` tab. In the `Temporary Files Settings` dialog window, click the `View Applets` button. In the lower right corner of the `Java Applet Cache Viewer` dialog window, clear the `Enable Caching` check box.

10. **Symptom QXCR1000199105**
    Issues starting two Java UI applets in two Mozilla web browsers on Windows

    Two Java UI applets cannot be started on the same machine within two Mozilla web browsers.

    Solution:

When each Mozilla web browser uses its own profile, it is possible to use two Java UI applets on the same machine within two Mozilla web browsers. To allow Mozilla to start with a different profile, set the environment variable using the following command:

```
set MOZ_NO_REMOTE=1
```

To add a new profile, start mozilla with the following command:

```
mozilla.exe -p
```

11. **Symptom QXCR1000286980**
Cannot start Java UI on HPOM for UNIX 8.20 Management Server

Java GUI on HPOM for UNIX 8.20 server on Itanium does not run with the default JRE version installed. The following error is displayed in the console window:

```
Error: could not find libjav.sl
Error: could not find Java 2 Runtime Environment
```

Solution

Install the supported Java Runtime Environment from the following location:

```
http://www.hp.com/products1/unix/java/
```

Specify the location of the directory where you have JRE installed using the *JAVA_DIR* environment variable. For example:

```
export JAVA_DIR=/opt/java1.4/jre
```

12. **Symptom QXCR1000211752 & QXCR1000144554**
The Interface Traffic Net Activity Tool Cannot be Started from the Java UI

When running NNM tools from the Java GUI, some characters may be garbled When running NNM tools from Java GUI, characters are garbled or are launched in English on Japanese, Korean or S-Chinese management servers.

Solution

The `LANG` environment variable should be added to the operator (`opc_op`) profile. For example, on a Japanese management server, Add the following `LANG` environment statement appropriate to the operating system of your management server in the `opc_op .profile` file:

HP-UX	Japanese:	**LANG=ja_JP.SJIS**
	Simplified Chinese:	**LANG=zh_CN.hp15CN**
	Korean:	**LANG=ko_KR.eucKR**
Solaris	Japanese:	**LANG=ja_JP.PCK**
	Simplified Chinese:	**LANG=zh_CN.EUC**
	Korean:	**LANG=ko_KR.EUC**

13. **Symptom QXCR1000197155**
Example XML File for Non-English Environments (opcservice)

To successfully upload the service definition file, you need to specify the correct encoding in the header of the xml definition file. It is currently not documented in the manuals how to write multi-byte service definition files. An example is given in the solution below.

Solution

Here are the examples how the header should look like for different languages.

Japanese `<?xml version="1.0" encoding="Shift_JIS"?>`

Korean	`<?xml version="1.0" encoding="EUC-KR"?>`
Simplified Chinese	`<?xml version="1.0" encoding="GB2312"?>`

For further information, refer to the chapter titled *The Service Configuration File Syntax* in the *HP Service Navigator Concepts and Configuration Guide*.

Example

A complete XML file for Korean:

```
<?xml version="1.0" encoding="EUC-KR"?>
<!-- this file was generated by opcsvcconv(1m) -->
<Services xmlns="http://www.hp.com/OV/opcsvc"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.hp.com/OV/opcsvc /etc/opt/OV/share/conf/OpC/mgmt_
sv/dtds/service.xsd">
<Service>
<Name>localsvc</Name>
<Label>Some Korean text</Label>
</Service>
</Services>
<!-- end of file -->
```

14. **Symptom QXCR1000237264**
When Exiting or Logging off from the HPOM for UNIX Java UI, an Error Message is Displayed

When Java UI is running in the HTTPS communication mode, the following error message is displayed, when exiting or logging off from Java UI:

```
ERROR MSG, 7:42:47 AM,
com.hp.ov.it.comm.OvEmbHttpsClient:
https status - InternalServerError:text/html,
Message = HTTP/1.1 500 Internal Server Error
Date: Wed, 11 May 2005 05:41:57 GMT
Transfer-Encoding: chunked
Server: BBC 05.20.010; opcuihttps 01.00.000
senderid: e6979118-aca1-750b-1f6a-de6eb9cfe391
Cache-Control: no-cache
Content-Type: text/html
```

Solution

This message can be safely ignored.

15. **Symptom QXCR1000309412**
Exceptions in the Java GUI Console Window

Sometimes the following exception is shown in the console window of the Java UI:

```
javlang.ClassCastException
at com.klg.jclass.chart.BarChartDraw.recalc(BarChartDraw.java:95)
at com.klg.jclass.chart.JCChartArecalcGraphExtents(JCChartArejava:2376)
at com.klg.jclass.chart.JCChartArerecalc(JCChartArejava:1124)
at com.klg.jclass.chart.JCChartAresetBounds(JCChartArejava:1266)
```

```
at com.klg.jclass.util.DefaultComponentLayout.layoutContainer(DefaultComponentLayout.java:59 4)
at javawt.Container.layout(Container.java:1020)
at javawt.Container.doLayout(Container.java:1010)
at com.klg.jclass.chart.JCChart.performLayout(JCChart.java:843)
at com.klg.jclass.chart.JCChart.doLayout(JCChart.java:785)
at javawt.Container.validateTree(Container.java:1092)
at javawt.Container.validateTree(Container.java:1099)
at javawt.Container.validateTree(Container.java:1099)
...
```

Solution

This exception can be safely ignored.

16. **Symptom QXCR100097658**
Msg Time Info In WebStart Java GUI in users PC TZ & not TZ specified in cfg

A property "user.timezone" was considered by the JNLP spec section 4.2 as "unsafe", so it could not be used by the Web Start. Because of this, administrators could not force operators to start Java GUI in the preferred time zone.

As a workaround, a new input argument was introduced: timezone. It was used to overwrite the default time zone of JVM, which is inherited from the OS. However, it turned out that this workaround is not effective if you started Java GUI using the UNIX command-line tool `ito_op`.

Solution

Make sure you start Java GUI using one of the following: `ito_op.bat`, `ito_op_applet.html` or `ito_op_ws.jnlp` (Web Start).

ECS/HP Composer

1. **Symptom QXCM1000413975**
   Limited Support of Asynchronous Callbacks Defined in Correlator Circuits

   Asynchronous function callbacks for the annotate node of the correlator circuits, which can be configured in the HP Composer UI in the Variables Definition tab, are only supported by HPOM if they are configured as type “string”.

   Solution

   HPOM default annotation server will execute the specified string as a corresponding command line call and will return the standard output as result. For all other data types, an error will be returned. There are no plans to support other asynchronous function calls except of type “string”.

2. **Symptom QXCR1000140462 and QXCR1000131660**
   Disabling the Event Correlation Template does not Stop Event Correlation

   Event correlation is still working even if all event correlation templates are disabled.

   Solution

   Stop HPOM Event Correlation (`opceca`) manually with the following command:

   ```
   ovc -stop opceca
   ```

Reporting

1. **Symptom QXCR1000138530**
   Service History Status Reports (SN Report Pack) Limit ID and Name Length

   With HPOM for UNIX 8, it is possible to specify service names or service labels that exceed 253 characters in length. Problems occur with these long names since the Crystal runtime engine used in Reporter 03.50 has a limitation for string lengths of 254 characters. The HPOM for UNIX Service Status History reports Version 03.50 do not support service names or service labels that are longer than 253 characters.

   If service names exceed the 253 character limit, the name is truncated. The status history data may be incorrectly calculated if the service names are not unique within the first 253 characters.

   Solution

   Do not use service names that are longer than 253 characters. The support for service names longer than 253 characters has been added to the HP Reporter 03.60 release, and the corresponding Service Navigator Report Package.

2. **Symptom QXCR1000328562**
   itochecker fails to create all reports if independent database server system is configured

   `itochecker` fails to create a full report on the HPOM server if an independent database server system is set. The following reports are missing:

   - Database Check
   - OVO Database Check
   - Nodes Check
   - Java GUI / Service Navigator

   Solution

   To solve this problem, do as follows:

   a. Add the following line to `/etc/opt/OV/share/conf/ovdbconf`:

      ```
      REMOTE_DB 1
      ```

   b. Run `itochecker` again.

Network Node Manager

For Network Node Manager specific problems, refer to the HP Operations Network Node Manager 7.5 Runtime Release Notes appropriate for your operating system:

`http://h20230.www2.hp.com/selfsolve/manuals`

WARNING **By default, the file:**
`OVNNMgr.OVNNM-RUN: /opt/OV/bin/ovtraceroute`

has the `setuid` bit set for root:
`-r-sr-xr-x 1 root bin`

Security concerned customers should change the permissions as follows:

`chmod 555 /opt/OV/bin/ovtraceroute`

---

1. **Symptom QXCR1000295810 and QXCR1000295800**
   Inappropriate Entries in /etc/services for ito-e-gui in NIS+ Environments

   If the `ito-e-gui` service is managed by NIS+, the service should not be listed in `/etc/services`.

   You can check if the ito-e-gui service is managed by NIS+ using the following command:

   `niscat services.org_dir | grep  ito-e-gui`

   Solution

   If the `ito-e-gui` service is managed NIS+, remove ito-e-gui service configuration line from `/etc/services`. The following is an example of the configuration line that should be removed:

   ```
   ito-e-gui       2531/tcp        # OpenView Operations Java Console
   ```

2. **Symptom QXCR1000297690**
   HPOM for UNIX Management Server cannot be Started

   After shutting down the management server you may not be able to start it again.

   Solution

   The system shutdown sequence is missing a link to `/sbin/rc2.d/` for the NNM and HPOM for UNIX processes.

   Create a link manually before shutting down your system using the following command:

   `ln -s /sbin/init.d/ov500 /sbin/rc2.d/K060ov500`

3. **Symptom QXCR1000217223**
   NNM license key Installation Using ovnnmInstallLic is not Documented

   NNM license key installation using the `ovnnmInstallLic` tool not documented.

   Solution

   A second, NNM, license key must be installed using the NNM license key installation tool `ovnnmInstallLic`, otherwise is this license key ignored and not installed.

   Use the following command to add NNM license passwords:

   `/opt/OV/bin/ovnnmInstallLic /tmp/save710/.license`

4. **Symptom QXCR1000205834**
   X-OVw Requires a Home Directory that may not Exist

   After successfully installing NNM 7.5, an HPOM HTTPS agent, and the HPOM for UNIX 8.1x Remote NNM package on an HP-UX system, opcctrlovw runs correctly.

   However, when attempting to run the X-OVw application `Start OVw`, the following error message is displayed:

   ```
   Warning opcacta (Action Agent) (22960 : Cannot change the current working directory to
   /home/opc_op for user opc_op.
   No such file or directory (OpC20-53)
   ```

   At this point, `/home/opc_op` does not exist.

   Solution

   To correct the problem, create the directory `/home/opc_op`.

5. **Symptom QXCR1000206586**
   Applications Using opcctrlovw are hard to use with Windows Java GUI

   Applications, such as Net Activity, sometimes do not start in the Windows Java GUI, when using `opcctrlovw`. Instead, error messages are printed in HPOM Communication Status window.

   Solution

   When the HPOM Java GUI is run on a Windows system, these error messages are sometimes displayed when some applications are started. The applications that may trigger this problem are those that display an ovw session to the Windows box.

   Error Message 1

   ```
   Command: opcctrlovw -display 15.2.118.164:0.0 -user "opc_adm" -action "IP Tables"
   AddressesForIface" produced the following output error:
   Error:  Can't open display: <IP Address>:0.0
   with Exit Code: 3
   ```

   Solution 1:

   An X-Windows emulator such as Reflection X or Hummingbird Exceed must be running on the Windows system.

   Error Message 2

   ```
   INTERNAL ERROR at: CWfong.cpp:264.
   Contact your HP Support representative.
   Could not conver "-*-*-medium-f-normal-*-12-*-*-*-*-m-*-*-*" to XFontSet.
   Try changing your "*.cwFont" resource.
   ```

   Solution 2

   The X-Windows emulator is not able to find the correct font. In this case you need to configure a font server, for example, on the HPOM for UNIX Management Server: xfs -port 7100 and then configured Reflection X to use this font server.

6. **Symptom QXCR1000196492**
   HA Environments should be in Maintenance Mode when setupExtTopo.ovpl is Run

   If you run `setupExtTopo.ovpl` to enable ET in a high availability environment, there is a possibility that some monitored processes could be restarted, triggering a failover.

When performing actions on an HPOM for UNIX management server installed in a cluster environment that result in the stopping of HPOM for UNIX management server processes, for example when installing patches, upgrading, or doing maintenance, it is necessary to first disable the HPOM for UNIX management server HA resource group and stop the HPOM for UNIX management server.

Solution

Switch the HA system to maintenance mode before running `setupExtTopo.ovpl`.

How to switch the HPOM for UNIX management server to and from maintenance mode is described in the section titled *Stopping the HPOM Management Server in a Cluster Environment for Maintenance* for the appropriate cluster type in the *HPOM Installation Guide for the Management Server*. This section describes how the HPOM for UNIX management server can be stopped without causing failover of the HPOM for UNIX management server HA resource group.

When this script has run successfully, start the HPOM for UNIX management server and check that the HPOM for UNIX processes are up and running, and then enable HPOM for UNIX management server monitoring.

7. **Symptom QXCR1000193099**
   Ovcd is not yet Started Message after installing NNM on System with HTTPS Agent

   If NNM 7.5 is installed on a UNIX system where an HPOM HTTPS agent is running, the `ovcd` process is stopped.

   Entering the command `opcagt -status` results in the following error message being displayed:

   ```
   Ctrl-1111 Ovcd is not yet started.
   ```

   Solution

   Enter the following command to restart the agent:

   ```
   opcagt -start
   ```

8. **Symptom QXCR1000188382**
   OSPF View in NNM-ET Views Stops Working if RAMS is Enabled

   RAMS functionality is supported with NNM 7.5, and can be easily enabled or disabled.

   When RAMS is disabled, the application call for OSPF View NNM-ET Views is:

   ```
   http://<$OPC_MGMTSV>:7510/topology/ospfView?viewInBrowser=true
   ```

   In this case, application OSPF View works correctly.

   If RAMS is enabled, OSPF View stops working because the following application call is still used:

   ```
   http://<$OPC_MGMTSV>:7510/topology/ospfView?viewInBrowser=true
   ```

   Solution

   If RAMS is enabled, modify the application and change the application call for OSPF View NNM-ET Views to:

   ```
   http://<$OPC_MGMTSV>:7510/topology/rexView?viewInBrowser=true
   ```

9. **Symptom QXCR1000187416**
   Net Activity/Network Polling requires HP Software Services/MIB Grapher

   When creating new user or using `opc_op`, and assigning the `Net Activity` application group, the `MIB Grapher` must also be assigned from `OV Services`. If this is not assigned, the following error is displayed next time you log on to the Motif GUI as the new user or as `opc_op`:

```
Error: Application "Network Monitor Statistics": parent "mibgraph" undefined.
Error: Application "mibgraph" undefined.
```

```
OpC-0830
Application(s) in the Application Desktop may not be started because application
Network Monitor Statistics is not registered.
```

When selecting `Net Activity` -> `Network Polling`, the following error is displayed:

```
OpC60-010
OVw Error with OVwCheckAction(netmonStatus): Application not found.
```

A related error is also displayed in the HPOM Error Information window.

Solution

Assign the `OV Services` group, or at least the `MIB Grapher` application, in addition to `Net Activity` to the `opc_op` user or when creating a new user.

10. **Symptom QXCR1000211829**
Applications in Jovw (old) Group may Fail

When trying to start applications such as `Highlight In IPMap` and `Jovw` from the `Jovw` (old) group in the Application Bank window, error messages are displayed:

Highlight In IPMap error:

```
Cannot find an ovw on host <hostname> with map named default using session ID
<hostname>:0.
```

Jovw error:

```
Cannot find an ovw on host <hostname> with map named default using session ID
<hostname>:0.
```

Solution

In order for these applications to work, an ovw session with the default map must be running on the host.

On the system *<hostname>* enter the command:

`/opt/OV/bin/ovw`

Make sure that `default` is displayed in the lower left corner.

To change to the default map, choose `Map` -> `Open` and select `default`.

It is recommended that NNM Dynamic Views be used rather than Jovw. The NNM Dynamic Views are available from the application group `NNM Views`.

11. **Symptom QXCR1000213132**
Wrong Japanese Name for [OV Extended Topology] Tool

The `OV Extended Topology` tool in the `OV Services` application group is labeled `Node View` in a Japanese environment, resulting in two `Node View` tool icons in this application group.

Solution

Open the Modify window of the application with the incorrect label and enter the correct name.

12. **Symptom QXCR1000209866**
The Interface Traffic Net Activity Tool Cannot be Started from the Java UI

The Net Activity tool `Interface Traffic` does not work when started directly from the Java UI.

Solution

You can start an NNM dynamic view, for example, a `Neighbor` view, and select a node in that view. The `Interface Traffic` tool is available under the menu options:

```
Performance -> Network Activity
```

The `Interface Traffic` tool can also be started from the Internet submap or from the Application Bank in the Motif UI, again using the menu options:

```
Performance -> Network Activity
```

13. **Symptom QXCR1000200666**
ovuispmd Fails to Start if Port 7777 is Already in Use

The `ovuispmd` process may fail to start if it is not able to use the port 7777.

The following error messages may be displayed:

```
ovuispmd FILED to start.
Unable to get port 7777.
Address already in use.
```

Solution

Restart the system. All NNM processes, including `ovuispmd`, should now be running.

Network Diagnosis Add-On Module

CAUTION For a complete list of NDAOM-related problems, refer to the NDAOM Release Notes document.

NDAOM

Tracing is centrally controlled by the `ndaom.cfg` configuration file present under the location:

`/etc/opt/OV/ndaom/conf/ndaom.cfg`

Trace areas are defined for bigger modules, such as the `ovnwlinkmon` or the `ovnwmonitor`. These modules read the configuration file, check whether tracing is enabled and whether the trace area is set.

Trace areas are: `ovnwmonitor`, `ovnwlinkmon`, `ALL`.

Trace levels are : `0 – 9` with increasing order of trace information.

NDAOM trace can be enabled by adding the following lines in `ndaom.cfg` file:

```
TRACE_AREA=[ovnwmonitor|ovnwlinkmon]
TRACE_LEVEL=[0 – 9]
```

NDAOM trace information file `ndaom.trc` can be found on the management server at:

`/var/opt/OV/ndaom/log`

Problem Diagnosis Probe

Tips for working with the Problem Diagnosis Probe:

- If the GUI applet is not working, check the java console for exceptions.
- If `pd central` will not start by using `ovstart`, try using `ovstop pd`, then running the PD manually with the command:

  `pdcentral.sh -start` or **`pdcentral.bat -start`**

  Also, try an `ovstop` then `ovstart` on UNIX systems for the `ovspmd` problem.
- Use `<DEBUG>true</DEBUG>` in the `pdconfig.xml` file to generate debug output in the `pd.log` file. This option should only be used briefly because it can generate large amounts of data.
- To verify that the probe is running and responding properly, use the command:

  `http://probe_name:8067/netpath/netpath.req?destination=sometarget` .
- To verify that the central application is running and responding properly, use the command:

  `http://nnmserver:8068/central/central.req?destination=probe_name|sometarget`
- To see the L2 data being returned by ET for an IP address pair, use the command:

  `http://nnmserver:7510/topology/NMTopoApi?api=getL2BetweenNodes&begin=ipaddress&end=ipaddress`
- To get a UI that allows SQL queries on the PD databases, use the commands:

  `pdcentral.sh -dbmgr` or **`pdcentral.bat -dbmgr`**

Tracing and Troubleshooting

1. **Symptom QXCR1000133724**
   TraceMon Cannot be Used on DHCP or NAT Nodes to Access Trace Server

   The TraceMon GUI on a system using DHCP or NAT cannot connect to a Trace Server if there is no name resolution of the GUI station possible.

   The Trace Server attempts to verify the validity of the connection request from the TraceMon GUI system by checking the name with DNS. If it cannot be resolved, the connection is refused.

   Solution

   Configure Trace Server to write to a file and copy the file to the TraceMon System.

Localization

1. **Symptom QXCR1000398226**
   Manager to manager forwarding of characters with the ASCII code does not work

   If characters with the ASCII code, for example Ä, are used in a text field of the HPOM message, the message is displayed correctly on the first manager. But after forwarding it to the second manager, the message is corrupted.

   Solution

   Restart HPOM in a different locale by executing the following commands:

   ```
   ovstop
   export LANG=C.iso885915
   ovstart
   ```

2. **Symptom QXCR1000214400**
   New Menu Items in Java GUI are in English Only

   Some new functionalities introduced with newer versions of JavaGUI come with new menu entries but they are all in english only.

   Solution

   These will be translated with a future update of HPOM for UNIX.

3. **Symptom QXCR1000190998**
   Input/Output and Virtual Terminal Applications Show Garbled Text

   On Spanish, Japanese, Simplified Chinese or Korean management servers, Input/Output and Virtual Terminal applications show garbled text instead of correct non-ASCII characters.

   Solution

   `xterm` and `hpterm` are not able to display non-ASCII characters, so for Input/Output and Virtual Terminal applications for the aforementioned languages, you must use `dtterm`. You may want to set `dtterm` as the default for those platforms where you want to use Input/Output and Virtual Terminal applications.

   To do this:

   a. Select `[Actions]` -> `[Set Defaults]`.

   b. Open a `Node Bank` window.

   c. In the listbox, select the agent platform for which you want to change the default value.

   d. Click `Advanced Options` and change the setting for `Virtual Terminal Emulator`.

   e. Save your change by clicking `OK`.

   After this change, adding a new node of this platform type will automatically have `Virtual Terminal Emulator` set to `dtterm`. For nodes that you have configured before changing the default, you must change this value manually from the `Advanced Options` for the node.

In addition, the `Character Set` for the agent platform and already configured node must match a locale that is already installed on the node, as listed in Table 5-1 on page 203.

Table 5-1 OM Agent Platform Character Sets and Locales

Agent Platform	Management Server Language	Character Set	Locale
HP-UX	**Japanese**	Shift-JIS	ja_JP.SJIS
		Japanese EUC	ja_JP.eucJP
		UTF-8	ja_JP.utf8
	Spanish	ISO 8859-15	es_ES.iso885915@euro
		UTF-8	es_ES.utf8
	Simplified Chinese	GB-2312	zh_CN.hp15CN
		UTF-8	zh_CN.utf8
	Traditional Chinese	ZHT16BIG5	zh_TW.big5
	Korean	Korean EUC	ko_KR.eucKR
		UTF-8	ko_KR.utf8
Solaris	**Japanese**	Shift-JIS	ja_JP.PCK
		Japanese EUC	ja_JP.eucJP ja japanese
		UTF-8	ja_JP.UTF-8
	Spanish	ISO 8859-15	es.ISO8859-15
		UTF-8	es.UTF-8
	Simplified Chinese	GB-2312	zh_CN.EUC zh.GBK zh_CN.GBK
		UTF-8	zh_CN.UTF-8
	Traditional Chinese	ZHT16BIG5	zh_TW.big5
	Korean	Korean EUC	ko_KR.EUC ko korean
		UTF-8	ko.UTF-8 ko_KR.UTF-8

Table 5-1 OM Agent Platform Character Sets and Locales (Continued)

Agent Platform	Management Server Language	Character Set	Locale
Linux	**Japanese**		
		Japanese EUC	ja_JP.EUC-JP
		UTF-8	ja_JP.UTF-8
	Spanish	ISO 8859-15	es_ES@euro
		UTF-8	es_ES.UTF-8
	Simplified Chinese	GB-2312	zh_CN
		UTF-8	zh_CN.UTF-8
	Traditional Chinese	ZHT16BIG5	zh_TW.big5
	Korean	Korean EUC	ko_KR.EUC-KR
		UTF-8	ko_KR.UTF-8

Japanese Version Issues

1. **Symptom QCCR1A69437**
   Message garbled on HP-UX 11.23 Itanium, RedHat AS 3.0, and Tru64 5.1A

   When running Japanese applications, messages are garbled on HP-UX 11.23 Itanium, RedHat AS 3.0, and Tru64 5.1A managed nodes.

   Solution

   To solve this problem, you must restart the agent in Japanese locales after the installation.

   Export `LANG` and `LC_ALL` to the proper Japanese character set, and then restart the agent by using `ovc -kill` and `ovc -start`.

2. **Symptom QXCR1000293835**
   Message Garbled on Win2003J

   Japanese messages, generated by `opcmsg` are garbled on a Win2003J managed node.

   Solution

   Do the following on the managed node:

   a. Change the `OPC_NODE_CHARSET` to `acp932` using the following command:

   ```
   ovconfchg -ns eaagt -set OPC_NODE_CHARSET acp932
   ```

   b. Restart the agent using the following commands:

   ```
   opcagt -stop
   opcagt -start
   ```

3. **Symptom QXCR1000193802**
   RH9.0 Hangs or Fails to Install Certificates from a Japanese/Korean Management Server

   Agent may be experiencing problems with Japanese locale `ja_JP.eucJP`.

   Solution

   Change default locale to **`ja_JP.utf8`**.

   To verify that locales are set correctly, perform an `rlogin` to the Linux node and execute the command:

   `locale`

   The locale `ja_JP.utf8` should be displayed.

4. **Symptom QXCR1000194960**
   ovc -start Hangs on Linux During Installation

   During the installation of certificates on Linux systems during installation, the ovc -start command hangs. This problem occurs if the locale on the managed node is set to `ja_JP.eucjp`.

   Using the `top` command, it can be seen that the `ovbbccb` process is consuming almost 100% of CPU.

   Solution

   To avoid this problem set `ja_JP.utf8` as a default locale:

   For example, in the `/etc/profile` file, enter the following lines:

   `export LANG=ja_JP.utf8`

```
export LC_ALL=ja_JP.utf8
```

5. **Symptom NSMbb69079**
   Logfile Entry Cannot Be Converted From eucJP to SJIS

   There is `Logfile Characterset` option available in the `Add/Modify Logfile` window. If you have selected a character set that is different from the current locale, the logfile conversion from one character set to another fails and a critical message is displayed in the message browser.

   Solution

   Select `Logfile Characterset` to match the current locale.

6. **Symptom NSMbb68102**
   Japanese Text on Title Bar of Output Window is Unintelligible (hpterm)

   Japanese text on title bar of output window opened by either `Issue Certificate` or Issue `Install Key for Certificate` tool is unintelligible.

   Solution

   Modify HP-UX management server node to use dtterm for Virtual Terminal Emulator.

7. **Symptom QXCR1000137593**
   Cannot Convert String to Type Font Structure Warning Message

   Motif Administrator and Operator GUI: When starting a Motif GUI, some font-related messages may appear on the command line:

   ```
   Warning: cannot convert string ... to type Font struct.
   ```

   Solution

   Every X application requests fonts from the application defaults files or from the code. The Xserver then searches all of the known fonts to locate the font request. If the Xserver does not find the requested font, it reverts back to the system font, and the warning message is displayed:

   ```
   owv:xt warning missing charsets in string to font setconversion.
   ```

   This is an Xtool kit warning from the remote system. Use your Xserver documentation to find the correct procedure for creating a permanent search path in an Xserver environment.

   Check also this document:

   ```
   http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_OV-EN004584
   ```

Korean Version Issues

1. **Symptom QXCR1000194960**
   ovc -start Hangs on Linux During Installation

   During the installation of certificates on Linux systems during installation, the `ovc -start` command hangs. This problem occurs if the locale on the managed node is set to `ko_KR.euckr`.

   Using the `top` command, it can be seen that the `ovbbccb` process is consuming almost 100% of CPU.

   Solution

   To avoid this problem set `ja_JP.utf8` as a default locale:

   For example, in the `/etc/profile` file, enter the following lines:

   ```
   export LANG=ja_JP.utf8
   export LC_ALL=ja_JP.utf8
   ```

2. **Symptom QXCR1000192730**
   HTTPS Agent Installation on Red Hat Fails During opcactivate (ko_KR.euckr)

   Problems may be experienced with the Korean locale `ko_KR.euckr`.

   Solution

   Change default locale to **`ko_KR.utf8`**.

   To verify if locales are set correctly, perform `rlogin` to the system and execute the `locale` command. It should display `ko_KR.utf8`.

3. **Symptom QXCR1000204232**
   Heartbeat Polling Messages do not Acknowledge Each Other on Solaris 9 Systems

   On Simplified Chinese and Korean HPOM management server installations running on Solaris 9 systems, heartbeat polling messages do not acknowledge each other.

   For example, a red *node down* message is not acknowledged by a following green *node up again* message.

   Solution

   This is planned to be fixed with the next HPOM for UNIX server patch.

4. **Symptom QXCR1000102961 & NSMbb68636**
   Solaris Korean: ovw Warnings of Duplicate Definitions

   For both the Motif Administrator and Operator GUIs, when starting a Motif GUI in Korean locale (ko) on Solaris 8, many warnings appear on the command line:

   ```
   Duplicate define has been ignored.
   ```

   Solution

   These warning messages can safely be ignored.

5. **Symptom QXCR1000137218**
   Cannot Display Alphanumeric Labels in Motif UI in Korean Environments

   Alphanumeric labels are not displayed correctly in Korean environments.

   Solution

   a. Create a link under `/usr/lib/X11`:

```
cd /usr/lib/X11
ln -s /usr/openwin/lib/locale/ko_KR.EUC ko_KR.EUC
```

b. Modify the `/usr/lib/X11/ko_KR.EUC/app-defaults/OVw` file as follows:

Original:

```
OVw*size30Font:-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
OVw*size20Font:-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
OVw*size10Font:-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
OVw*smallFont:-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
```

Updated:

```
OVw*size30Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
OVw*size20Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
OVw*size10Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
OVw*smallFont: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-*-gothic-medium-r-normal--16-160-*-*-*-*-ksc5601.1987-0
```

Modify the `/usr/lib/X11/ko_KR.eucKR/app-defaults/OVw` file as follows:

Original:

```
OVw*size30Font:-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
OVw*size20Font:-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
OVw*size10Font:-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
OVw*smallFont:-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
```

Updated:

```
OVw*size30Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
OVw*size20Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
OVw*size10Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
OVw*smallFont: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
-hp-batang-medium-r-normal--*-*-*-*-*-*-ksc5636.1989-0
```

Simplified Chinese Version Issues

1. **Symptom NSMbb67982 and NSMbb68001**
   Cannot Display Alphanumeric Labels in Motif UI in Simplified Chinese Environments

   Alphanumeric labels are not displayed correctly in Simplified Chinese environments.

   Solution

   a. Create a link under `/usr/lib/X11`:

   ```
   cd /usr/lib/X11

   ln -s /usr/openwin/lib/locale/zh_CN.EUC zh_CN.EUC
   ```

   b. Modify the `/usr/lib/X11/zh_CN.EUC/app-defaults/OVw` file as follows:

   Original:

   ```
   OVw*size30Font:-*-song-medium-r-normal--16-140-*-*-*-*-*-*
   OVw*size20Font:-*-song-medium-r-normal--16-140-*-*-*-*-*-*
   OVw*size10Font:-*-song-medium-r-normal--16-140-*-*-*-*-*-*
   OVw*smallFont:-*-song-medium-r-normal--16-140-*-*-*-*-*-*
   ```

   Updated:

   ```
   OVw*size30Font:-adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-song-medium-r-normal--16-140-*-*-*-*-*-*
   OVw*size20Font:-adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-song-medium-r-normal--16-140-*-*-*-*-*-*
   OVw*size10Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-song-medium-r-normal--16-140-*-*-*-*-*-*
   OVw*smallFont: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-song-medium-r-normal--16-140-*-*-*-*-*-*0
   ```

   c. Modify the `/usr/lib/X11/zh_CN.hp15CN/app-defaults/OVw` file as follows:

   Original:

   ```
   OVw*size30Font:-hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   OVw*size20Font:-hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   OVw*size10Font:-hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   OVw*smallFont:-hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   ```

   Updated:

   ```
   OVw*size30Font:-adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   OVw*size20Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   OVw*size10Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   OVw*smallFont:  -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-song-medium-r-normal--*-*-*-*-*-*-gb2312.1980-1
   ```

2. **Symptom QXCR1000204232**
   Heartbeat Polling Messages do not Acknowledge Each Other on Solaris 9 Systems

   On Simplified Chinese and Korean HPOM management server installations running on Solaris 9 systems, heartbeat polling messages do not acknowledge each other.

   For example, a red *node down* message is not acknowledged by a following green *node up again* message.

   Solution

   This is planned to be fixed with the next HPOM for UNIX server patch.

Traditional Chinese Version Issues

1. **Symptom QXCR1000214444**
   Cannot Display Alphanumeric Labels in Motif UI in Traditional Chinese Environments

   Alphanumeric labels are not displayed correctly in Traditional Chinese environments.

   Solution

   a. Create a link under `/usr/lib/X11`:

   ```
   cd /usr/lib/X11
   ln -s /usr/openwin/lib/locale/zh_TW.big5 zh_TW.big5
   ```

   b. Modify the `/usr/lib/X11/zh_TW.big5/app-defaults/OVw` file as follows:

   Original:

   ```
   OVw*size30Font: -*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   OVw*size20Font:-*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   OVw*size10Font: -*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   OVw*smallFont: -*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   ```

   Updated:

   ```
   OVw*size30Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   OVw*size20Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   OVw*size10Font: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   OVw*smallFont: -adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15, \
   -*-*-medium-*-normal--*-*-*-*-*-*-big5-1
   ```

   Modify the `/usr/lib/X11/zh_TW.big5/app-defaults/OVw` file as follows:

   Original:

   ```
   OVw*size30Font:-hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   OVw*size20Font:-hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   OVw*size10Font:-hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   OVw*smallFont:-hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   ```

   Updated:

   ```
   OVw*size30Font:-adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   OOVw*size20Font:-adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   OVw*size10Font:-adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   OVw*smallFont:-adobe-times-medium-r-normal--*-*-*-*-*-*-iso8859-15,\
   -hp-sung-medium-r-normal--*-*-*-*-*-*-*-tchinesebig5
   ```

2. **Symptom QXCR1000192091**
   Traditional Chinese Locale, Core Agent Uses Simplified Chinese Catalog Instead of English

   When running some command line commands, such as `ovc`, `ovpolicy`, and `ovcert`, some Traditional Chinese characters in the output of the command are not readable.

   Solution

   On Traditional Chinese systems, the following will make sure that the strings are displayed in English.

   Move the catalog files in the directory `/opt/OV/msg/zh` to `/opt/OV/msg/zh_CN`.

NOTE On Solaris systems, if the locale is `zh`, moving the catalogs will also cause the help strings to be displayed in English.

Spanish Version Issues

1. **Symptom QXCR1000198059**
   English Welcome Message After Installing Spanish HPOM for UNIX

   When installing in a Spanish environment, the welcome message text is displayed in English.

   Solution

   This is a language issue and does not affect any other functionality. You may safely ignore this, you can upload your own customized welcome message text, or disable it. For further information on how to work with the welcome message, refer to the `opcuistartmsg` manpage.

2. **Symptom QXCR1000285811**
   A number of NNM 7.5 AE/SE filesets not removed by the ovoremove script

   After deinstallation of NNM 7.5 AE/SE (published in July 2005) using the NNM remove script or `ovoremove` script, the following NNM filesets could still be found on the system:

Name	Version	Description
HPOv3ComAgt	2.50.000	HP NNM Advanced Edition Device Support for 3Com
HPOvAlcatelAgt	2.50.000	HP NNM Advanced Edition Device Support for Alcatel
HPOvBayAgt	3.00.000	HP NNM Advanced Edition Device Support for Nortel Bay
HPOvCDPAgt	2.50.000	HP NNM Advanced Edition Device Support for CDP
HPOvCentilAgt	1.50.000	HP NNM Advanced Edition Device Support for Centillion
HPOvCiscoAgt	2.60.000	HP NNM Advanced Edition Device Support for Cisco
HPOvEDPAgt	2.51.000	HP NNM Advanced Edition Device Support for EDP
HPOvExtremeAgt	2.50.000	HP NNM Advanced Edition Device Support for Extreme
HPOvFoundryAgt	2.51.000	HP NNM Advanced Edition Device Support for Foundry
HPOvPassAgt	3.00.000	HP NNM Advanced Edition Device Support for Nortel Passport
HPOvProAgt	2.50.000	HP NNM Advanced Edition Device Support for HP Procurve

   Solution

   Manually deinstall all remaining NNM filesets with `swremove` tool.

A HPOM Management Server Patches Overview

This appendix lists all the enhancements, which were introduced with the HPOM 8.25 and superseding management server and Java GUI client patches.

NOTE For more information about all these enhancements, see “New Features with HPOM for UNIX 8” on page 16, and Chapter 5, “Last-Minute Changes to Documentation.”

Management Server Patches

8.35 Management Server Patch

The following enhancements are available with this patch:

- Since HPOM 8.33, it is possible to send the forward manager information to the trouble ticket if `OPC_TT_SHOW_FORW_MGR` is set to `TRUE`. However, if a message was not forwarded, no Forward Manager information was sent to trouble-ticketing system. Starting with HPOM 08.35, an empty string is sent as a Forward Manager information for non-forwarded messages.
- The `MGMTSV_KNOWN_MSG_NODE_NAME` variable can now be used in message key relations.

High Availibility Environments

The following high availibility environments are supported on the HP Operations management server with this patch:

- Veritas Cluster Server 5.0 on HP-UX 11.31
- HP Serviceguard 11.19 on HP-UX 11.31

8.34 Management Server Patch

The following enhancements are available with this patch:

- It is now possible to allow actions that were defined or modified in the agent MSI. In the `remactconf.xml` file, a new condition can be set:

  ```
  <if>
    <certified>msi</certified>
  </if>
  ```

  This means that either regular actions or MSI changed actions from an HTTPS node are allowed. On the other hand, actions from a DCE node are not allowed.

- To better deal with changed `OvCoreId`s (for example, because the agent was reinstalled), the following new error message and the variable are introduced:

  — `OpC40-649`

If OPC_LOG_DROPPED_MSGS is set to TRUE, opcmsgm now also logs messages received from the nodes for which the OvCoreId is different from the one known to the management server.

— OPC_MSGFORW_SYNC_COREIDS

If the OPC_MSGFORW_SYNC_COREIDS variable is set to TRUE, the OvCoreId of a node is automatically updated by received messages in a MoM environment. When a message that was forwarded from another server is received, and the OvCoreID of the node from the message is different than the one in the database, the OvCoreId is automatically updated in the database and the OpC40-664 internal message is sent to notify the operators.

- Avoiding duplicate OvCoreIds is enhanced in the following ways:
  - — itochecker now checks for duplicate core IDs during the HPOM database check.
  - — The new opcdbidx option -ovcoreid is added to check for duplicate OvCoreIds in the database.
  - — opcnode -chg_id now checks if another node already uses the same OvCoreID, and in that case issues an error.
- opcdbck performance and usability are improved, so that the opcdbck output is now more readable and the tool reports only real errors.
- A new variable is introduced - OPC_REPLACE_MGMTSV_VARIABLE_IN_CMAS. If this variable is set to TRUE, the Message Manager replaces the <$OPC_MGMTSV> variable with the management server hostname in the custom message attribute's value when a message is received.
- The agent hotfix deployment tool together with the PDF file is installed on the server with this patch:

  /opt/OV/contrib/OpC/Hotfix_deployment_tool
- Now it is possible to use an IP address to connect to a node by setting a new configuration variable - OPC_COMM_USEIP_URI.
- listguis now also displays template administrator sessions.
- The ovoremove script now asks if the database should be left intact during the HP Operations management server deinstallation.

8.33 Management Server Patch

The following enhancements are available with this patch:

- It is now possible to set the RES_RETRY and RES_RETRANS configuration variables for the management server.
- If a policy is assigned to both a virtual node and a physical node, a warning is printed to System.txt, and a warning message is generated during the distribution.
- Messages can be suppressed before being passed to the MSI by setting the OPC_SUPPRESS_OUTAGE_BEFORE_MSI configuration variable to TRUE.
- Messages with duplicate message IDs can be suppressed before being passed to the MSI by setting the OPC_SUPPRESS_DUPL_MSGID_BEFORE_MSI configuration variable to TRUE.
- A new configuration variable is introduced - OPC_TT_SHOW_FORW_MGR. If it is set to TRUE, the name of the HP Operations server that forwarded the message to the current server is passed as a parameter to the trouble ticket system and the notification service system (after the number of suppressed duplicate messages).

- It is now possible to register for messages and message events at the same time by using the message change event interface. The new `OPCSVIF_MSG_EVENTS_ALL` define has been added for the interface type, as well as the new `OPC_MSG_EVENT_ALL_MSG` event mask, which allows getting both new messages and change events in one stream.
- The default scripts for the policy-based message storm detection now remove the template version string from the message source, which is needed for 8.51 or newer agents. In case older agents are used and some template names are ending with a version string, the new `OPC_POLICYSTORM_LEAVE_VERSION` setting can be set to `TRUE` in order to prevent the removal of the version string.
- The HP Operations management server now copies the agent bundle XML file to the target node during the remote deployment. This is necessary for a proper switch of the agent to the HPOM for Windows management server later on.
- HP Operations management server side support for AIX 6.1 and Windows 2003 IPF HTTPS platforms has been added.

8.32 Intermediate Management Server Patch

NOTE No enhancements are available with this patch, only bug fixes.

8.31 Management Server Patch

The following enhancements are available with this patch:

- Oracle 11g support.
- A new ECS template is provided for the policy-based message storm detection.
- To avoid the duplicate suppression of the messages that do not have a message key and improve performance, an automatic message key creation is introduced.
- Only one `ovoinstall` script per management server platform is used, it allows agent patch installation before running `opcconfig`.
- Several changes are introduced in the HPOM heartbeat polling area to avoid false alerts.
- The itochecker report is improved, the report output is accessible for remote systems via the following URL: `http://<mgmt_server>:3443/ITO_OP/ito_rpt/report.html`
- A new config variable `OPC_DONT_REPLACE_MGMTSV_VARIABLE` is introduced to configure an action to be executed on the management server from which it is initiated.
- A new optional attribute `ip_addr` is added to the `opcnode`, which allows to specify the preferred IP address for a node with multiple IP addresses.
- The `opcdispm` binary now uses the AAS (Adaptive Address Space) feature, which provides a new address space layout named Mostly Private Address Space (MPAS).

8.30 Management Server Patch

The following enhancements are available with this patch:

- PAM failed login counter is implemented for each operator in the corresponding namespace to reduce the number of attempts to use invalid/expired passwords.

- Threshold policy can be customized locally on the node through using the XPL config variables file.
- Installation of the HTTPS agents was improved as follows:
  - The HTTPS agent installation now detects and report if `REXEC` service is not enabled to prevent the installation failure.
  - The HTTPS agent installation on virtual cluster nodes is prevented to eliminate possible damage to the HPOM server.
- The `ha_mon_cb` cluster monitor script (linked to `M200_cb`) has been changed to exit if `ovbbccb` is not running, which then causes failover.
- The database update algorithm was improved to reduce the database update time.
- The bulk message insert was improved to provide the same functionality as the single message insert.
- The itochecker report was improved.
- Suppression of error message per process is now enabled.
- Enhanced Auto and Operator Action signature checking.
- New Message Key filter attribute is added for message filtering. Saving Message Key filter setting is limited to 256 character.

APIs

New API functions and enhancements available with this patch:

- `opcdata` and other corresponding API man pages are updated in order to show all attribute info.
- Man pages for `opcdbmaint_api.3` and `opcdbmgmtsv_api.3` APIs are introduced.

CLIs

New and enhanced CLIs available with this patch:

- `opcdelmsgs` tool is enhanced to delete elements from other queue files.
- Non interactive approach for acknowledge messages is possible with improved `opcack` tool (with `-c` option).
- New `opclaygrp` is introduced to manage layout groups and node hierarchies.

  It enables to: create, delete, list layout groups and node hierarchies, move layout groups within same node hierarchy.

Other Enhancements and Fixes

- The database update algorithm was improved to reuse the `node_id` and `commit` once per message bulk. The time for database update was reduced.
- Server backup and restore scripts are updated to support the `log_archive_dest_n` parameter. The old `log_archive_dest` parameter is deprecated by Oracle 10g.
- `opc_recover` now works in a cluster environment.
- The `opcdbsetup` script now works with a non-default Oracle user and sets the `system` password for an Oracle user.

8.29 Management Server Patch

The following enhancements are available with this patch:

- Auto-granting feature of certificate request handling
- Improved certificate request handling

8.27 Management Server Patch

The following enhancements are available with this patch:

- Improved message processing for count and suppress duplicates
- Improved startup time of HPOM server processes
- Possibility of automatic and independent restart of aborted HPOM processes
- Parallel agent queries support by `opcragt`
- `opcragt -cleanstart` functionality added for HTTPS agents
- Improved error message for unknown nodes
- Enhanced profile report
- `itochecker` properly handles nodes with multiple IP addresses resolving to the same node name
- `opccfgupld` option for deleting templates not existing in upload files
- Modified internal error message of `opccfgout` for nodes with unresolvable IP assigned
- Notification messages can go directly to the history log
- Java GUI client version control

APIs

New functions of APIs are available with this patch:

- for deleting the container element without deleting the object itself
- for getting and modifying the trouble ticket interface
- for adding, deleting, getting, and modifying the instruction text interface
  - `opccfgttest` utility improved to test `opcinstruction_*()` APIs
- for adding, deleting, getting, and modifying notification services
- for adding, deleting, getting, and modifying the notification schedule
- for interacting with the database
- for accessing the pattern matching code

CLIs

The following new CLIs are available with this patch:

- for getting and modifying the trouble ticket interface
- for getting, adding, modifying, and deleting the instruction text interface
- for adding, getting, modifying, and deleting notification services (including the schedule)

8.25 Management Server Patch

The following enhancements are available with this patch:

- `opchbp` for changing the interval of heartbeat monitoring
- `opcownmsg` for setting, unsetting, and changing HPOM messages ownership
- Motif UI SSH-based virtual terminal

Java GUI Client Patches

8.35 Java GUI Client Patch

The following enhancement is available with this patch:

- A newer JRE 1.6.0_16 is provided for Microsoft Windows managed platforms.

8.34 Java GUI Client Patch

The following enhancements are available with this patch:

- A new check box is added to the `Preferences` dialog to enable or disable the `Communication Status` dialog – the `Show Communication Status` dialog. In addition, a new variable in `itooprc` is introduced - `show_comm_status_dlg` (with `yes` being the default value).
- The fallback mechanism can now be configured by using two new `itooprc` parameters:
  - `https_fallback` (if secure communication is used)
  - `socket_fallback` (if non-secure communication is used)
- Java GUI filtering now supports CMAs with HPOM style pattern matching.

8.33 Java GUI Client Patch

The following enhancement is available with this patch:

- A newer JRE 1.5.0_17 is provided for Microsoft Windows managed platforms.

8.31 Java GUI Client Patch

The following enhancements are available with this patch:

- By default, a popup notification does not take into account the Message View filter, it shows also messages which are filtered out by the CF definition. A new flag is added to the `Preferences` dialog box to change this behavior.
- HTTPS and FTP hyperlinks in Java GUI messages are supported.
- `OVPM_GRAPH` integration is added to the Java GUI.
- The embedded web browser is removed from the Preferences window. The ActiveX browser and the external browser are still available.

8.30 Java GUI Client Patch

The following enhancement is available with this patch:

- Disabled embedded browser

8.29 Java GUI Client Patch

The following enhancement is available with this patch:

- Save service graph layout feature

8.27 Java GUI Client Patch

The following enhancements are available with this patch:

- Sorting services by the Label attribute
- History Message Browser functionality can be disabled for operators
- Logging capability is added to the `ito_op_applet_cgi.ovpl` CGI script

8.25 Java GUI Client Patch

The following enhancements are available with this patch:

- HP One Voice look & feel
- Java GUI detaching windows
- Java GUI message view filtering
- HTML application output as an internal webpage
- Java GUI startup options
- `opcwall` for Java GUI
- Custom filename for configuration file
- Verify Java client console version by using CLI

Java GUI Online Help Patches

8.26 Java GUI Online Help Patch

- Japanese Java GUI online help update.

8.25 Java GUI Online Help Patch

- English Java GUI online help update.

8.21 Java GUI Online Help Patch

- English Java GUI online help update.

8.11 Java GUI Online Help Patch

- Korean Java GUI online help update.

Certificate Server Patches

8.25 Certificate Server Patch

- HPOvSecCS Lcore component version 01.00.220.
  Fixed granting certificate requests and updated Certificate Management Server.

NOTE This patch does not install HPOvSecCS (Certificate Server) component. Once patch is installed HPOvSecCS component has to be manually installed.

Server Accessories Patches

8.33 Server Accessories Patch

- Includes changes required for DMA 8.20.

Server Config API Java Patches

8.33 Server Config API Java Patch

- Includes changes required for DMA 8.20.

8.30 Server Config API Java Patch

- Added missing `libjopcsrvservice.so` library.
- Fixed some memory leaks.

8.25 Server Config API Java Patch

- Several new methods have been added.

8.22 Server Config API Java Patch

- Added a new `OpcInterface` class with some wrapper methods.

8.21 Server Config API Java Patch

- Java API has been provided on the server side.