HP Operations Manager

for the management server on the Red Hat Enterprise Linux operating system

Release Notes

Software Version: 9.10
Release Notes Publication Date: May 6, 2013

Edition 7

This document provides an overview of HP Operations Manager (HPOM) version 9.10. It contains important information not included in the manuals or in online help.

The first page of this document contains the version number, which indicates the software version and the publish date, which changes each time the document is updated. To check for recent updates or to verify that you are using the most recent edition, select **Operations Manager for UNIX** at the following location:

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

This document provides information about the following topics:

- Media Kit Contents
- Changes with Latest Patches
- What's New in the HPOM 9.xx Releases
- Integration with Other HP Software Solutions
- Coexistence with Other HP Software Solutions
- Obsolescence Announcements
- Installation Notes
- Known Problems, Limitations, and Workarounds
- Documentation Errata
- Local Language Support
- HP Software Support
- Legal Notices

Media Kit Contents

The HPOM media kit contains a number of CDs and DVDs required to install the HPOM foundation product, HP Operations Agent 11.00, HP Performance Manager 9.00, SiteScope 11.1x, HP Reporter 3.9x, NNMi 9.xx, MSES and TIBCO SPI, and Infrastructure SPIs 2.0. To use these products, you must also purchase a valid license.

Changes with Latest Patches

This section describes changes that are available with the latest HPOM patches.

HP Operations Management Server Patch

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

Table 1   Management Server Patch 9.10.240

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	**Linux**	**Solaris**
HPOM consolidated server 9.10.240	PHSS_43465	OML_00067	ITOSOL_00789

IMPORTANT Make sure that you install the latest management server patch before running the `ovoconfigure` script.

The following changes are available with this patch:

- The `/opt/OV/bin/OpC/utils/opcmsgchg` utility is available for allowing severity and message text modification.

- The `opcragt` command now supports the specification of a per-node timeout. It can be specified by using either the new `-timeout` option or the `OPCRAGT_TIMEOUT` configuration variable. Because cancelling threads may lead to side effects, `opcragt` does not cancel a timed-out thread. Instead, it ignores the timed-out thread and starts a new one.

  It is also possible to set timeouts for the `opcragt -start` and `opcragt -stop` calls by using the `OPCRAGT_START_TIMEOUT` and `OPCRAGT_STOP_TIMEOUT` configuration variables.

  The `OPCRAGT_MAX_THREADS_TOTAL` configuration variable is also available for limiting the total number of `opcragt` (including the timed-out) threads.

- A new option, `copy_desc`, is available for the `opcpolicy` command. When `copy_desc` is set to `yes`, the policy group description is copied, as follows:

  ```
  -copy_group pol_group=<from> pol_group_to=<to> [ level= <level> ] \
  [ copy_desc=<yes|no> ]

  level=1 : copy policy group tree (without assignments)
  level=2 : copy policy assignments into existing tree (no tree creation)
  level=3 : copy node+nodegrp assignments into existing tree (no tree creation)
  level=4 : copy policy group tree (with assignments; default)
  copy_desc=yes : copy policy group description
  copy_desc=no : doesn't copy policy group description (default)
  ```

- The following HA Manager–related changes are now available:

  — When sending the local status to the remote HA Manager fails, the remote node is not marked as FAULTED after one failure, but after a specified number of failures (the default value is 3). To specify after how many failures the remote node should be marked as FAULTED, set the MAX_COMM_PROBLEMS variable in the HA Manager configuration file to a desired value.

  — Node alive timeout, which is the time when remote status needs to be updated, is now increased. The default value is 60 seconds. You can change the default value by setting the NODE_ALIVE_TIMEOUT variable in HA Manager configuration file.

    The node alive timeout (that is, time during which the remote node status must be updated) can be set by using the NODE_ALIVE_TIMEOUT variable in the HA Manager configuration file (the default value is 60 seconds). If the node status is not updated in the specified time, the node becomes FAULTED.

  — The node sends its local status every 15 seconds (the default value). You can set another value by using the MAX_SEND_LOCAL_STATUS_TIME variable in the HA Manager configuration file.

  — The HARG that is FAULTED on a local node can be automatically cleared only if it is ONLINE on some other node. This behavior is disabled by default. To enable it, set the HARG_AUTOCLEAN_FAULTED_TIME variable in the HA Manager configuration file to a number that is greater than zero. This number represents the number of seconds that elapses from the moment the HARG becomes FAULTED until the moment the autoclean is performed.

  — The HA Manager configuration is automatically reloaded when it is modified.

- QCCR1A153519The opcuiwww.sh utility is modified so that when PAM or LDAP is enabled or configured on the HP Operations management server, opcuiwww.sh starts opcuiwww.ldap instead of the regular opcuiwww process. There is no need to replace the original opcuiwww binary with opcuiwww.ldap any more.

- A new option, -upgrade, is available for the opchistupl command. This option is used for uploading data of a particular locale. For example:

  /opt/OV/bin/OpC/opchistupl -upgrade ja_JP.SJIS /tmp/hist

- Two new options are available for the startInitialSync.sh utility:

  — The -dumpOnly option dumps the topology (for troubleshooting purposes).

  — The -syncOnly option synchronizes previously dumped topology from the current directory (if not specified otherwise).

- OPCUIWWW_DISABLE_ONLINE_CONFIG_SYNC: The behavior of the DISABLE_NOTIF_ONLY option is modified.

  If you set the OPCUIWWW_DISABLE_ONLINE_CONFIG_SYNC configuration variable to DISABLE_NOTIF_ONLY, a configuration update notification message does not appear in the Java GUI if basic changes (for example, a responsibility matrix change, a node change, a message group change, a tool change, and so on) are done. In this case, synchronization of configuration data is done without the operator being informed about it. However, if advanced changes (for example, a profile change) are done, a configuration update notification message appears informing the operator to reload the configuration so that the changes can take place.

- The following configuration variables are introduced:

  — OPC_FILTERS_BY_LAYOUT_GRP_LABEL: If you set this configuration variable to TRUE, node filters do not filter messages only by the layout group name, but also by the layout group label.

— DISABLE_SITESCOPE_NODE_MODIFICATION: If you set this configuration variable to FALSE (the default value), node deletion requests are not checked and therefore all requested deletions are performed. To load a new value, you must restart the Service Discovery server. If you set this configuration variable to TRUE, all node deletion requests that are received by the Service Discovery server are checked. When Site Scope sends a node deletion request, node attributes are checked and only nodes with attributes "Machine type = other other" and "Control type = message_allowed" are deleted. If deletion requests come from any other source than SiteScope, all requested nodes are deleted.

— OPC_SERIALIZE_SERVICE_MODEL: Used for preventing a core dump under a heavy load. Keep in mind that the performance in case of multiple parallel read requests might be decreased when using this variable. To use it, run the following command:

/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_SERIALIZE_SERVICE_MODEL TRUE

— OPC_CSA_LINUX_X64_PLATFORM: Allows you to set to which agent platform the certificate requests from Linux x64 nodes should be mapped (the default is Intel/AMD x64(HTTPS) -> Linux (MACH_BBC_LX26RPM_X64)).

• The following licensing-related changes are available:

— The All Nodes and the Selected Node reports now query for the HPOM 9.10 licensing related tables. In addition, the Selected Node report shows the particular licenses required by this node.

— You can exclude agentless nodes from the Target Connector license check and report if they are already licensed through another HP BTO Software product. For example, you can exclude SNMP devices that are monitored by HPOM through HP Network Node Manager i (NNMi) and are already licensed through NNMi. To configure licensing for agentless nodes, see "Configuring Licensing for Agentless Nodes" on page 14.

— A new option, -show, is available for the opcremsyschk command. It checks the messages that arrived within the last 24 hours, determines which message nodes have no agent installed, and shows the nodes that potentially require a Target Connector license.

For detailed information about configuration variables, see the *HPOM Server Configuration Variables* document.

New Support Announcements

The HP Operations management server patch 9.10.240 introduces support of the following:

Red Hat Enterprise Linux Advanced Platform/Red Hat Cluster Suite 5.9 HPOM is now supported on Red Hat Enterprise Linux Advanced Platform/Red Hat Cluster Suite 5.9.

VERITAS Cluster Server 5.1 Support on RHEL 6.xx VERITAS Cluster Server version 5.1 is now supported on RHEL 6.xx. For detailed information about supported RHEL 6.xx versions, see "Cluster Support" on page 16.

IMPORTANT You must install Service Pack 1 for VERITAS Cluster Server 5.1.

For detailed information about management server software requirements, see the *HP Operations Manager Installation Guide for the Management Server*.

Java GUI Patch

The following Java GUI patch is available:

Table 2 **Java GUI Patch 09.10.240**

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	**Linux**	**Solaris**
Java GUI 9.10.240	`PHSS_43515`	`OML_00068`	`ITOSOL_00790`

The following changes are available with this patch:

- The Java GUI installation now creates a new `lib` directory in the installation tree. This directory contains the `OvEmbWebBrowser21.dll` and `OvEmbWebBrowser27.dll` libraries. When the Java GUI is started as an application, the `dll` libraries are loaded from the `lib` directory.

  When starting the Java GUI as an applet or by using WebStart, a newly introduced parameter, `dll_path`, enables you to specify where the `dll` libraries will be extracted and loaded from. For example:

  — If the Java GUI is started as an applet:

  Standard connection:

  ```
  http://<server>:8081/OvCgi/ito_op_applet_cgi.ovpl?trace=\
  true&dll_path=<drive>:\<directory>
  ```

  Secure connection:

  ```
  https://<server>:8444/OvCgi/ito_op_applet_cgi.ovpl?trace=\
  true&dll_path=<drive>:\<directory>
  ```

  — If the Java GUI is started by using WebStart:

  Standard connection:

  ```
  http://<server>:8081/OvCgi/ito_op_applet_cgi.ovpl?trace=\
  true&webstart=true&dll_path=<drive>:\<directory>
  ```

  Secure connection:

  ```
  https://<server>:8444/OvCgi/ito_op_applet_cgi.ovpl?\
  webstart=true&trace=true&dll_path=<drive>:\<directory>
  ```

NOTE   If the `dll_path` parameter is not set or if the path is write protected or invalid, the `dll` libraries are extracted to the default location and loaded from it. This default location is as follows:

```
%OSDRIVE%\USERS\\AppData\Local\Temp
```

- The Export button that you can use for exporting or writing messages to a file without using a printer is now available in the Message Properties window (right-click popup menu from the message browser) and also from the main menu (click **Actions->Messages->Export**). This button has the similar options to a printer. The following is exported by using the Export button:

  — selected message

— all messages in the browser
— details about selected messages
— details about all messages in the browser

IMPORTANT If you have JRE 1.7 installed, use the Export button instead of a printer because printing to `FILE:` with Generic / Text Only printer produces an empty document.

- Service Actions are now executed on user selected nodes only if there are no predefined nodes in service `.xml` file for these actions.

- Changing labels for Message Browser columns in the Customize Message Browser Columns window now results in changing the corresponding message attributes in the Message Properties window.

- The `noapp` parameter from the `itooprc` resource file is enhanced.

  By using this parameter you can disable both Start and Start Customized... actions. Settings made by using this option override settings made by using the Tailored set of Tools option (which is accessible from Edit->Preferences...->General menu), and they also apply regardless of the number of applications that are assigned to a user.

  The `noapp` value is loaded only at the Java GUI startup. The possible values are `true` and `false` (the default is `false`).

  When the `noapp` parameter is disabled from the `itooprc` file, the value of Tailored set of Tools is loaded from the `itooprc` file.

HPOM Core Server Patch

The following core server patch is available:

Table 3   HPOM Core Server 09.10.230

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	**Linux**	**Solaris**
HPOM Core Server 9.10.230	`PHSS_43032`	`OML_00055`	`ITOSOL_00777`

This patch contains the following packages:

- `HPOvOprEl` (HP Operations Embedded Licensing) 02.12.103

- `HPOvSecCS` (HP Software Certificate Management Server) 11.03.031 and 11.10.035

- `HPOvJxpl` (HP Software Cross Platform Component Java) 11.03.030 and 11.10.035

- `HPOvJsec` (HP Software Security Core Java) 11.03.030 and 11.10.035

- `HPOvJbbc` (HP Software HTTP Communication Java) 11.03.030 and 11.10.035

IMPORTANT This patch only places the packages onto your HPOM server system. Therefore, make sure that you carefully follow the instructions for installing the packages that you can find in the patch text.

CAUTION	Although during the patch installation you are asked to install the packages by following the instructions in the `/opt/OV/contrib/OpC/CORE/Readme` file, make sure that you do not follow those instructions, but the ones that you can find in the patch text.

When installing the packages, keep in mind that it is also important which HP Operations agent version you have installed on the management server. Namely, the following packages are installed only if the version of the HP Operations agent is as required:

- The `HPOvSecCS` 11.10 and `HPOvJxxx` 11.10 packages are installed if the HP Operations agent version installed on the management server is 11.10 or higher.

- The `HPOvSecCS` 11.03 and `HPOvJxxx` 11.03 packages are installed if the HP Operations agent version installed on the management server is 11.04 or higher, but below 11.10.

  Because the version of `HPOvSecCS`, which is installed by manually running the `install_core_packages.sh` script after the patch is installed, depends on the version of the agent, the installation order is important:

  — *Step 1:* Install the HP Operations agent 11.10 (or 11.04, if you still use the 11.0x agent version) locally on the management server.

  — *Step 2:* Install the HPOM core server patch, and then run the `install_core_packages.sh` script.

  If the HP Operations agent is installed after the patch, the `install_core_packages.sh` script must be rerun after the agent software is deployed to the local node on the management server.

NOTE	The `HPOvSecCS` 11.03 and HP Operations agent 11.04 combination is required if you want to keep the HP Operations agent version 11.0x and autogranting is used.

NOTE	With `HPOvSecCS` 11.10.035, there is an increase in the default RSA key length (from 1024 to 2048 bits). Therefore, a new CA certificate is created with a new key length on the server. However, the existing CA certificates on the server do not get modified. As part of the upgrade, a new CA certificate with the alias CA_*<ovcoreid>*_*<ASYMMETRIC_KEY_LENGTH>* is added.
	It is recommended that you back up your certificates before installing the packages. In a cluster environment, back up the certificates only on the active node.
	For example:
	/opt/OV/bin/OpC/opcsvcertbackup -backup -passwd *<password>* \ -file /backup/cert_backup

Recreating Certificate Requests on Passive Cluster Nodes

When the updated HP Software core packages are installed, you must recreate certificate requests on passive cluster nodes. To do this, follow these steps:

1. On the active cluster node, start all the processes that are controlled by the OV Control (`ovcd`):

   /opt/OV/bin/ovc -start

2. On the passive cluster node, stop all the processes that are controlled by the OV Control (ovcd):

   /opt/OV/bin/ovc -kill

3. Check the value of the CERT_INSTALLED variable:

   /opt/OV/bin/ovconfget sec.cm.certificates CERT_INSTALLED

4. If the CERT_INSTALLED variable is set to TRUE, set it to FALSE:

   /opt/OV/bin/ovconfchg -ns sec.cm.certificates -set CERT_INSTALLED FALSE

5. Start the CORE components:

   /opt/OV/bin/ovc -start CORE

6. On the active cluster node/certificate server, check if there is a certificate request from the passive cluster node:

   /opt/OV/bin/ovcm -listpending -l

   If there is no certificate request, initiate a new certificate request on the passive cluster node:

   /opt/OV/bin/ovcert -certreq

7. On the active cluster node/certificate server, grant the selected certificate request:

   /opt/OV/bin/ovcm -grant *<RequestID>*

8. On the passive cluster node, start the COREXT and AGENT components:

   /opt/OV/bin/ovc -start COREXT AGENT

HPOM Server Accessories Patch

The following server accessories patch is available:

Table 4   HPOM Server Accessories 09.10.230

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	**Linux**	**Solaris**
HPOM Server Accessories 9.10.230	PHSS_43292	OML_00064	ITOSOL_00786

This patch contains the following shared component packages:

- HPOvJREB (HP Software JRE) 01.07.007

NOTE   With this patch, a newer JRE version is provided for all platforms except Microsoft Windows platforms, 1.7.0_07. For detailed information, see Table 5 on page 43.

- HPOvTomcatB (HP OpenView TomcatB Servlet Container) 06.00.035
- HPOmWs (HP Operations Manager Web Service) 09.10.059
- HPOprWsInc (HP Operations Manager Incident Web Service) 09.10.060

IMPORTANT   This patch only places the packages onto your HPOM server system. Therefore, make sure that you carefully follow the instructions for installing the packages that can be found in the following file:

`/opt/OV/contrib/OpC/ACCESSORIES/Readme`

What's New in the HPOM 9.xx Releases

NOTE	Changes that are introduced with the latest patches for the HP Operations management server and the Java GUI are not included in this section.

New Features

HPOM 9.xx contains the following new features:

Localization

HPOM 9.10 is localized to Japanese, Korean, Simplified Chinese, and Spanish. For details, see "Local Language Support" on page 70.

64-Bit Application

HPOM is a 64-bit application. All the HPOM major binaries, libraries, scripts, and other utilities ported to the Linux operating system run as 64-bit applications on AMD or Intel x86-64 platforms.

Web-based Administration for HPOM

HPOM provides a new web-based Administration UI which replaces the Motif UI. The key benefits of the new web-based Administration UI are:

- Web-based configuration of HPOM.

- Concurrent use by multiple administrators with different access rights.

- Improved navigation and editing of HPOM configuration items.

- Policy (template) versioning and comparison capabilities to quickly identify configuration changes and differences.

You can install the Administration UI on the HPOM system after the server installation is complete. HPOM Administration UI user documentation is available online at the Support web site.

The following enhancements are available:

- The AdminUI allows creation of conditions for the SNMP policy with `SpecificTrapID` in the range of `int32` or `uint32`. If the value is inside the range of `uint32`, it is converted to appropriate `int32`.

- If you specify a non-existing Into directory when editing the database maintenance settings, a message appears stating that the value must be reset together with a marker indicating the field.

- When deploying the service discovery policy with credentials from the HP Operations management server, the `xml` file is created in the `%ovagentdir%\tmp\agtrep` directory.

- The Instance filter mode is now handled correctly when loading policies. The Administration UI performs checks on the `OBJECT` field instead of the `INSTANCERULE` field.

- Message reports based on the `opcmsgsrpt` tool using the `-n` option work in Internet Explorer.

- The `OPC_CHECK_READFILE` variable value is considered during validation. The overall validation issues an error when the following happens:

— Both the Logfile and Readfile fields are not filled.

— The Readfile field is filled and the Execute field is not filled.

— The Readfile field is not filled, while OPC_CHECK_READFILE is set to TRUE (the default value), and the Execute field is filled.

• Multi-line input in the message policy is supported.

• It is possible to select "On Server Log Only" and "Notification" in the End Actions tab (in "Measurement Threshold Policy").

For Administration UI known problems and workarounds, see "Administration UI" on page 64.

New Policy Types

HPOM templates are now referred to as policies, and provide new monitoring capabilities:

• The **Windows Management Interface** (WMI) policy type monitors the properties of WMI classes and instances, and responds when a property matches a value you select, or when an instance you select is created.

• The **Nodeinfo** policy type allows you to configure some aspects of agent behavior, for example, buffer sizes, IP addresses, and port numbers for client-server communication.

• The **Service Process Monitoring** policy type monitors services and processes that are running on managed nodes and sends a message when the state of the service or the process changes.

• The **Measurement Threshold** policy type evaluates performance data and responds if the data does not remain within acceptable levels. This policy type is useful if you want to monitor parameters that are constantly changing, such as CPU load, disk space, number of running processes, and so on. You can also use VB Script or Perl to perform your own calculations and decide if the threshold has been crossed.

• The **ConfigFile** policy type is used by Smart Plug-Ins (SPIs) such as SAP or Microsoft Exchange to configure instrumentation after SPIs are deployed on nodes.

• The **Windows Event Log** policy type allows access to several event log sources.

Policy Versioning

HPOM 8.xx templates are automatically converted into *policies* when uploaded to HPOM 9.xx. Policies serve the same purpose as templates, but policies are versioned. You can assign specific versions of a policy to managed nodes, node groups, or policy groups. You can also rollback to a specific version of a policy, and assign policies by using the following modes: FIX, LATEST, and MINOR_TO_LATEST.

Category-Based Instrumentation Distribution

You can associate instrumentation with policies by using *categories*. This association ensures that the management server automatically deploys instrumentation required by a policy when it deploys that policy. Categories increase your control over which instrumentation is distributed, and to which managed nodes, thus reducing the amount of instrumentation that needs to be distributed.

Category-based instrumentation enhances and replaces the selective distribution concept, which is still available for backward compatibility. Plan your upgrade to category-based instrumentation, because selective distribution will be deprecated.

Policy and Instrumentation Compatibility

Policies, policy groups, and instrumentation developed for HPOM on UNIX and HPOM on Linux are compatible with HPOM on Windows, and vice versa.

Subagent Management

This version of HPOM introduces a new type of subagent registration based on policy management features. Subagent assignment is managed by assigning subagent policies. Different versions of subagents have different versions of the corresponding subagent policies. This allows you to see which subagent is assigned to a managed node.

The subagent policies are not meant to be edited and are provided by a subagent supplier. Assigning such a policy to a node and deploying it using new options of the `opcragt` command installs the corresponding subagent on the node. The actual subagent policy is not deployed to the managed node and is not visible in the `opctemplate`/`ovpolicy` output.

Custom Service Auto-Discovery and Topology Synchronization

You can now create new service auto-discovery policies to discover services in your environment and automatically populate your service hierarchy. The services that you discover can belong to any existing service type, including any new service types that you decide to configure. In an environment with multiple HP Operations management servers, you can also automatically exchange node and service configurations between management servers by configuring topology synchronization.

For detailed information, see the *Custom Service Auto-Discovery and Topology Synchronization Guide*, which is available for download from the following location:

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

Online Configuration Synchronization

This release of HPOM introduces automatic synchronization of configuration data between the HPOM management server and the Java GUI without forcing the operator to log on again to make the changes effective. Synchronization can involve changes to nodes, applications, policies, groups, user profiles, and so on. The configuration data uploaded by using `opccfgupld` does not require server restart.

It is also possible to completely disable the online Java GUI synchronization by setting the `OPCUIWWW_DISABLE_ONLINE_CONFIG_SYNC` configuration variable to `TRUE`:

ovconfchg -ovrg server -ns opc -set OPCUIWWW_DISABLE_ONLINE_CONFIG_SYNC TRUE

NOTE   If this variable is set to `TRUE`, the operator does not receive notifications about configuration changes. Therefore, the administrator must inform operators about major configuration changes, so that operators use the `Reload Configuration` option to get the current configuration.

Disabling the online Java GUI synchronization has an effect only on configuration changes and does not affect the Service Load on Demand functionality.

High Availability (HA) Manager

HA Manager is a light-weight solution that allows the configuration of an automatic failover of the virtual IP address in a server pooling setup in a similar way as in a regular failover cluster.

The HA Manager feature enables you to do the following:

- Switch an IP address from one node to another node within a server pooling environment. In this case, no hardware cluster is needed and HP Operations agents and HPOM GUIs can communicate using that high availability virtual IP address.

  For details, see the *HP Operations High Availability Through Server Pooling* document.

• Control other resources besides virtual IP addresses and make them high available.

For detailed information about the HA Manager feature, see the *High Availability Manager* white paper.

Auditing

Auditing is redesigned to provide centralized event logging, four audit levels, and individual event logging configuration. Note that the audit information is no longer stored in a database, so old audit entries are lost when upgrading to HPOM 9.xx. The individual audit area variables are managed by `opcsrvconfig(1m)` and `ovconfchg(1m)`.

Unicode (UTF-8) support

This version of HPOM 9.xx introduces Unicode support. Both the Oracle database and the management server work exclusively with the UTF-8 character set, which provides multilingual support.

Remote Database Platform Independence

The HPOM remote database is platform independent. For details, see the *HPOM Installation Guide for the Management Server*.

RAC Support

Oracle Real Application Clusters (RAC) represents a scalable and manageable solution for sharing access to a single database among many or several nodes in a high availability cluster environment.

This shared access makes possible that, even during a system fault on one of the nodes, data can be accessed from any one of the remaining nodes. Work on the failed node is recovered automatically without administrator intervention and without data loss.

Oracle RAC is an Oracle Corporation exclusive technology that enables building large systems from commodity components and is the foundation for Enterprise GRID computing.

The Oracle Database server can be installed and used with HPOM on any platform supported by the HP Operations management server. HPOM online backup and restore are supported in RAC environment.

Licensing

License management is redesigned to allow other product components to easily and flexibly integrate with HPOM. A license reporting tool, OM License Reporter (`omlicreporter`), is introduced to enable checking status and availability of the HPOM licenses as well as generating HTML license reports.

In cluster environments the licenses can be installed on the shared disk. Only one license is required for a HA cluster, which is different from previous releases, when multiple licenses were required. The Administration UI does not run without a valid server license.

Configuring Licensing for Agentless Nodes To configure licensing for agentless nodes, follow these steps:

1. Generate a list of agentless nodes for the target connector license filter as follows:

    a. Open a command prompt and type the following:

    ```
    /opt/OV/bin/ovconfchg -ovrg server -ns tclfilter -set dumpfile \
    /var/opt/OV/share/tmp/OpC/mgmt_sv/dumpfile.txt
    ```

    b. Wait for the next license check. License checks are executed daily.

    c. Open `dumpfile.txt` and identify the nodes that you want to exclude from the target connector license check. Note down their IP addresses or hostnames.

2. Configure a filter that excludes agentless nodes by IP addresses or hostnames, as follows:

   a. In a command prompt, type the following:

      `/opt/OV/bin/ovconfchg -ovrg server -ns tclfilter -set hostnamefilter <filter>`

      In this instance, `<filter>` is a string that contains patterns of hostnames or IP addresses. For example, the pattern `^192.10.<*>.<*>|<*>.example.com$` excludes all nodes with IP addresses starting with `192.10.` or with hostnames ending in `example.com`.

   b. Specify a file with patterns to be excluded by typing the following:

      `ovconfchg -ns tclfilter -set filterfile <filterfile>`

NOTE	Each line is treated as a pattern. Lines that start with "#" are treated as comments and are ignored.

---

   c. Wait for the next license check to regenerate the list of nodes in `dumpfile.txt`.

   d. Open `dumpfile.txt`. Nodes prefixed with `FILTERED` are excluded from the target connector license check, while nodes prefixed with `NOT FILTERED` are included in the check.

NOTE	Set `dumpfile.txt` so that the configured filter will work.

Deploying SiteScope Configuration with HPOM

The combined functionality of SiteScope and HPOM provides an effective and in-depth monitoring solution that enables you to manage SiteScope templates with HPOM. To fully utilize and benefit from all the advantages of proactive monitoring, you can operate with unified policy concepts between HPOM and SiteScope, which means that SiteScope templates and monitors can be configured through the HPOM policy assignment and deployment.

For detailed information, see the *Deploying SiteScope Configuration with HPOM* document that you can download from the following web site:

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

HPOM Web Services

HPOM Web Services enable you to develop remote clients that access HP Operations management servers using industry-standard terminology and technical standards, instead of product-specific interfaces. HPOM provides the Incident Web Service and the Tool Web Service. The Incident Web Service enables clients to access HPOM messages. The Tool Web Service enables clients to execute tools from an HP Operations management server.

Cockpit Views

The HPOM cockpit view is a web-based interface that displays the state of the environment monitored by HPOM. Cockpit views help users to quickly assess the health and readiness of the environment to support the business.

The cockpit views consist of an indicator panel and the message browser. The indicator panel displays one or more message filter groups, the message browser displays messages for each filter.

Secure SSL Connection

To improve security in your environment, a secure SSL connection can be used to connect to the HPOM web pages. Port 8444 is used for the secure connection. For example,
https://<management_server>:8444/ITO_DOC

Red Hat Enterprise Linux (RHEL) Support

HPOM is supported on the following:

- RHEL 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, and 5.9

NOTE	If your RHEL version is 5.5 or higher, make sure that you upgrade to HP Operations agent 11.00 or higher, so that HPOM runs in a supported environment.

- RHEL 6.0, 6.1, 6.2, and 6.3

To set up HPOM in a RHEL 6.0, 6.1, 6.2, or 6.3 environment, follow these steps:

1. Install the HP Operations agent and patch it to version 11.02.11 (patch ID is OALIN_00003) or higher.

2. Start the installation by using the latest `ovoinstall` script that you can find at the following location:

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

3. Before continuing with the server configuration, install management server patch 9.10.230.

4. After the installation and configuration procedures are finished, install agent depot packages.

   Because of a known problem with the software status flag in the HPOM database (QCCR1A142496), make sure that you set the proper software status flag. To do this, run the following command on the management server:

   `/opt/OV/bin/OpC/opcsw -i -a`

5. *Optional:* Install core server patch 9.10.230, accessories patch 9.10.230, and Java GUI patch 9.10.230.

For more information, see the *HPOM Installation Guide for the Management Server*.

SELinux

SELinux running in the enforcing mode, which is the default mode that executes the SELinux security policy in a Red Hat Enterprise Linux environment, is now supported with HPOM.

Cluster Support

HPOM 9.xx supports HP Operations management server installation in the following cluster environments:

- Red Hat Enterprise Linux Advanced Platform/Red Hat Cluster Suite 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, and 5.9, as well as 6.0, 6.1, 6.2, and 6.3

IMPORTANT	The procedure for installing and configuring HPOM in a cluster environment that is described in the *HPOM Installation Guide for the Management Server* differs in some steps depending on the version of Red Hat Enterprise Linux Advanced Platform/Red Hat Cluster Suite you have. Starting with version 6.0, be aware of the following changes:

— Locations of vgchange and mount tools:

Use /sbin/vgchange instead of /usr/sbin/vgchange and /bin/mount instead of /usr/sbin/mount.

— During HPOM server configuration, the remote shell (remsh) and secure remote shell (ssh) connections are checked before the HA resource group name.

— Checking remsh and ssh connections is performed on a primary node as well.

You must also make sure that in a Red Hat Cluster Suite 6.xx environment, the HP Operations agent version is 11.10.35 or higher (or 11.04, if you still use the 11.0x agent version).

- Veritas Cluster Server 5.1

IPv6 Support

You can use the following Internet Protocol version 6 (IPv6) functionalities with HP Operations management server 9.10.200 or higher and HP Operations agent 11.00.044 or higher:

- adding, deleting, and modifying IPv6 nodes

- adding and deleting external nodes that match IPv6 addresses

- adding and processing messages for IPv6 nodes by using the server MSI

- message forwarding of IPv6 node messages (all participating management servers must have version 9.10.200 or higher and the OPC_IPV6_ACTIVE configuration variable set to TRUE)

- IPv6 SNMP traps and remote MIB monitoring

- remote WMI monitoring for IPv6 nodes

- NNMi to HPOM on Linux SNMP IPv6 trap integration

In general, it is preferable to work with node names rather than with IPv6 addresses because they are easier to use (for example, when filtering messages and when using host information in policies such as specifying a remote MIB monitoring target).

NOTE	The HP Operations management server and the HP Operations agent can run only on nodes that have an IPv4 address. To deal with IPv6, the HP Operations agent must run on a dual-stack node (a network node that supports both IPv4 and IPv6). From such a dual-stack system, pure IPv6 nodes can be remotely monitored.

The required Administration UI version is 9.10.

The following functionalities are not supported:

- installing the HP Operations agent on a node where only an IPv6 address is set up

- performing heartbeat polling for IPv6 nodes

- deploying data to or reading data from IPv6 nodes by using the `ovdeploy` command line interface

- executing actions on IPv6 nodes

To enable the IPv6 support on the management server, set the `OPC_IPV6_ACTIVE` configuration variable to TRUE:

```
ovconfchg -ovrg server -ns opc -set OPC_IPV6_ACTIVE TRUE
```

New Variables

In addition to variables introduced to support auditing, the following configuration variables are introduced:

OPC_ACK_DUPLS_IF_NORMAL_MSG	OPC_MSGKEY_MODIFY_TEXT
OPC_ALLOW_DUPLICATE_IP	OPC_NAMESRV_EXPIRE_MODE
OPC_ALWAYS_KEEP_CURRENT_POLICY_STATUS	OPC_NAMESRV_TTL
OPC_CFGDWN_OMIT_VIRTUAL_GROUP_DOWNLOAD	OPC_NO_ACK_VIA_CORR_IF_OWNED
OPC_CFGUPLD_BLOCK_RETRY	OPC_OVHARG_START_LOCAL_AGENT
OPC_CSA_ALLOW_IP_MISMATCH	OPC_PING_SIZE
OPC_CSA_USE_OS_BITS[a]	OPC_REJECT_CMA_DELETIONS
OPC_CFGUPLD_ONLINE_SVC_UPDATE	OPC_SOURCE_FORW_NOTIF_TO_TT
OPC_DEPLOY_IF_CALLBACK_FAILS	OPC_SUPPRESS_IF_NO_CORRELATION
OPC_DIST_OMIT_ERROR_AGT_NOT_INST	OPC_SUPPRESS_IF_NO_CORRELATION_MSGAPPLICATION
OPC_DONT_EMPTY_NS_CACHE	OPC_SUPPRESS_IF_NO_CORRELATION_MSGGROUP
OPC_DONT_LOG_REUSED_COREIDS	OPC_SUPPRESS_IF_NO_CORRELATION_MSGOBJECT
OPC_EMPTY_NS_CACHE	OPC_TRUNC_MSG
OPC_ENABLE_FWDCHAIN_FWDSENDER_CMA	OPC_XPL_SQL_TRACE
OPC_FORWARD_READONLY_MSGS	OPCRAGT_OMIT_ERROR_AGT_NOT_INST
OPC_HBP_DOUBLE_CHECK_DELAY	OPCUIWWW_KILL_APP
OPC_HBP_DOUBLE_CHECK_DELAY_BUFFER	OPCUIWWW_KILL_APP_TIMEOUT
OPC_HBP_DOUBLE_CHECK_DELAY_UNREACHABLE	
OPC_HBP_DOUBLE_CHECK_RETRIES	
OPC_IPV6_ACTIVE	
OPC_JGUI_VER_DOWNLOAD_URL	
OPC_KILL_OPCUIWWW	
OPC_LOGONLY_OUTAGE_SKIP_MSI	
OPC_MGMTSV_IPADDR_ON_LOAD_BALANCER	
OPC_MGMTSV_NAME_ON_LOAD_BALANCER	
OPC_MSG_BULK_INSERT_RATE	

    a. When using this feature, make sure that you use the HP Operations agent version 11.04 or higher on the management server and the managed node. In addition, it is also required to have version 11.03.031 or higher of the `HPOvSecCS` package on the management server. Otherwise, the process aborts.

For more information on the server configuration variables, see the *HPOM Server Configuration Variables* manual.

For the information on the audit-related variables, see the *HPOM Administrator's Reference*.

New CLIs

HPOM 9.xx includes the following new command line interfaces:

`BBCTrustServer.sh`	`opcappl`	`opcpolicy`
`mib2policy`	`opcinstrumcfg`	`opcsrvconfig`
`omlicreporter`	`opcmsggrp`	`opcunack`
`opcactdwn`	`opcpoltype`	`ovolicense`
`opcactupl`		

For more information, see the corresponding manual pages.

New APIs

For information about the following new APIs, see the API manual pages.

`opc_distrib_highprio()`	`opcnodegrp_get_policy_groups()op`	`opcpolicybody_modify_by_name()`
`opcapi_crypt_string()`	`cpolicy_assign_categories()`	`opcpolicygrp_get()`
`opcapi_namesrv_free_hostent()`	`opcpolicy_assignment_mode_set()`	`opcpolicygrp_add()`
`opcapi_namesrv_gethost()`	`opcpolicy_copy()`	`opcpolicygrp_create()`
`opcinstrum_get_categories()`	`opcpolicy_copy_assignments()`	`opcpolicygrp_modify()`
`opcinstrum_get_category()`	`opcpolicy_deassign_categories()`	`opcpolicygrp_delete()`
`opcinstrum_add_categories()`	`opcpolicy_delete()`	`opcpolicygrp_copy()`
`opcinstrum_del_categories()`	`opcpolicy_edit()`	`opcpolicygrp_get_list()`
`opcinstrum_modify_categories()`	`opcpolicy_edit_body()`	`opcpolicygrp_get_data()`
`opcnode_assign_policy_groups()`	`opcpolicy_get()`	`opcpolicygrp_assign_policies()`
`opcnode_deassign_policy_groups()`	`opcpolicy_get_categories()`	`opcpolicygrp_deassign_policies()`
`opcnode_get_policy_groups()`	`opcpolicy_get_data()`	`opcpolicygrp_list_assignments()`
`opcnode_assign_policies()`	`opcpolicy_get_list()`	`opcpolicytype_add()`
`opcnode_deassign_policies()`	`opcpolicy_get_list_by_type()`	`opcpolicytype_add_from_xml()`
`opcnode_get_policies()`	`opcpolicy_header_create()`	`opcpolicytype_get()`
`opcnode_assign_categories()`	`opcpolicy_list_assignments()`	`opcpolicytype_get_template()`
`opcnode_deassign_categories()`	`opcpolicy_list_resolved_assignme`	`opcpolicytype_modify()`
`opcnode_get_categories()`	`nts()`	`opcpolicytype_delete()`
`opcnodegrp_assign_policies()`	`opcpolicy_modify()`	`opcpolicytype_write_xml()`
`opcnodegrp_deassign_policies()`	`opcpolicy_update_assignments()`	`opcpolicytype_get_name_by_uuid()`
`opcnodegrp_get_policies()`	`opcpolicybody_get()`	`opcpolicytype_get_uuid_by_name()`
`opcnodegrp_assign_policy_groups()`	`opcpolicybody_modify()`	`opcpolicy_add()`
`opcnodegrp_deassign_policy_groups()`		

Feature Enhancements

The following enhancements are introduced:

Enhanced Java GUI

For a complete description of the Java GUI functionality, read the *HPOM Java GUI Operator's Guide*. The following is a summary of the enhanced Java GUI features:

- Service Enhancements

  A Service Map Table view is now available in addition to the Graph and Custom views. This view is similar to the message browser, listing services and their properties in a table. Service Map Table View is available for service submaps and custom maps, but not for service graphs.

- Message Enhancements

  The following enhancements are introduced with the current release:

  — When performing exporting, dragging or printing messages from a message filter browser, the messages are sorted in the same way as they were in the message filter browser.

  — When using relative time filtering with enabled relative time recalculation, message browser is refreshed with new messages and does not display the messages that become too old to satisfy the filter criteria. This behavior can be enabled by the administrator using the OPCUIWWW_FILTER_RELATIVE_TIME_RECALC server parameter.

- Java GUI Window Enhancements

  — A new option, Stay On Top, is added to the Preferences dialog. This option enables the Java GUI windows (main and detached) to stay on top of other windows. A stay_on_top parameter is introduced in itooprc, its default value is no.

  — Frequently used tools are displayed above the separator line in the pop-up menu for starting tools, so they can be easily accessed.

  — You can now prevent a hyperlink from appearing in the pop-up dialog when Java GUI version controlling is used. To do this, set the OPC_JGUI_VER_DOWNLOAD_URL configuration variable to NONE.

- Miscellaneous

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

  — HPOM Java GUI can be launched with WebStart. A link for the WebStart launch of Java GUI is added to the HPOM home page: http://<server_name>:8081/ITO_OP/.

  — The Java GUI functionality is extended to support HTTPS and FTP hyperlinks in messages.

  — For Java GUI clients connected in HTTPS mode, the listguis tool shows the following information: hostname (fully qualified domain name), IP address, connection type (https vs. socket), connection port (for example, 2531 for socket communication).

    The output of listguis shows the master (m), client (c), and client tool (ct) opcuiwww processes.

    In the Java GUI Login dialog box, you can choose between the https and socket connection type (the socket connection type, which is the default, is automatically selected).

  — Some terminology is changed to be aligned with HPOM on Windows. For example, Applications are now called Tools.

  — A new configuration variable, OPC_JGUI_CUSTOM_LINK_PROTOCOLS, is introduced to allow defining the custom URL protocols. Multiple protocols should be separated with ',' or ':'. For example:

    ovconfchg -ovrg server -ns opc -set OPC_JGUI_CUSTOM_LINK_PROTOCOLS file,exp2

  — HTTPS protocol is now supported for the Global Settings functionality.

  — It is possible to disable the frequently used tools feature by setting the value to 0 in the Preferences dialog box or the number_of_frequently_used_tools parameter in itooprc.

    You can also use the OPC_JGUI_TOOLS_FREQUENCY_ENABLED configuration variable to enable or disable the frequently used tools feature. If you want to enable this feature, set the configuration variable to TRUE. If you want to disable this feature, set the configuration variable to FALSE.

  — The following new parameter is introduced: select_only_managed_nodes.

If the `select_only_managed_nodes` parameter is enabled (that is, its value is set to `on`, `true`, or `yes`), only the regular node or nodes are selected (if no regular nodes are found, the external node or nodes are selected). If the `select_only_managed_nodes` parameter is disabled (that is, its value is set to `off`, `false`, or `no`) or if it is omitted (that is, it is not set), all nodes are selected.

— When a new user logs on to the Java GUI, the other users are not affected anymore.

The itooprc File Enhancements The following new parameters are introduced in the `itooprc` resource file:

`chg_source_to_source_pol`: If this parameter is enabled, you can change the name of the Source column in the message browser to Source Policy. The format of the `chg_source_to_source_pol` parameter is as follows: yes|no (the default value is no).

NOTE Because of performance reasons, the Source column cannot display the condition parameter for all messages in the message browser.

`export_all_windows_msgs`: If this parameter is enabled, you can export all selected messages from all open message browsers to a file. The format of the `export_all_windows_msgs` parameter is as follows: yes|no (the default value is no).

`show_operator_as_services_root`: If this parameter is enabled, the Services root node in the service graph is no longer named Services, but after the operator to whom the service was assigned.

IMPORTANT The `show_operator_as_services_root` parameter works only if the service configuration file contains the operator name inside the `<Operator>` tag. If the service configuration file does not contain the operator name inside the `<Operator>` tag, the Java GUI does not replace the Services root node with the operator name.

For more information about the service configuration file syntax, see the HPOM Administrator's Reference.

Setting the Severity Labels To set the severity labels according to your preferences, you can use the following server configuration variables:

- `OPC_JGUI_SEV_EN`
- `OPC_JGUI_SEV_ES`
- `OPC_JGUI_SEV_KO`
- `OPC_JGUI_SEV_CN`
- `OPC_JGUI_SEV_JA`

Each of these server configuration variables corresponds to one of the supported locales and is loaded when the locale is selected. The server configuration variable must have a value that consists of six severity labels separated by commas and listed in the following order: UNKNOWN, NORMAL, WARNING, MAJOR, and CRITICAL. For example:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_JGUI_SEV_EN \
this,is,new,custom,severity,label
```

If you do not want to change one or more severity labels, use the `?` character instead of a severity label. For example:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_JGUI_SEV_EN \
this,is,?,custom,severity,?
```

If you want one or more severity labels to contain white spaces, the whole server configuration variable must be within straight quotation marks. For example:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_JGUI_SEV_EN \
"unknown,normal,custom warning,my minor,major,critical"
```

If the `?` character is used within the quoted server configuration variable value, the default severity label is loaded for the corresponding severity. For example:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_JGUI_SEV_EN \
"unknown,normal,?,my minor,major,critical"
```

NOTE   If the value of the server configuration variable has fewer or more than six labels, the value is ignored and the default severity labels are loaded.

Enhanced Message Forwarding in Flexible Management Environment

Message forwarding in flexible management environment is enhanced as follows:

- Server-to-server message forwarding between HPOM 8.xx and HPOM 9.xx using the HTTPS protocol is supported.

- When no keyword (`MSGCONTROLLINGMGR | NOTIFYMGR`) is set with HPOM 9.xx, `MSGCONTROLLINGMGR` (normal messages) is assumed. With HPOM 8.xx, if no keyword was provided, the read-only messages were displayed by default (`NOTIFYMGR` was assumed).

- It is no longer required to restart the management server to read a modified `msgforw` file. It is however necessary to run the `ovconfchg` command (without options) to read a modified configuration.

- Enabled filtering based on CMAs. CMA value can contain an expression for the pattern matching.

  Syntax: `CMA NAME "<name>" VALUE "<pattern>"`

NOTE   CMA names can be used with an "`|`" (`OR`) operator.

Example of accepting all messages which have CMA `cma1` or `cma2` set:

`CMA NAME "cma1|cma2" VALUE "<*>"`

Construct patterns like in policy conditions.

- In addition to already existing filters, it is possible to filter by CMA, `ownership` and `last_time_received`. These filters are only available on the command line (not in the interactive mode). The `ownership` filter allows filtering for ownership of messages. Possible values are `ME`, `OTHER`, and `UNOWNED`. The `last_time_from` and `last_time_to` filters use the same format as `time_from` and `time_to`. However, they use the `last_time_received` field of a message for filtering.

  The CMA filter allows filtering for one or more CMAs. Make sure that you prefix the CMA name with `CMA:` and use the notation `CMA:<CMA-name>=<value>`. If multiple CMA filters are specified, all of them must match.

- Nodes can be filtered with patterns:

  Construct patterns like for external nodes. Any one of the patterns specified in one line will match.

  Syntax: NODEPATTERN *<pattern_type>* "*<pattern>*" [*<pattern_type>* "*<pattern>*" [...]]

  In this instance, *<pattern_type>* can be either IPPATTERN or NAMEPATTERN.

  Example of matching all nodes, which IP address is 192.168.*.*:

  NODEPATTERN IPPATTERN "192.168.<*>.<*>"

  Example of matching the nodes, which hostname is *.hp.com:

  NODEPATTERN NAMEPATTERN "<*>.hp.com"

- Enabled filtering on node groups:

  Syntax: NODE NODEGROUP "*<node_group>*" [NODEGROUP "*<node_group>*" [...]]

- The /opt/OV/contrib/OpC/mom/addmsgforwmgr.sh utility is now available for adding a manager to the msgforw file.

Integrating a New Management Server into an Existing Flexible Management Environment

Synchronizing messages in a flexible management environment when a new management server is to be added is enhanced by introducing the opcactdwn and opcactupl command line interfaces for downloading and uploading active messages. With the -target_mgmtsv option that is available with opcactdwn, the active messages in the database are prepared to be handled as "forwarded" messages. This means that later message operations such as adding annotations, acknowledging, and owning are synchronized.

To integrate a new management server into an existing flexible management environment, follow these steps:

1. Install the new management server and upload configuration data.

2. Stop the HP Operations management server processes on the new management server.

3. Clear the active messages on the new management server by running the following command:

   /opt/OV/bin/OpC/opcdbinst -act

4. Prepare or update the msgforw file for the old and new management servers (for example, add the new management server to the old management server's msgforw file).

5. Activate the message forwarding modification on the old management server or servers by using ovconfchg. New incoming messages and message operations are buffered for the new management server on the old management server or servers.

6. Copy the msgforw file to the new management server.

7. Download the active messages by running the following command on the old management servers:

   opcactdwn -file *<act_msgs>* -target_mgmtsv *<new_server>*

   By doing this, existing messages are prepared for later message operations such as adding annotations, acknowledging, and owning so that they can be synchronized from each old management server to the new management server.

8. Copy the active message download files from one of the old management servers (whichever you choose) to the new management server.

9. Upload the active messages on the new management server by running the following command:

   opcactupl *<act_msgs_file>*

10. Start the HP Operations processes on the new management server by running the following command:

    `ovc -start`

NOTE	The same procedure can be used later on to synchronize management servers if they are out of synchronization (for example, if queue files or the SnF forwarding buffer on the target management server had to be cleared).

Enhanced HPOM Backup and Restore

HPOM backup and restore are enhanced. New backup scripts `opcbackup_online` and `opcbackup_offline` and restore scripts `opcrestore_online` and `opcrestore_offline`, which are based on the Oracle Recovery Manager (RMAN), are introduced.

The `opcbackup_online` and the `opcrestore_online` tools support the local and remote database installation. The `opcrestore_offline` and `opcrestore_online` scripts can automatically restore backed up data of a local database without user intervention even if control files or the complete database are missing. The support for using `opcbackup_online` and `opcbackup_offline` with a remote database is enhanced.

Enhanced CLIs

The following command line interfaces are enhanced:

- opcack
- opcagtdbcfg
- opcappl
- opccfgupld

- opccfguser
- opccmachg
- opccsa
- opcdelmsg

- opchbp
- opchistdwn
- opclaygrp
- opcnode

- opcpolicy
- opcragt
- opcsrvconfig
- opctempl

For details about command line interface changes and enhancements, see the corresponding manual pages.

Enhanced APIs

New functions in APIs are the following:

- The `opcdata_set_*` API was enhanced to allow setting the CMAs in the message filter data structure. The message keys filtering is not enabled yet.

- The `opctemplfile_*` and `opctempl_*` APIs are adapted to be backward compatible. It is now possible to add the HPOM 8.xx templates (for example, for the NNMi integration) by using the `opctempl -add` command.

- Configuration Stream Interface (CSI) is an extension of the Message Stream Interface (MSI) for synchronizing the configuration changes. CSI provides registration for the configuration changes to the internal (server processes, Java GUI) and external (API clients) configuration consumers. It can be used within the `opcif_open()` API. New interface types include:

  `OPCSVIF_CFG_CHG_EVENTS` enables registration for all configuration changes.

  `OPCSVIF_CFG_CHG_EVENTS_GUI` used with Java GUI to enable registration of events related to a specific operator.

- `OPCDATA_CSI_STRING (int)` is added to the `opcconn_get_capability()` and `opcconn_set_capability()` APIs. It returns the name of the client that opened a CSI with the `opcif_open()` call, and is used to prevent this client from getting back its own configuration changes.

- `opcsync_inform_server()` is enhanced to inform the server and GUI processes of new configuration changes. The HPOM server and GUIs are kept up-to-date each time a change is performed.

- The `opcmsg_get_instructions()` C API function, which is used by the HP Operations Manager i (OMi) and HPOM web services, resolves the instruction interface text by running the specified action.

  To avoid that the API hangs, a timeout of 120 seconds is set. You can adjust the timeout period by using the `OPC_API_INSTRIF_TIMEOUT` server configuration variable.

NOTE   If you do not want to accept this default behavior, you can configure the API not to resolve the instruction interface text. To do this, set the `OPC_API_NO_INSTR_IF` server configuration variable to `TRUE`.

Other Enhancements

Other enhancements with this release are the following:

- The Hotfix deployment tool is now installed with the product. Hotfix Deployment tool supports hotfixes for Lcore, CODA and EA AGENT binaries. Because the tool uses the `sp` option of `ovdeploy`, the `ovdeploy` version should be 06.20.052 or higher on the management server and on the managed node.

- HPOM is enhanced to enable importing of the SNMP trap policies from the third-party tools, such as `mib2policy`.

- When migrating from HPOM 8.xx and uploading HPOM 8.xx configuration by using the `opccfgupld` command, the DCE nodes are added as `ip/other/other`. This allows forwarding HPOM 8.xx messages.

- To synchronize the HPOM node bank with the HP Performance Manager node list, the following new script is available:

  `/opt/OV/contrib/OpC/OVPM/ovpm_import_nodes.pl`

- The `ovdbstat` contributed tool is provided in the `/opt/OV/contrib/OpC/ovdbstat.tar` package. The package contains a readme file, an example output, and required scripts.

- The `ovoupgrade_9.0x` script is enhanced to redeploy default policy types so that the `server_and_or_agent` field is recreated in the `opc_policy_type` table.

NOTE   During the upgrade procedure, when the `ovoupgrade_9.0x` script asks to manually install available server patches, you must install HPOM 9.10.200 management server patch. The `ovoupgrade_9.0x` script then automatically reuploads default policy types and recreates the `server_and_or_agent` field in the `opc_policy_type` table.

If the patch is installed after the upgrade procedure is finished, you must run the following command to redeploy default policy types and recreate the `server_and_or_agent` field in the `opc_policy_type` table:

`# /opt/OV/contrib/OpC/reupload_policy_types.sh`

- HPOM now supports Network Address Translation (NAT) for message forwarding between HP Operations management servers in a flexible management environment.

- The `sel_nodes` report is enhanced to reflect when the SSH installation method is used.

- The `itochecker` tests can now be skipped on the passive cluster node by adding the `p` option to other options (for example, `itochecker -12345p`).

- The service engine now transforms and sends detailed configuration change events for services and service associations to Service Discovery (needed for DMOM).

- The outage template syntax is enhanced so that it contains a new keyword, `DELAY`, which is used to delay matching messages for a given number of minutes.

- Setting custom message attributes based on different message conditions (for example, a node name, an IP address, a message text, severity, and so on) is introduced. A new configuration file, `msgmodify`, is introduced. This file allows message matching based on various attributes.

- The `itochecker` tool can be used with a remote database.

- It is now possible to assign an instrumentation category to a policy group, not only to a policy.

- Operators are now able to acknowledge and unacknowledge, as well as own and disown messages when nodes are disabled.

- When a PAM authentication is enabled (`OPC_USE_PAM_AUTH` variable is set to `TRUE`) on the server, node hierarchy is assigned to a newly created user.

- When installing bootstrap HP Operations agent 11.00 on a remote node, agent patch software is also installed along with base agent version software.

- Transferring overlay files during the registration of a new platform of the HP Operations agent patch is supported.

- The `-debug` option is added to the `/opt/OV/bin/OpC/utils/opc_chk_node_res.pl` script. By using this option, you can check how long it takes to run the `gethostbyname` command.

- The failover of the Java GUIs and the managed nodes in a server pooling environment is enhanced as follows:

  — Use of "Gratuitous ARP." This means sending an ARP update on the new host of the virtual IP by using arping in the following HA Manager script:

    `/opt/OV/bin/OpC/utils/ha/ha_virtual_ip`

  — `disable_java_gui` and `enable_java_gui` can be used in the HARG start and stop scripts within the HA Manager server pooling setup. To switch the Java GUIs by using the virtual IP, create the following symbolic links:

    # **ln -s /opt/OV/bin/OpC/utils/disable_java_gui \
    /var/opt/OV/hacluster/hpom-server/K050_disable_java_gui**

    # **ln -s /opt/OV/bin/OpC/utils/enable_java_gui \
    /var/opt/OV/hacluster/hpom-server/S700_enable_java_gui**

- The following two new options can now be used with the `opchamgr` tool: `-daemon` (used for monitoring and starting the HA Manager) and `-daemon_running` (used for the daemon itself).

- The autogranting contrib tools are added to `/opt/OV/contrib/OpC/autogranting`.

Changes

HPOM contains these changes compared with HPOM 8.3x.

Installation of HPOM Management Server

New installation and configuration scripts, `ovoinstall` and `ovoconfigure`, ensure fast and simple installation and configuration. The installation process now separates the software installation from the software configuration tasks, and break and re-entry points are available for easy customization and improved troubleshooting.

For detailed information about the prerequisites which must be met before installing and configuring HPOM, and the procedures themselves, refer to the *HPOM Installation Guide for the Management Server*.

Configuration Settings on the HPOM Management Server

The table below shows how configuration variables default values are changed with the HPOM 9.xx release in comparison with the 8.xx release. Note that these settings are not visible when using `ovconfget -ovrg server` if the default has not been changed or explicitly set.

Variable	HPOM 8.xx Default	HPOM 9.xx Default
OPC_HTTPS_MSG_FORWARD	FALSE	TRUE
OPC_NAMESRV_CACHE_SIZE	100	5000
OPC_NAMESRV_RETRIES	3	1
OPC_NAMESRV_MAX_TIME	unset	200
OPC_USE_LOWERCASE	FALSE	TRUE
OPCUIWWW_BULK_MODE	FALSE	TRUE
OPCUIWWW_NEW_MSG_NO_DB	FALSE	TRUE
OPC_JGUI_WEBBRW_APPL_RESULT	FALSE	TRUE
OPC_UPDATE_DUPLICATED_SEVERITY	NONE	LAST_MESSAGE
OPC_UPDATE_DUPLICATED_MSGTEXT	NONE	LAST_MESSAGE
OPC_OPCCFGDWN_ALL_INCLUDE_ SELDIST_SERVICES	FALSE	TRUE
OPCRAGT_USE_THREADS	FALSE	TRUE
OPC_FORWM_MAX_BULK_SIZE	0	100
OPC_TTNS_TIMEOUT	0	300
OPC_MSG_BULK_INSERT_RATE	not supported	100

The behavior of some variables was changed as follows:

In the previous HPOM releases it was possible to send the Forward Manager information to the trouble-ticket system if OPC_TT_SHOW_FORW_MGR was set to TRUE. However, if a message was not forwarded, the Forward Manager information was not sent to the trouble-ticket system. Now, an empty string is sent instead of the Forward Manager information for non-forwarded messages.

Java GUI Support for Web Browsers

The embedded web browser is no longer available with the Java GUI. The only valid browsers are browsers with ActiveX and external browsers. web_browser_type in itooprc also supports activex. Thus, the valid values are external and activex.

On Windows, a browser with ActiveX is the default browser. On Unix, only external browser is available. The valid values for the configuration variable OPC_JGUI_INTERNBRW_DISABLED are ACTIVEX and NONE.

Node Management

With this release of HPOM, node names must be unique. In previous product versions it was the combination of the nodename and network type which needed to be unique. You could have the same nodename for an IP-node and a non-IP node, for example, if the name-service was not accessible when the first message for the node arrived, and later it was accessible.

HPOM 9.xx makes no difference in handling IP nodes and non-IP nodes (type "Other"). This is the same approach which was previously enforced with the `OPC_NEW_NAMERES` setting.

The handling of nodes for external events has also been changed. An external node of type "IP Name" also matches messages from non-IP nodes.

The external node type "IP Name" is changed to "Name" and the external nodes of type "Other" are converted to type "Name" during the upgrade.

The pattern matching of external nodes is now case-insensitive.

Changed Policy Names

With HPOM 9.10, the string "NT" in names of policies, policy groups, tools, and tool groups is changed to the string "Windows." For example, "NT Tools" are now named "Windows Tools."

Changed Port for HTTP Connection

The port used for connecting to the HPOM web pages was changed to 8081. For example, http://<management_server>:8081/ITO_DOC

Event Correlation Services (ECS) Support

ECS provided as Correlation Composer or ECS Designer is supported with HPOM 9.xx as follows:

- ECS Process Config File Location

    The location of the configuration for the ECS process on the management server (`opcecm`) is moved to the shared disk. This avoids certain problems in HA cluster environments.

    Old location: `/var/opt/OV/conf/OpC/mgmt_sv`

    New location: `/var/opt/OV/shared/server/datafiles/policies/ec`

- Enhanced functionality of the symbolic nodename $MGMTSV

    The symbolic nodename $MGMTSV can now be used in APIs and CLIs to:

    — Assign and deassign ECS policies or policy groups containing ECS policies to $MGMTSV, for example:

    ```
    # opcnode -[de]assign_pol node_name="\$MGMTSV" net_type=NETWORK_NO_NODE \
    pol_type=ec pol_name=<name> [ version=<ver> ]
    ```

    — List assigned policies of $MGMTSV, for example:

    ```
    # opcnode -list_ass_pols node_name="\$MGMTSV" net_type=NETWORK_NO_NODE
    ```

    The calls to deploy policies (`opcragt -dist`) and to deploy data/fact stores (`ovocomposer`) are unchanged compared to HPOM 8.xx.

- Using ECS Designer Remotely

    When you have HPOM installed on the operating system where the ECS Designer is not available, you cannot develop ECS correlation services with ECS Designer on these systems. However, you can develop them on a platform where the ECS Designer is supported (for example, Windows XP and Windows Vista) and then use these correlation services on the HPOM system where the ECS Designer is not supported.

- Verification Status of ECS Circuits

  In previous product versions, ECS circuits could not be deployed to an agent or the management server during the verification check, and were regarded as unverified. In HPOM 9.xx, the distinction between verified and unverified ECS circuits is dropped. It is expected that all ECS circuits are verified (checked for syntax correctness). For unverified HPOM 8.xx circuits uploaded during the configuration upload to HPOM 9.xx, a warning containing the relevant policy name and circuit is printed by opccfgupld. As opposed to HPOM 8.xx, the data can be deployed with HPOM 9.xx.

- A new event correlation policy is provided for policy based message storm detection. For details, see the *HPOM MessageStorm Detection whitepaper*.

- The default ECS circuit was updated with a new version of the Composer Correlator ECS circuit.

Smart Plug-in (SPI) Support

To know about supported SPI versions with HPOM 9.xx and for recent updates, see the support matrix at:

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

SPI DVD 2010 for HPOM 9.xx includes SPIs for Linux.

You can migrate the HPOM 8.xx configuration data to HPOM 9.xx. This includes templates and instrumentation of SPIs from the 2008.1 SPI CD that are installed on HPOM 8.xx, downloaded from, and then uploaded to HPOM 9.xx. To migrate SPI from HPOM 8.xx to HPOM 9.xx, first upgrade the HP Operations management server to version 9.xx, and then migrate the SPIs from HPOM 8.xx to HPOM 9.xx. For more details, see the *Release Notes* of the respective SPI.

NOTE	The existing Infrastructure SPI 1.6 is supported with HPOM 9.xx. The Infrastructure SPI DVD release cycle is separate from main stream SPI DVD.
	The existing HPOM SPIs (from 2006.1 SPI CD and 2008.1 SPI CD) cannot be installed on HPOM 9.xx.

Other Changes

Other changes with this release:

- The MGMTSV_KNOWN_MSG_NODE_NAME variable can now be used in message key relations.

- A new OpenVMS agent based on the agent version 8.60 is available.

- A new contrib tool, the /opt/OV/contrib/OpC/om_server_switch.sh script, is introduced.

  Usage:

  ```
  /opt/OV/contrib/OpC/om_server_switch.sh <new_long_hostame> <new_IP_Address> \
  <old_long_hostame> <old_IP_Address> [ nowait ]
  ```

  It makes it easier to ignite or clone an additional HPOM server by using an image template. Such an image needs some modifications which are done through this script. The script can do the following:

  — Change internal OM related configuration files.

  — Change DB listener files to the new hostname and IP address.

  — Create a new ovcoreid for the local agent and management server.

  — Create a new set of node and root certificates.

— Restart Oracle, OM server, and the local agent.

— Clean policy cache.

— Deploy policies to a local agent.

— Install a new license (manually).

- It is now possible to have duplicate IP addresses in the database. In such a case, make sure that the different nodes with the same IP address can be reached through HTTPS proxies, because normal routing does not work with the same IP. Also, HBP must be set to RPC only. This is because you cannot use the `ping` command, which can lead to errors.

  You can enable this feature by setting the following configuration variable:

  # ovconfchg -ovrg server -ns opc -set OPC_ALLOW_DUPLICATE_IP TRUE

- It is now possible to ignore an IP address mismatch in the certificate request. You can enable this feature by setting the following configuration variable:

  # ovconfchg -ovrg server -ns opc -set OPC_CSA_ALLOW_IP_MISMATCH TRUE

Integration with Other HP Software Solutions

HPOM 9.xx provides integrations with other HP Software solutions, such as Network Node Manager i (NNMi), Business Availability Center (BAC), and Dependency Mapping Automation (DMA). For a complete list and more information, visit the Support web site:
http://support.openview.hp.com/sc/integration_catalog.jsp

SiteScope

When using the HPOM SiteScope Adapter in conjunction with SiteScope 10.10 and newer versions, explicitly enable the creation of SiteScope group MG files, because it is not selected by default when SiteScope is installed. (See also the *SiteScope Release Notes*.) Enable the configuration files option in **Preferences -> General Settings -> Main Panel**. When upgrading from an earlier version of SiteScope that has this option selected, the MG configuration files are supported. The SiteScope discovery is not available, if the option is disabled.

Coexistence with Other HP Software Solutions

HPOM 9.xx can coexist on the same system with the following HP Software products:

- HPOM Java GUI 9.xx
- HP Operations Agent 8.60
- HP Operations Agent 11.00
- HP Operations Agent 11.10
- HP Performance Agent 5.00
- HP Performance Manager 8.21
- OM Dependency Mapping Automation 8.20
- SiteScope 11.1x

HPOM 9.xx cannot be installed on the same system with some HP Software products. The following HP Software products can be used with HPOM but must be installed on a remote system:

- SiteScope 10.10
- Network Node Manager i (NNMi) 8.xx and 9.xx

Obsolescence Announcements

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

NOTE   This section applies for users that migrate to HPOM 9.10 from HPOM 8.xx.

Obsolete Java GUI Platforms

- HP-UX PA-RISC all versions

- HP-UX Itanium 11.23

- Sun Solaris 8 and 9

- Red Hat 8

- Mac OS X 10.3 and lower versions

The HPOM Java GUI no longer supports the embedded browser capability.

Obsolete HPOM Agent Platforms

- HP MPE/iX
- HP-UX 10.20, 11.00, 11.22 (Itanium)
- Linux Kernel 2.2 and 2.4, all derivatives
- Microsoft Windows 2000 (all editions; unless there is an extended Microsoft support contract)
- Microsoft Windows 2003 without SP

- Microsoft Windows NT 4.0
- Microsoft Windows XP (SP1 and prior)
- Novell NetWare 4.x
- OpenVMS 7.3.1
- RedHat Enterprise Linux 2.1, 3.x
- Tru64 UNIX

Motif UI

The Admin Motif UI is obsolete. The Web-based Administration UI is used instead. For more information about the new Administration UI, see "Web-based Administration for HPOM" on page 11.

The operators Motif UI is obsolete; use the Java GUI instead.

Template Administrator

The template administrator user is obsolete as a part of a Motif UI functionality. You cannot use template administrator users to log in to the HPOM Administration UI. If you upload or create a template administrator user on HPOM, it is not used for HPOM Administration UI.

Instead of template administrator, use `ompolicy_adm` user to log in to the HPOM Administration UI or add a new HPOM Administration UI user and assign it to `ompolicy_adm` user group. An HPOM Administration UI user has rights to view and edit all policies. You should first log in as `admin` or `opc_adm` to the HPOM Administration UI, add a Policy administrator user, and assign that user the ompolicy_adm user group.

A utility is also provided to convert template administrator accounts into HPOM `ompolicy_adm` accounts. Refer to the *HPOM Administration UI Administration and Configuration Guide*, chapter "User Migration from HPOM 8.xx to AdminUI" for details.

DCE Communication

The DCE obsolescence includes the obsolescence of DCE-based agents, of communication to and from DCE-based agents, DCE-based message forwarding between management servers, escalating messages, the DCE security (the security library), the OpenAgent architecture, as well as Novell Netware agent, the RPC daemon agent, and Sun RPC agent. Also, the DCE RPC based communication on the HPOM management server has been changed to a queue and pipe mechanism.

HPOM Server to Server Configuration Upload with the opcmgrdist utility

Server to server configuration upload with the `opcmgrdist` utility is no longer supported. You can download configuration data on server A with `opccfgdwn`, copy the configuration data, for example, with secure copy (`scp`) to server B, and upload it there with `opccfgupld`.

Operator-initiated Message Escalation

The possibility to forward or escalate an HPOM message to another HPOM server by pressing the escalate button in the HPOM operational UIs is obsolete.

Obsolete Management Server Processes

The following HPOM processes are obsolete:

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

libnspsv Library

The libnspsv library is deprecated. However, it is still present on the HP Operations management server for backward compatibility. You can still use the integrations, applications or scripts linked to this library in previous product versions.

Changed Control over HPOM Processes

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

NNM 7.x Integration

NNM 7.x cannot be installed on the same system as HPOM and cannot be integrated with HPOM, thus the integration with NNM is obsolete. As a consequence of this, HPOM does not support integration with the `OV_PLATFORM` type applications, for example, `OV Applications` and `OV Services` are not used anymore. Also, the `netop` and `itop` operators are obsolete.

The `opcctrlovw` fileset is not provided with the HPOM installation, but it can be migrated from the previous product versions.

Service Navigator Value Pack (SNVP)

No new version of SNVP is available with the HPOM 9.xx. Check the HP Dependency Mapping Automation software and HP Operations Manager i software as potential replacements.

Obsolete CLIs and CLI options

All CLIs provided by NNM are no longer available on the HPOM management server. Therefore CLIs such as ovstart, ovstop, ovstatus, ovw, ovaddobj no longer exist. Check your working procedures and scripts for NNM commands and make the adjustments, where appropriate. Other obsolete CLIs:

- opc_backup
- opc_recover
- opcauddwn
- opccfgdwn: the -subproduct and -platform options
- opccfgupld: the -ascii option
- opccfgupld: the -deloldtempls option
- opclic
- opcmgrdist

- opcmomchk: the -escalation option
- opcpwd
- opcsvreg
- opcsvskm
- opctmplrpt
- opctranm
- ovbackup.ovpl
- ovrestore.ovpl

NOTE	The opcccfgupld -ascii option is listed when opccfgupld -help is invoked and it is described in the opccfgupld manual page.

Obsolete Configuration Variables

- DCEMR_PROG
- DISTM_PROG
- LISTENER_NAME
- 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

Obsolete APIs

- opcsync_inform_user()
- opcmsg_escalate()

Obsolete Documentation

The following manuals are no longer available with HPOM:

- *Service Navigator Concepts and Configuration Guide*

  Note, that the information contained in this guide was distributed among other HPOM manuals, for example, *HPOM Administrator's Reference* and *HPOM Java GUI Operator's Guide*.

- *HPOM Developer's Reference*
- *HPOM Application Integration Guide*
- *HPOM Security Advisory Guide*

Miscellaneous

- NIS+ is not supported as it is no longer available on RHEL, LDAP is used instead.
- ECS Designer is not supported on the management server.
- Expressions `<S>` and `<nS>`

  The pattern-matching expressions `<S>` and `<nS>` used in templates are obsolete.
- Obsolete `itooprc` parameters

  — `which_browser`

  — `auto` and `manual` values for `web_browser_type`

  — `ice_proxy*`

  — `web_browser_html_appl_result`
- Obsolete values for configuration variable `OPC_JGUI_INTERNBRW_DISABLED`

  — `EMBEDDED`

  — `BOTH`
- Obsolete port used for connecting to HPOM web pages: `3443`
- Hide Node Group from Responsibilities field

  The Hide Node Group from Responsibilities field of a node group is not used in HPOM 9.xx anymore. Use the Edit View functionality in the Administration UI instead.

Installation Notes

Installation requirements and instructions for installing HPOM, are documented in the *HPOM Installation Guide for the Management Server*. After installation the document can be found at:

`/opt/OV/www/htdocs/ito_doc/C/manuals/InstallationGuide.pdf`

To check for recent updates or to verify that you are using the most recent edition, go to the HP Support web site.

HPOM 9.xx introduces a new approach to product installation and configuration. Installing and configuring the HPOM software on the management server are fast and easy procedures due to the HPOM installation and configuration scripts, `ovoinstall` and `ovoconfigure`, which guide you through the entire installation and configuration procedure.

For general installation requirements, see Chapter 1, "Installation Requirements for the Management Server" of the *HPOM Installation Guide*.

For detailed information about the prerequisites, which must be met before installing and configuring HPOM, and the procedures themselves, refer to the *HPOM Installation Guide for the Management Server*.

The `README.txt` readme file located on HPOM media DVD describes the HPOM media DVD contents and layout and helps you to locate products and documentation.

Hardware Requirements

Make sure that your system meets the following hardware requirements:

• HP Operations agent 8.xx requires 300 MB of disk space, while its installation or upgrade requires 600 MB. Starting with HP Operations agent 11.00, the required disk space for the HP Operations agent varies depending on the platform. For detailed information about disk space requirements, see the HP Operations agent documentation.

Software Requirements

This section lists additional software requirements that are not documented in the HP support matrices. To check for recent updates on the HP Operations management server and HP Operations agent supported operating systems, visit the following URL:

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

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Management Server

For detailed information about the management server software requirements, refer to the *HPOM Installation Guide for the Management Server.*

Refer to Chapter 2 of the *HPOM Installation Guide for the Management Server* for detailed instructions on how to install HPOM, and to "Known Problems, Limitations, and Workarounds" on page 50 for known problems and their workarounds.

NOTE	It can be very helpful to set the PATH variable to include the following HPOM directories on the management server: `/opt/OV/bin`, `/opt/OV/bin/OpC`, `/opt/OV/nonOV/perl/a/bin` and `/opt/OV/bin/OpC/utils`.

Likewise, export the MANPATH variable to access HPOM manual pages:

```
export MANPATH=$MANPATH:/opt/OV/man
```

Oracle Database

The supported Oracle database versions are 11g Release 1 with 11.1.0.7 Patch Set and 11g Release 2 (versions 11.2.0.1, 11.2.0.2, and 11.2.0.3). These Oracle database versions must be installed to provide important enhancements in security and reliability.

NOTE	Oracle 11gR2 version 11.2.0.3 is supported by HPOM also in remote database and RAC environments.

The Oracle compatible parameter specifies the release with which Oracle must maintain compatibility. By default, an HPOM installation sets the Oracle compatible parameter to 11.1.0.0.

IMPORTANT	Install the Oracle binaries *before* the HPOM 9.xx installation, but *do not* create any kind of database, because HPOM requires specific settings.

Oracle 11g Release 2 operating system requirement is Red Hat Enterprise Linux 4 Update 7 or Red Hat Enterprise Linux 5 Update 2.

Several prerequisite OS packages need to be installed for the Oracle database. You can find them at the following location:

- **For Oracle 11.1:**

  http://docs.oracle.com/cd/B28359_01/install.111/b32285/toc.htm

  Required package versions (or later):

```
compat-libstdc++-33-3.2.3-61
elfutils-libelf-0.125-3.el5
elfutils-libelf-devel-0.125-3.el5
glibc-2.5-12
glibc-devel-2.5-12
glibc-common-2.5-12
gcc-4.1.1-52.el5
gcc-c++-4.1.1-52.el5
kernel-headers
libgcc-4.1.1-52.el5
libaio-0.3.106-3.2
libaio-devel-0.3.106-3.2
libstdc++-4.1.1-52.el5
libstdc++-devel-4.1.1-52.el5
lm_sensors-2.10.0-3.1
```

```
net-snmp-5.3.1-19.el5
net-snmp-utils-5.3.1-19.el5
unixODBC-2.2.11-7.1
unixODBC-devel-2.2.11-7.1
sysstat-7.0.0-3.el5
binutils-2.17.50.0.6-2.el5
make-3.81-1.1
```

- **For Oracle 11.2:**

  http://docs.oracle.com/cd/E11882_01/install.112/e24326/toc.htm

  Required package versions (or later):

```
binutils-2.17.50.0.6
compat-libstdc++-33-3.2.3
compat-libstdc++-33-3.2.3 (32 bit)
elfutils-libelf-0.125
elfutils-libelf-devel-0.125
gcc-4.1.2
gcc-c++-4.1.2
glibc-2.5-24
glibc-2.5-24 (32 bit)
glibc-common-2.5
glibc-devel-2.5
glibc-devel-2.5 (32 bit)
libaio-0.3.106
libaio-0.3.106 (32 bit)
libaio-devel-0.3.106
libaio-devel-0.3.106 (32 bit)
libgcc-4.1.2
libgcc-4.1.2 (32 bit)
libstdc++-4.1.2
libstdc++-4.1.2 (32 bit)
libstdc++-devel 4.1.2
make-3.81
sysstat-7.0.2
unixODBC-2.2.11
unixODBC-2.2.11 (32 bit)
unixODBC-devel-2.2.11
unixODBC-devel-2.2.11 (32 bit)
```

Packages can be obtained from the official operating system site.

By default, HPOM uses port 1521 for Oracle listener. If you want to use this port, make sure that the ncube port is commented out in /etc/services (if this file exists on your system):

```
# cat /etc/services |grep ncube
#ncube-lm 1521/tcp # nCube License Manager
#ncube-lm 1521/udp # nCube License Manager
```

For detailed information about installing and setting up the Oracle database, see the *HPOM Installation Guide for the Management Server*.

Upgrading the Oracle Database

When upgrading the Oracle database, you must perform the following tasks:

- Task 1: Checking System Requirements

- Task 2: Before Upgrading the Oracle Database Installation

- Task 3: Upgrading the Oracle Database Installation

- Task 4: Preparing the New Oracle Database to Be Used with the HP Operations Management Server

---

NOTE	It is recommended that you back up your system before upgrading the Oracle database.

Checking System Requirements Make sure your system meets the requirements stated in the Oracle documentation. There might be a difference in required operating system versions, patches, and kernel parameters for different Oracle versions.

Before Upgrading the Oracle Database Installation Before you upgrade an Oracle database installation, follow these steps:

1. As the root user, create the directories required by the Oracle installation, and then change the ownership and set correct permissions.

   For example, run the following commands:

   umask 022

   mkdir -p /opt/oracle/product/11.2.0

   chown -R oracle:oinstall /opt/oracle/product/11.2.0

   chmod 755 /opt/oracle/product/11.2.0

2. As the root user, set the Oracle environment variables in /home/oracle/.profile of the oracle user as follows:

   export ORACLE_SID=openview

   export ORACLE_BASE=/opt/oracle

   export ORACLE_HOME=$ORACLE_BASE/product/11.2.0

   export ORACLE_TERM=hp

   export PATH=$PATH:$ORACLE_HOME/bin

Upgrading the Oracle Database Installation When upgrading the Oracle database installation to a higher version, you first install a new Oracle RDBMS version, and then upgrade the existing Oracle database to this new version.

IMPORTANT	The procedure described in "Upgrading the Oracle Database from Version 11.1.0.7 to Version 11.2.0.3" on page 41 can be generally used for upgrading any Oracle database version, but you must make sure that the values in the old ORACLE_HOME directory and the new one differ if you upgrade from 11.1.0.7 to any of the supported Oracle database 11g Release 2 versions (that is, the values may not be 11.2.0 in both directories).

Upgrading the Oracle Database from Version 11.1.0.7 to Version 11.2.0.3

To upgrade the Oracle database from version 11.1.0.7 to version 11.2.0.3, follow these steps:

1. As the `oracle` user, start the Oracle Universal Installer of the new Oracle database version to which you want to upgrade the existing Oracle database version. To do this, run the following command:

   `<path>/runInstaller`

   In this instance, `<path>` is the full path of the database directory on the installation media.

   After the Oracle Universal Installer is started, follow the instructions for installing the Oracle database described in the HPOM Installation Guide for the Management Server.

2. In another window, as the `oracle` user, stop the current listener by running the following command:

   `/opt/oracle/product/11.1.0/bin/lsnrctl stop LISTENER`

3. Copy the `sqlnet.ora`, `tnsnames.ora`, `tnsnav.ora`, and `listener.ora` files from `/opt/oracle/product/11.1.0/network/admin/` to the following location:

   `/opt/oracle/product/11.2.0/network/admin/`

   To do this, run the following commands:

   `cp /opt/oracle/product/11.1.0/network/admin/sqlnet.ora \`
   `/opt/oracle/product/11.2.0/network/admin/`

   `cp /opt/oracle/product/11.1.0/network/admin/tnsnames.ora \`
   `/opt/oracle/product/11.2.0/network/admin/`

   `cp /opt/oracle/product/11.1.0/network/admin/tnsnav.ora \`
   `/opt/oracle/product/11.2.0/network/admin/`

   `cp /opt/oracle/product/11.1.0/network/admin/listener.ora \`
   `/opt/oracle/product/11.2.0/network/admin/`

NOTE Make sure that you manually change `11.1.0` to `11.2.0` in all files under `/opt/oracle/product/11.2.0/network/admin/`.

Check that all values in the files under `/opt/oracle/product/11.2.0/network/admin/` are `11.2.0` by running the following command:

`grep 11.1.0 /opt/oracle/product/11.2.0/network/admin/*`

The `listener.ora` file should look as follows:

```
LISTENER =
  (ADDRESS_LIST =
       (ADDRESS=
          (PROTOCOL=IPC)
          (KEY= openview)
       )
       (ADDRESS =
         (PROTOCOL = TCP)
         (HOST = <hostname>)
         (PORT = 1521)
       )
  )
CONNECT_TIMEOUT_LISTENER = 10
LOG_DIRECTORY_LISTENER = /opt/oracle/product/11.2.0/network/log
LOG_FILE_LISTENER = LISTENER
SID_LIST_LISTENER =
  (SID_LIST =
```

```
    (SID_DESC =
      (SID_NAME=openview)
      (ORACLE_HOME=/opt/oracle/product/11.2.0)
    )
  )
  TRACE_LEVEL_LISTENER = OFF
```

4. If the listener for 11.2.0 is not started automatically, as the `oracle` user, run the following command:

   /opt/oracle/product/11.2.0/bin/lsnrctl start LISTENER

5. After exiting the Oracle Universal Installer, run the `utlu112i.sql` script as described in the "Upgrading to the New Release of Oracle Database" chapter of the *Oracle Database Upgrade Guide 11g Release 2 (11.2)* and resolve all warnings.

IMPORTANT	The `utlu112i.sql` script must be run from the environment of the database being upgraded.

---

6. Run the Oracle Database Upgrade Assistant to upgrade the database software. Make sure that you carefully follow the instructions described in the *Oracle Database Upgrade Guide 11g Release 2 (11.2)*. When asked whether to use the Automatic Storage Management option, select **Do Not Move Database Files as Part of Upgrade**.

IMPORTANT	When modifying any of the existing HPOM Oracle database settings, make sure that you update the corresponding configuration entries inside the Administration UI. Otherwise, the Administration UI will not be able to connect to Oracle.
	For detailed information about modifying the Administration UI environment, see the *Administration UI Administration and Configuration Guide* that you can download from the following location:
	http://support.openview.hp.com/selfsolve/manuals

Preparing the New Oracle Database to Be Used with the HP Operations Management Server To prepare the new Oracle database to be used with the HP Operations management server, follow these steps:

1. Change `11.1.0` to `11.2.0` in the `/etc/opt/OV/share/conf/ovdbconf` file.

2. Make sure that `libclntsh` is linked to the correct library from the new Oracle database by following these steps:

   a. Run the following commands:

      cd /opt/OV/lib64

      **rm -f libclntsh.so libclntsh.so.1.0 libclntsh.so.10.1 libclntsh.so.11.1 \
      libopcora.so libnnz11.so**

   b. Link the libraries by running the following commands:

      ln -s /opt/oracle/product/11.2.0/lib/libclntsh.so libclntsh.so

      ln -s /opt/oracle/product/11.2.0/lib/libclntsh.so libclntsh.so.1.0

      ln -s /opt/oracle/product/11.2.0/lib/libclntsh.so libclntsh.so.10.1

      ln -s /opt/oracle/product/11.2.0/lib/libclntsh.so libclntsh.so.11.1

```
ln -s /opt/oracle/product/11.2.0/lib/libclntsh.so libopcora.so

ln -s /opt/oracle/product/11.2.0/lib/libnnz11.so libnnz11.so
```

c. Restart the HP Operations management server processes by running the following command:

```
/opt/OV/bin/ovc -start
```

IMPORTANT   If you decide to remove the HP Operations management server, change 11.1.0 to 11.2.0 in the /opt/OV/bin/OpC/install/defaults.conf file before you run the ovoremove script with the -u option.

You must also make sure that /var/opt/oracle/oratab contains the proper string of the upgraded Oracle database (for example, openview:/opt/oracle/product/11.2.0:N).

Java GUI

Before installing the HPOM Java GUI, ensure that your system meets the hardware and software requirements described in this section.

HPOM bundles the JRE for all supported platforms. The JRE for MS Windows platforms is available through the latest Java GUI patch, while the JRE for all other platforms is available through the latest server accessories patch.

Table 5   Support Matrix - Java GUI

Java Runtime	JRE	JRE Plug-in	JRE Plug-in	JRE Plug-in	JRE Plug-in
TYPE	**as Application**	**Internet Explorer (32-bit)[a] 6 or higher**	**Safari 5.x**	**Mozilla Firefox[b] 17**	**Chrome**
Windows 2000 Windows XP Windows 2003 Windows Vista Windows 7	1.7.0_07	1.7.0_07	N/A	1.7.0_07	1.7.0_07
Windows 2003 for HP-UX on HP integrity	N/A	1.7.0_07	N/A	1.7.0_07	1.7.0_07
Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 Red Hat Enterprise Linux 6.0, 6.1, 6.2, 6.3	1.7.0_07	N/A	N/A	1.7.0_07	1.7.0_07
Solaris 10	1.7.0_07	N/A	N/A	1.7.0_07	1.7.0_07
HP-UX 11i v3 on HP Integrity	1.7.0_07	N/A	N/A	1.7.0_07	N/A
Mac OS X Mac OS X running on Intel processors	1.7.0_07	N/A	1.7.0_07	1.7.0_07	1.7.0_07

a. The 64-bit version of Internet Explorer is not supported.

b. This is the recommended browser because all platforms support it.

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

https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXJDKJRE60

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

`export JAVA_DIR=/opt/OV/nonOV/jre/b`

NOTE	If you still have HPOM 8.xx management servers in your environment, you can use the Java GUI for HPOM 9.xx to connect to such management servers.

HP Operations Agents

HPOM 9.10 is delivered with HP Operations agent 8.60. HPOM 9.10 can also communicate with other 8.xx HP Operations agents as well as HP Operations agent 11.00 and higher. For more information about the supported HP Operations agent versions, platforms, known problems and workarounds, see the *HP Operations Agent Release Notes* which can be found at the following location: http://support.openview.hp.com/selfsolve/manuals

As a prerequisite for the HP Operations agent installation, your system must meet operating system specific software and hardware requirements. Supported platforms and requirements can be found online at the following location: http://support.openview.hp.com/selfsolve/document/KM323488

To properly perform the HP Operations agent installation, consider the following:

- 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
```

- The installation of the HP Operations agent version 11.03 or higher with the Force option reads the profile file. You must set the configurable values such as the MINPRECHECK option in following file:

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

These values are then stored in the profile file and read when the agent installation with the Force option is performed.

IMPORTANT	Make sure you have either REXEC, RSH, or SSH services enabled on the remote agent before you start the HPOM agent installation from the HPOM management server. Otherwise the agent installation fails.

Cluster Environment

While installing and configuring the HP Operations management server on cluster nodes, make sure that cluster node names are the same as hostnames. Otherwise, the configuration fails.

NOTE	The HP Operations management server can be installed in a cluster environment in which the HP Operations agent is already installed on the cluster nodes.

Known Installation Problems and Workarounds

Symptom QCCR1A142711
ovoinstall operating system patches check fails on RHEL 6.0, 6.1, 6.2, and 6.3

When the `ovoinstall` script checks the operating system patches that are currently installed on the HP Operations management server, the check fails on RHEL 6.0, 6.1, 6.2, and 6.3.

Solution

Check manually if the reported operating system patches are installed on the system. To do this, run the following command:

```
ovoconfigure -check patches
```

Symptom QCCR1A133792
HPOM 9.10 installation changes the owner ID of the /etc directory

When HPOM 9.10 is installed, the installation changes the owner ID of the `/etc` directory to the `bin` user and group.

Solution

After HPOM 9.10 is installed, manually restore the owner ID of the `/etc` directory to the original value.

Symptom QCCR1A95802
Wrong entry in /etc/hosts file after RHEL OS is installed from a template using VMware

If you have installed your RHEL system using VMware from a template, check the following line in your `/etc/hosts` file:

```
127.0.0.1        localhost.localdomain localhost
```

Sometimes, VMware template deployment changes this entry (adds a hostname within), which can cause problems during the HP Operations management server installation.

Solution

If this line is not like above, correct it before installing the HP Operations management server.

Symptom QCCR1A108869: Errors during deinstallation or upgrade

At the management server deinstallation or upgrade, the following errors may occur, if some product that depends on the same packages as the HP Operations management server is left on the system:

- Deinstallation:

```
 ERROR:     Error occurred while removing HPOvTomcatB package
    Please check /var/opt/OV/log/OpC/mgmt_sv/installation.log.error
    for details
```

- Upgrade:

```
Removing local Agent . . . . . . . . . . . . . . OK
Removing SPIs  . . . . . . . . . . . . . . . . . OK
Stopping Server  . . . . . . . . . . . . . . . . OK
```

```
Removing database   . . . . . . . . . . . . . . . OK
Removing documentation . . . . . . . . . . . . . OK
Removing Agent software  . . . . . . . . . . . . FAILED
```

Solution

Before proceeding with the deinstallation or upgrade, check the log file. If a dependency on other packages caused the error, see if you can remove the packages that caused the dependency. After you remove these packages, repeat the deinstallation or upgrade as follows:

```
[repeat,skip,back,exit,?] : repeat
      Removing Agent software  . . . . . . . . . . . OK
```

If you need these packages on your system, use skip when an error occurs to continue with the deinstallation or upgrade. For example:

```
[repeat,skip,back,exit,?] : skip
```

Symptom QCCR1A98812
Remote database configuration fails with ORA-01450: maximum key length (6398) exceeded

After the HPOM is installed and the database is created as a remote database, the database configuration fails with the following error:

```
Error opcdbinst(6722) : Database: ORA-01450: maximum key length (6398) exceeded <

 (OpC50-15)

Aborting installation of HPOM tables in database. (OpC55-1)

ERROR:   Error occurred in the program opcdbinst during creation of the

      database tables.
```

Solution

Instead of the default block size of 8K for the database, use the block size of 16K as documented in the *HPOM Installation Guide for the Management Server*:

```
db_block_size 16384
```

IMPORTANT   You cannot change the specified block size afterwards. If you use the default block size, you will need to drop the database and create it again with the correct db_block_size.

Symptom QCCR1A109494
Cannot open pipe rqsccep

After HPOM is installed, the following error appears in System.txt:

```
0: ERR: Mon Jun 21 13:49:51 2010: opcdispm (8348/1): [mpisv.c:816]: Cannot open pipe
/var/opt/OV/share/tmp/OpC/mgmt_sv/rqsccep. open(2) failed.No such device or address
(OpC40-616)
```

Solution

You can safely ignore this error.

Symptom QCCR1A110546
Error appears in ovoinstall, during the local agent installation

During ovoinstall, the following messages may appear:

```
Starting Server  . . . . . . . . . . . . . . . . OK
Installing local Agent . . . . . . . . . . . . . FAILED
ERROR: Agent installation failed. Please check
/var/opt/OV/log/OpC/mgmt_sv/installation.log for details.
```

The log file contains the following:

```
...
Installing HPOvAgtEx package.
Updating HPOM database now that HPOM on system <mgmt. sv.> has been successfully installed
or activated.
ERROR:   Cannot update HPOM software status flag on database for system <mgmt. server>.
```

Solution

1. Restart the server processes as follows:

   # /opt/OV/bin/ovc –kill

   # /opt/OV/bin/ovc –start

2. Manually set the flag as follows:

   # /opt/OV/bin/OpC/opcsw –installed [<mgmt. sv hostname>]

Migration from Previous Product Versions

If you have HPOM 8.xx installed on an operating system that is not supported by HPOM 9.10 (Solaris 8 or Solaris 9, HP-UX on PA-RISC or HP-UX 11i v2 on Itanium), you can migrate it to HPOM 9.10 on a different system with a supported operating system. For details, see *HPOM Installation Guide for the Management Server*.

NOTE	With HPOM 9.10, the string "NT" in names of policies, policy groups, tools, and tool groups is changed to the string "Windows." For example, "NT Tools" are now named "Windows Tools."

When you migrate from a previous version of HPOM, you upload the old configuration to the management server. Old policies, policy groups, tools, and tool groups with the "NT" string are uploaded to the system where the new ones with the "Windows" string reside. Consequently, these objects get duplicated.

Though the duplication of objects does not affect your system, it is recommended to migrate to the new configuration. To migrate to the new configuration, assign new objects (with the "Windows" string in the name) to all nodes that have old objects (with the "NT" string in the name) deployed. The following scenarios are possible:

- If you have custom policies or tools in the old policy or tool group, move them to the new policy or tool group. If such group is also assigned to a managed node, remove it and assign the new group.

- If you have old unchanged policies or tools deployed on managed nodes, deploy new policies or tools to these nodes and remove old ones.

- If you have old policies that were updated, copy the updated version to the new policy, remove the old policy version, and then deploy the new version of this policy.

Upgrade to HPOM 9.10

The *HPOM Installation Guide for the Management Server* contains detailed instructions on upgrading to HPOM 9.10, as well as information on product versions, from which you can perform an upgrade.

Check the http://support.openview.hp.com/selfsolve/manuals web site for the latest version of the *HPOM Installation Guide for the Management Server*.

Administration UI

IMPORTANT	HPOM for UNIX 9.0.1 Administration UI cannot be upgraded to HPOM for UNIX 9.1.0 Administration UI. You must deinstall the old version, remove the obsolete files manually (`/opt/OV/OMU/adminUI`), and then install the new version.

When installing Administration UI, consider the following:

- To avoid problems because of changes in the JavaScript code of the product, make sure to clear your browser cache or use "Shift-Reload" after reconnecting to the web application server.

- For connecting to UNIX boxes, VNC may cause problems with the Install Anyway HPOM for UNIX Administration UI installer. It is recommended to use other tools.

For detailed information about prerequisites that must be met before installing and configuring Administration UI, as well as instructions for installing, see the *HPOM Administration UI Installation Guide*.

Known Problems, Limitations, and Workarounds

Management Server

Symptom QCCR1A143489
opccfgupld fails to upload policies if the index file contains DOS line endings CR+LF

If the index file contains DOS line endings CR+LF, `opccfgupld` fails with the following error:

```
Character set of download data not compatible with installed set.
+ opccfgupld terminated with 1 warning(s)/error(s)
```

Solution

To solve this problem, check the line endings in the index file. If the index file contains DOS line endings CR+LF, convert it to LF only (Unix).

Symptom QCCR1A139583
Warnings appear in the System.txt file after installing management server patch OML_00050

After the installation of management server patch `OML_00050`, the following warnings appear in the `System.txt` file on the management server:

```
0: WRN: Wed Apr 4 10:00:03 2012: opcuiwww (25030/47311614522128): [OvCorOsNls.cpp:252]: Bad
input character converting string from "UTF8" to "ucs2".
Invalid or incomplete multibyte or wide character (OpC20-274)
```

Solution

The reason for these warnings is messages containing umlauts. Because HPOM supports only UTF-8 encoding that enables the usage of multilingual characters in different HPOM elements and eliminates the problems associated with the character set incompatibility, make sure that you set up a UTF-8 based locale to avoid this problem. For details, see the *HPOM Administrator's Reference*.

An incompatible locale used in `xinetd` can also cause conversion problems. To avoid these kinds of problems, change the `ito-e-gui` configuration file so that the correct locale is set for the Java GUI. For example, to set the locale to `en_US.UTF-8`, set the environment attribute in the `/etc/xinetd.d/ito-e-gui` file as follows:

```
service ito-e-gui
{
        flags          = REUSE
        socket_type    = stream
        wait           = no
        user           = root
        server         = /opt/OV/bin/OpC/opcuiwww.sh
        env            = LANG=en_US.UTF-8 LC_ALL=en_US.UTF-8
        log_on_failure += USERID
        disable        = no
}
```

After that, restart `xinetd` by running the following command:

`# /sbin/service xinetd restart`

Symptom QCCR1A136484
opcpkgdwn tool can fail on HPOM 9.xx with the HP Operations agent version 11.00 or later

If you run the `opcpkgdwn` tool on HPOM 9.xx with the HP Operations agent version 11.00 or later, an error message might appear.

Solution

This is the expected behavior because the `opcpkgdwn` tool does not support the HP Operations agent version 11.00 or later.

Symptom QCCR1A133885
HPOM 9.xx no longer supports hidden node groups

With HPOM 9.xx, hidden node groups are no longer supported. However, if you hid a node group in HPOM 8.xx before migrating to HPOM 9.xx and it is in the responsibility of an operator, it does not show up in the Administration UI responsibility matrix.

Solution

Clear the Hide Node Group from Responsibilities box for all the node groups that are hidden (the Visible field in the All Node Groups view is not selected).

Symptom QCCR1A116035
Dependency on the obsolete PerfView component

The `ServNav` examples found in the `perf.tar` package cannot be used anymore because the package depends on the obsolete `PerfView` component.

Solution

The package will be removed because it depends on the obsolete component.

Symptom QCCR1A115800
Policy with a modified version cannot be uploaded to the database by using opccfgupld

When a policy with a modified version is uploaded to the database by using the `opccfgupld` command, the upload is unsuccessful.

Solution

To upload a modified policy, use `opctempl` instead of `opccfgupld`.

Symptom QCCR1A56839
Implications of mgrconf/configsettings being policies

Since mgrconf and configsettings are policies with HPOM 9.xx, they are disabled by `opctemplate -disable -all` and `ovpolicy -disable -all`. This can have unexpected implications. For example, running a status or an action from a management server fails, even if the server is the primary manager, unless the requesting server is configured as the default manager.

Symptom QCCR1A58840
While purging policies in MOM setup, mgrconf policies also get purged

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

Symptom QCCR1A95152
HPOM 8.xx reports may fail on HPOM 9.xx because of missing condition tables

If you upgrade HPOM 8.xx to HPOM 9.xx, you can use the HPOM 8.xx reports. However, HPOM 8.xx reports (copied or customized from HPOM 8.xx or current OV Reporter and OVPI report pack reports) may fail if they query the HPOM 9.xx database. This happens because some template and condition tables were obsolete with the HPOM 9.xx (opc_monitor_cond, opc_trap_cond, and opc_cond).

Solution

Update the HPOM 8.xx reports so that the condition from the opc_monitor_cond, opc_trap_cond, and opc_cond tables are not queried.

Symptom QCCR1A57809
Templates are still assigned to physical nodes after changing name to Virtual Node

When you run the `opc_node_change.pl` script after changing the virtual node name, the old virtual node name is not deleted. Consequently, policy assignments to the old virtual node are not changed. If you unassign policies from the new virtual node, they are still assigned to old virtual node, and are still distributed to the physical nodes.

Solution

Unassign manually policies from the old virtual node group, delete nodes from that group, and delete the group, using the `opcnode` command:

```
# /opt/OV/bin/OpC/utils/opcnode -deassign_pol_group -node_name=<node_name> \
-net_type=<network_type> -pol_group=<policy_group_name>
# opcnode -deassign_node group_name=<nodegrp_name> node_name=<node_name> \
-net_type=<network_type>
# opcnode -del_group group_name=<nodegrp_name>
```

In this instance, *<nodegrp_name>* is the old virtual node name.

Symptom QCCR1A118594
Adding or removing a physical node to or from a virtual node is not synchronized through DMOM

Adding physical nodes to a virtual node or removing physical nodes from a virtual node is not reflected within DMOM configuration synchronization between management servers.

Symptom QCCR1A90865
Warning messages on the standard output and in System.txt during upload of HPOM 8.xx configuration:

```
Warning - Platform missing (net/machine=1/17).
Warning - Platform missing (net/machine=1/41).
Warning - Platform missing (net/machine=1/40).
Object already available in database (opc_node_defaults: 1/43).
Warning - Platform missing (net/machine=1/27).
Object already available in database (opc_node_defaults: 1/44).
Warning - Platform missing (net/machine=1/6).
Object already available in database (opc_node_defaults: 1/49).
Object already available in database (opc_node_defaults: 1/0).
Warning - Platform missing (net/machine=1/38).
Object already available in database (opc_node_defaults: 1/47).
Warning - Platform missing (net/machine=1/11).
Object already available in database (opc_node_defaults: 1/45).
Object already available in database (opc_node_defaults: 5/20).
Warning - Platform missing (net/machine=1/26).
Warning - Platform missing (net/machine=1/9).
```

```
Warning - Platform missing (net/machine=1/8).
Warning - Platform missing (net/machine=1/10).
Object already available in database (opc_node_defaults: 1/50).
Warning: not all requested objects were processed.
```

Solution

The warning messages can be safely ignored. All warnings appear when DCE platforms are uploaded.

Symptom QCCR1A90937
During upgrade from HPOM 8.xx to 9.xx, opccfgupld on HPOM 9.xx aborts while processing template groups

This occurs on the HPOM 8.xx system when the configuration setting `OPC_DOWNLOAD_TEMPL_INDIVIDUAL` is set to `TRUE`. Several lines of output similar to the following are produced to `stderr` and to the `opccfgupld` logfile `/var/opt/OV/log/OpC/mgmt_sv/opccfgupld.log` on HPOM 9.xx before the program exits with 1: `"Illegal value OSSPI_SOL_NP_Filesystems_1 (function upload: templ group conversion)"`

Any data that should have been uploaded after the template groups is skipped.

Solution

1. Check to see if the HPOM 8.xx setting for `OPC_DOWNLOAD_TEMPL_INDIVIDUAL` is set to `TRUE`:

   # /opt/OV/bin/ovconfget -ovrg server opc OPC_DOWNLOAD_TEMPL_INDIVIDUAL

2. If yes, repeat the download on 8.xx with the setting changed to `FALSE`:

   # /opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_DOWNLOAD_TEMPL_INDIVIDUAL FALSE
   # rm -rf *<previous_download_dir>*
   # /opt/OV/bin/OpC/opccfgdwn *<options_from_last_call>* *<previous_download_dir>*

3. Copy the download directory to the HPOM 9.xx system and repeat the upload:

   # /opt/OV/bin/OpC/opccfgupld -replace -subentity *<further_options_from_last_call>*

After that, the HPOM 9.xx database should be consistent again.

Symptom QCCR1A109996
ovdeploy -cmd ovodetect -host <node_name> is reporting errors

The `ovdeploy -cmd ovodetect -host *<node_name>*` command returns the following error message:

```
ERROR:  (depl-228) Could not get OS type.
         (depl-400) Message returned from the target node:
        Caller is not authorized to perform the requested operation.
```

Solution

Use the following command:

 # ovdeploy -cmd ovodetect -host *<node_name>* -ovrg server

Symptom QCCR1A120261
Distributing instrumentation to unsupported platform agents is possible only from the category directory

If the agent on the unsupported agent platform is installed and uploaded to the HPOM 9.10 database, distributing category-based instrumentation from the category subdirectories is not possible. Only instrumentation placed directly in the category directory (for example, in `/var/opt/OV/share/databases/OpC/mgd_node/instrumentation/*<category>*`) is deployed to the agent instrumentation directory.

Solution

This is the expected behavior.

Symptom QCCR1A94198
InfraSPI: Errors found in messages after deployment of some packages

In the multibyte environments, incomplete messages appear in the message browser after deployment of "SI-MSWindowsPrintServiceRoleMonitor", "SI-MSWindowsFaxServerRoleMonitor", and "SI-MSWindowsWebServerRoleMonitor". Multibyte characters are removed.

Solution

Check whether the HP Operations management server processes run in the utf8 locale by running the following command:

```
# /opt/OV/bin/ovdeploy -cmd set |grep LANG
```

If it is not the utf8 locale (for example, `LANG=ja_JP.sjis`) modify the setting to the correct locale by running the following command:

```
# /opt/OV/bin/ovconfchg -ns ctrl.env -set LANG ja_JP.utf8
```

Restart the processes by running the following commands:

```
# /opt/OV/bin/ovc -kill
# /opt/OV/bin/ovc -start
```

Symptom QCCR1A118485
opcmona 08.60.501 does not match processes with parameters if the parameter in the condition is empty

If in the `Service_Process_Monitoring` policy, the `Parameters` field in the condition for the monitored process is empty, and this process was started with parameters, patches 08.60.005 and 08.60.501 or higher have different behavior:

08.60.005: The empty `Parameters` field in the condition matches all processes, regardless whether they were started with or without parameters.

08.60.501 or higher: The empty `Parameters` field in the condition matches only the processes that were started without parameters.

Solution

If you want that patch 08.60.501 or higher has the same behavior as patch 08.60.005, put `<*>` in the `Parameters` field.

Symptom QCCR1A118240
Not specifying the complete path and extension of a command leads to unintended behavior

If you do not specify the complete path and extension of the command (for example, the `Program` field contains only `SPICollector`) and if there is another program with the same name, the latter may get executed if its path or extension is specified in the predefined `%PATH%` or `%PATHEXT%` system variable. This results in the unintended behavior.

Solution

Add the complete path and extension of the command in the `Program` field. For example, in the Windows environment, specify the command as follows:

```
%OvInstrumentationDir%\SPICollector.exe
```

Symptom QCCR1A109842
-purge option (opcragt) doesn't work for local agent

It is not possible to delete instrumentation from a local node (a node installed on the same system with HPOM management server) by using the `opcragt -purge` command.

Solution

Manually delete instrumentation from the `/var/opt/OV/bin/instrumentation` directory.

Symptom QCCR1A107431
ovoareqsdr OMU Request Sender is not setting ovoadif -l ovosv=1

The `ovoareqsdr` OMU Request Sender does not set `ovoadif -l ovosv=1`. Consequently, the License report shows `0` instead of `1`. For example:

```
Operations Management Server
HP Operations Manager   1    0     OK     ovosv
```

Solution

1. On the management server, run the following command:

   `ovoadif -l ovosv=1 general_licmgr=<server_FQDN>`

   NOTE   The server and the agent must be running.

   ---

2. Check that the license requirement is set by running the following command:

   `ovolicense -r -p HPOM -detailed`

3. In the Node Information section, search for the server node and check the Used Licenses. The HP Operations Manager license must be set to `1`.

Symptom QCCR1A90622
Invalid network type for nodes of type PATTERN_OTHER.

After a node with the network type `PATTERN_OTHER` is added, its network type is set to `PATTERN_IP_NAME`.

Solution

This is expected behavior, as `PATTERN_OTHER` is internally mapped to `PATTERN_IP_NAME`. Keyword `PATTERN_OTHER` is deprecated. Use `PATTERN_IP_NAME` instead.

Symptom QCCR1A96746
Certificate request grant and add node functionality failing for AIX LPAR nodes

The add and grant functionality is failing for AIX LPAR nodes on AIX 5.3 and 6.1.

Solution

1. Manually add the node using the `opcnode` command. For example:

   `opcnode -add_node node_name=<nodename> net_type=NETWORK_IP group_name=linux \`
   `mach_type=MACH_BBC_AIX_PPC`

2. Manually grant the certificate request using the following command:

   `# opccsa -grant <certificate request ID>`

You can obtain CertID using the following command:

`# opccsa -list_pending_cr`

Symptom QCCR1A95886
Error message in System.txt during deinstallation of remote agent

During remote agent deinstallation or re-installation, the following errors appear in the System.txt file on the management server:

```
0: ERR: Wed Aug 26 13:18:48 2009: ovdeploy (8173/1): (depl-86) Unable to execute command
'opc_inst' on node '<node>'.
1: ERR: Wed Aug 26 13:18:48 2009: ovdeploy (8173/1): (depl-176) Message returned from host
'<node>':
2: WRN: Wed Aug 26 13:18:48 2009: ovdeploy (8173/1): (bbc-422)
HttpOutputRequestImpl::ReceiveResponse() caught OvXplNet::ConnectionRefusedException_t.
<null>
3: WRN: Wed Aug 26 13:18:48 2009: ovdeploy (8173/1): (bbc-71) There is no server process
active for address: https://<node>/com.hp.ov.depl/bbcrpcserver.
0: ERR: Wed Aug 26 13:20:21 2009: ovoareqsdr (9482/1): [rqshbp.cpp:1669]: OV Communication
Broker (ovbbccb) on nod <node> is down. (OpC40-1913)
```

Solution

These errors and warnings can be safely ignored.

Symptom QCCR1A90462
opcconn_cs_reset() sometimes does not reset status message

It is possible that after calling opcconn_cs_reset() API function the status message is not reset.

Solution

To ensure that you always get the correct message, call opcconn_cs_set() with an empty string (not NULL!) as the 'message' parameter after calling opcconn_cs_reset().

Symptom QCCR1A110001
"/ovconfget not found" error or failover occurs during online restore

When running an online restore script, an error "/ovconfget not found" may appear.

Additionally, in cluster environments, the monitoring of the Oracle cluster group remains active during the database restore. This provokes a failover.

Solution

Before calling the online restore script, stop monitoring of the Oracle resource group as follows:

```
# /opt/OV/lbin/ovharg -monitor ov-oracle disable
```

You can reenable it after the successful completion of the restore procedure as follows:

```
# /opt/OV/lbin/ovharg -monitor ov-oracle enable
```

Symptom QCCR1A90808
System.txt: There is no server process active for address:
'https://localhost/com.hp.ov.agtrep.notificationreceiver/bbcrpcserver'

This error message may be printed in System.txt every time the ovconfchg operation is executed.

Solution

If no policy of type svcdisc was deployed to an agent, the error message can be ignored.

Symptom QCCR1A96506
MoM changes not detected

Sometimes the Message Manager does not detect changes to the `msgforw` file even after the `ovconfchg` utility was invoked. If the Message Manager does not automatically reread the configuration file, manually restart the Message Manager process.

Solution

Restart the Message Manager process with the following command:

`# ovc -restart opcmsgm`

Symptom QCCR1A111815 SQL select stmt takes long, causes opcmsgm delay

It takes too long for the Message Manager to process messages, if the SNMP ECS Traps template is enabled and there are many messages in the active or history browser.

Solution

You can speed up the message lookup by `original_msgid` by creating the following secondary indexes in the database:

```
echo "create index opcx_act_original_msgid on opc_act_messages (original_msgid) \
tablespace OPC_INDEX1;" | /opt/OV/bin/OpC/opcdbpwd -e sqlplus
```

```
echo "create index opcx_hist_original_msgid on opc_hist_messages (original_msgid) \
tablespace OPC_INDEX2;" | /opt/OV/bin/OpC/opcdbpwd -e sqlplus
```

Symptom QCCR1A105603
HPOM integrated with NNMi through northbound, error related to "target connector" licenses missed

License report might show an incorrect number of Target Connector licenses required.

Solution

Consider that you do not need a Target Connector license for nodes, that produce messages originated from HP products. Therefore, to get the number of needed Target connector licenses, you should manually check how many of the reported nodes have HP products installed and then deduct the total number by the number of HP product nodes.

Symptom QCCR1A95948
NNMi group is not visible by default for user opc_adm

Responsibilities for the message group NNMi are not configured by default for user `opc_adm`.

Solution

Add user responsibilities manually by running the following command:

```
/opt/OV/bin/OpC/opccfguser -v -assign_respons_user -user opc_adm -node_group \
-list <node_group> -msg_group -list NNMi
```

Symptom QCCR1A91821
HP Performance Manager tools executed on another HP Performance Manager server require clean-up before installing HP Performance Manager integration

After installing new version of HP Performance Manager or upgrading it, the old HP Performance Manager server name is still used for HP Performance Manager. The problem is that the HP Performance Manager installation script fails to change the HP Performance Manager server name in the database:

`/opt/OV/contrib/OpC/OVPM/install_OVPM.sh <new OVPM server>:8081`

Solution

Before installing a new HP Performance Manager server on the HPOM management server, remove all the HP Performance Manager policies and tools. For example:

```
/opt/OV/bin/OpC/opcappl -del_app app_name="OVPM Global History"
/opt/OV/bin/OpC/opcappl -del_app app_name="OVPM HTML contrib"
/opt/OV/bin/ovconfchg -ovrg server -ns opc -clear OPC_OVPM_GRAPH
```

Symptom QCCR1A94498
How to configure HP Performance Manager if you did not do it during installation

Solution

If you did not install HP Performance Manager during the HPOM installation and you want to install it later, run the following command:

```
# /opt/OV/contrib/OpC/OVPM/install_OVPM.sh <nodename>:<port>
```

For example:

```
# install_OVPM.sh elisa.deu.hp.com:8081
```

Symptom QCCR1A97123
When PM is installed together with HPOM server "ovpm stop" should not stop ovtomcatB process

When you install HP Performance Manager 8.21 on the system where HPOM server is installed and stop the ovpm process using the /opt/OV/bin/ovpm stop command, also the ovtomcatB process is stopped. When ovtomcatB is not running, the web access to the HPOM management server is not possible and you cannot browse HPOM html manpages, manuals, Java GUI launcher, etc.

Solution
Run the following command:

```
/opt/OV/bin/ovc -start ovtomcatB
```

Symptom QCCR1A96745
ovoremove fails to remove HPOvXpl because of dependencies to agent localization packages

ovoremove fails when removing HPOvXpl with the following error:

```
HPOvSecCo (6.20.050) . . . . Removed
HPOvXpl   (6.20.054) . . . . . FAILED
ERROR: Error occurred while removing HPOvXpl package
Please check /var/opt/OV/log/OpC/mgmt_sv/installation.log.error for details.
```

Solution

Ignore this error by selecting skip. After ovoremove finishes, remove the packages manually if they are not needed by other products. Use the following command:

```
# rpm -e HPOvXpl HPOvLczC HPOvLces HPOvLcko HPOvLcja
```

Symptom QCCR1A90795
SiteScope tools are not shown in Java GUI for any operator

The SiteScope integration uploads series of tools to the HPOM database, but these tools are not assigned by default to any operator, so these tools are not shown in the Java GUI.

Solution

Manually assign the SiteScope tools to the operators using the opccfguser command or Administration GUI. For more information, see the *opccfguser(1m)* manual page.

Symptom QCCR1A96583
The maximum length for a node name may vary.

While the database accepts a maximum of 2048 characters for a given fully qualified domain name (FQDN), consider that there may be limitations on the DNS server, the operating system level, or other programs that may cause HPOM not to function properly with these nodes.

Solution

FQDNs should not exceed 256 characters. If they do, it may be helpful to add an `IP/nodename` entry in the `/etc/hosts` file.

Symptom QCCR1A90167/QCCR1A92949
Non IP Node gets resolved if name is in DNS

When you try to add a non-IP node that is registered in the DNS, its network type is changed from OTHER to IP and you get a warning. The result is that the non-IP node has an IP network type.

For example:

```
# /opt/OV/bin/OpC/utils/opcnode -add_node node_name=ovruxt62.rose.hp.com \
net_type=NETWORK_OTHER mach_type=MACH_BBC_OTHER_NON_IP group_name=hp_ux layout_group=/
```

```
Warning: Mismatch between node name and IP address (according to the DNS)
Please check to which IP address the hostname is resolved
and if that IP is resolved back to the original hostname.
```

```
Operation successfully completed.
```

Checking with `opcnode -list_nodes` shows that it was added as an IP node with the `MACH_BBC_OTHER_NON_IP` platform:

```
# /opt/OV/bin/OpC/utils/opcnode -list_nodes node_list=ovruxt62.rose.hp.com
```

```
List of all Nodes in the HPOM database:
================================
Name          = ovruxt62.rose.hp.com
Label         =
IP-Address    = 15.8.156.145
Network Type = NETWORK_IP
Machine Type = MACH_BBC_OTHER_NON_IP
Comm Type     = COMM_BBC
DHCP enabled = no (0x22)

================================
```

Solution

It is not possible to add an IP node (a node that is resolvable and has an IP address) as non-IP node. Change the invalid platform from `non_ip/other/other` using `opcnode -chg_machtype`.

For example:

```
# /opt/OV/bin/OpC/utils/opcnode -chg_machtype node_name=ovruxt62.rose.hp.com \
net_type=NETWORK_IP mach_type=MACH_BBC_OTHER_IP
```

Symptom QCCR1A97290
If Oracle service ($ORACLE_HOME/network/admin/listener.ora) is disabled, the Administration UI cannot connect to the HPOM server

If you disable the Oracle service by modifying `$ORACLE_HOME/network/admin/listener.ora` using the OvProtect utility, Administration UI will not be able to connect to your management server.

Solution

Do not disable the Oracle service using the OvProtect utility.

Symptom QCCR1A92537
Cannot open pipe oprtjnitp

After installation of HPOM, the following error is seen in `System.txt`:

```
0: ERR: Fri May 15 19:03:23 2009: opcdispm (15894/1078278464): [mpisv.c:816]: Cannot open
pipe
/var/opt/OV/share/tmp/OpC/mgmt_sv/oprtjnitp. open(2) failed. No such device or address
(OpC40-616)
```

Solution

You can safely ignore this error.

Symptom QCCR1A97644
Adding a service with empty name must drop a warning

When adding a service without a name (`<MsgSvcName></MsgSvcName>`) by using the `opcsercvice - add <file>` command, no error message displays. However, after such service is added, you can get the following error message, for example, when searching in history for some other services under this service:

```
Database: ORA-01400: cannot insert NULL into
"OPC_OP"."OPC_SERVICE_MSGS"."MSG_SERVICE_NAME"
```

This error occurs, because `MsgSvcName` cannot be empty in the Oracle database.

Solution

In the XML file, delete the `<MsgSvcName></MsgSvcName>` line.

Symptom QCCR1A103457
Service Depth is not displayed correctly

When you run a verbose listing of a service added to a server, the depth value for the service has no value.

Solution

Ignore this. This does not affect the management server and Java GUI functionality.

Symptom QCCR1A139299
Windows event log variables not being captured on Windows 2008 servers

Variables for Log-File-Encapsulator policies do not work with eventlog policies deployed to Windows 2008 nodes running HPOM agent.

Solution

These variables cannot be used with W2K8 and above.

Symptom QCCR1A143706
Adding External Node with net_type=PATTERN_OTHER Name resolution

When adding an external node with the network type `PATTERN_OTHER`, the network type is mapped to `PATTERN_IP_NAME`.

When a message for an external node with `net_type=PATTERN_IP_NAME` arrives, `opcmsgm` tries to resolve the node name.

Solution

To skip the name resolution attempts the workaround is to use the regular non-IP nodes. In case an external node pattern matches a single node, a regular node of type non-IP/other/other can be added instead of adding an external node.

Symptom QCCR145210
opcbackup_online and opcrestore_online are not cluster aware

The opcbackup_online and opcrestore_online commands do not contain the necessary logic for backing up and restoring HPOM in a cluster setup.

Solution

Backup only one node, and restore to the same node.

Symptom QCCR157490
Server documentation enhancement for ovbbccb open connections

On HPOM 9 management servers with high number of RCP nodes, the ovbbccb process opens many connections and eventually runs out of available file descriptors. As a result, the agents start buffering.

Solution

Increase the maximum number of allowed file descriptors by using the limits.conf, as follows:

```
tail /etc/security/limits.conf
```

```
* soft nofile 4096
```

```
* hard nofile 4096
```

This sets the maximum available descriptors for all users as 4096.

Java GUI

Symptom QCCR1A150887
Problem with the Java GUI main window when launching the Java GUI on Mac OS X by using WebStart

When launching the Java GUI on Mac OS X by using WebStart, the title bar of the main window is not visible. After moving the Java GUI window under the Mac OS X title bar, you cannot move it anymore, but only resize it. If you save console settings, the Java GUI window is displayed under the Mac OS X title bar next time you launch the Java GUI and you have the same problem with moving the Java GUI window.

Solution

Restore the defaults originally provided by your HPOM administrator by selecting File->Reload Assigned Defaults from the menu bar. In this case, you lose all the changes you made to the Java GUI and saved with the File->Save Console Session Settings option, but you prevent the Java GUI window being displayed under the Mac OS X title bar.

Symptom QCCR1A147514
Errors appear when opening the Java GUI on Mac OS X

When opening the Java GUI on the Mac OS X system, the following error messages appear:

```
<Error>: CGContextGetCTM: invalid context 0x0
<Error>: CGContextSetBaseCTM: invalid context 0x0
<Error>: CGContextGetCTM: invalid context 0x0
<Error>: CGContextSetBaseCTM: invalid context 0x0
```

Solution

You can safely ignore these error messages.

Symptom QCCR1A108463
Java GUI error "Tool halted due to reconnection" appears if a short hostname is used

When you start a customized tool and add an additional node as a short hostname, the `Tool halted due to reconnection` error occurs.

Solution

Use a long hostname instead.

Symptom QCCR1A97287 opcuihttps multiple coredumps

Process `opcuihttps` sometimes core dumps when stopped. Consequently, Java GUI cannot connect through the secure communication layer (HTTPS).

Solution

Start the `opcuihttps` process manually.

Symptom QCCR1A57461
Wrong cursor shape after resizing Windows/Dialogs

When using the HP One Voice or Metal look and feel, the cursor stays in resizing shape when it is inside the window or dialog, after quickly resizing windows or dialogs and releasing the mouse button. This can be visible:

• In windows: when the cursor is on the title bar or on menu bar.

• In dialogs: in the whole dialog.

Solution

Use a different look and feel.

Symptom QCCR1A56713
No notification about error with https_only enabled

When variable `https_only` is set to `yes` in `ito_op.bat` and secure connection cannot be established, the user is not notified, but the login dialog appears again.

Solution

Check the console for an error message.

Symptom QCCR1A110581
Instruction text interface not working through Instructions tab in the Msg. properties window

If you use the Instructions tab in the Message Properties window to get the instruction text, the instructions call does not start.

Solution

To get the instruction text of a message from the Instructions tab in the Message Properties window, click the **Annotations** tab, and then click the **Instructions** tab again.

NOTE   You can get instructions text also by right-clicking a message in the Message Browser and selecting Instructions from the pop-up menu.

Symptom QCCR1A58168
Java GUI should start if TNS_ADMIN is in use without any customization

If you choose to use a different folder for storing the `tnsnames.ora` file, you may have problems when trying to run Java GUI.

Solution

Edit the `/opt/OV/bin/OpC/opcuiwww.sh` file to export the `TNS_ADMIN` variable at the beginning:

```
# export TNS_ADMIN=<alternate location>
```

Symptom QCCR1A97264
Browser layout is lost when column filter is loaded more than once from the same dialog

When opening a column filter dialog, the custom saved filter loads only the first time. When you try to load it more times, with the column filter dialog being opened, the browser layout is lost and default column labels are used.

Solution

Switch between the text tab and the simple/advanced tab for two times and the custom labels will display. again.

Symptom QCCR1A104940
Submap or Custom map changes its table view into map view after reload configuration.

Submap or custom map on a service graph has a table view. After reconnecting the Java GUI service graph, view changes to the map view.

Solution

In the Java GUI, click **Edit->Preferences->Services tab**. Ensure that the `Use Service Load on Demand` option is enabled. Log off Java GUI and then log on again.

Symptom QCCR1A109287
Title of the Java GUI Web browser is unreadable.

On the pages that use non-English characters the title of the internal JGUI Web browser is unreadable.

Solution

Set an external Web browser as the default Web browser for the Java GUI.

In the Java GUI, click **Edit->Preferences**, select the Web Browser tab in the Preferences window, and use the **Browse** button to choose an external Web browser.

Symptom QCCR1A110095
Cannot open links with left click in JGUI OLH through Active X

If you opened Java GUI through ActiveX, the Java GUI online help links do not open when you left-click on them. This problem does not occur when Java GUI is opened in an external web browser.

Solution QCCR1A156831
"Full Authentication" may not work with the Webstart Java GUI

Java GUI may not work if started like Webstart in case Full Authentication is used.

Solution

This is the expected behavior.

Symptom QCCR1A150970
Java GUI freezes while trying to close any open window

If shortcut bar contains too many items, Java GUI freezes while trying to close open windows.

Solution

Use the `show_shortcut_pane` start-up option for setting the visibility of the Shortcut Bar. When this option is set to `TRUE` or `ON` (the default value), the Shortcut bar is visible in the current Java GUI session. You can set the `show_shortcut_pane` option in the local `itooprc` file. This option cannot be read from the global `itooprc` file.

Administration UI

Symptom QCCR1A145496
Scheduled policies and actions do not run if the values are not specified correctly

If the details of the schedule are not specified correctly, scheduled policies and actions do not run.

Solution

Specify the details of the schedule at which the task should run using the fields displayed. Keep in mind that wild cards such as the asterisk (*) are not allowed (to specify *all* values, leave the field blank). However, you can use the comma (,) and the hyphen (-) to specify ranges.

For example:

- *Minute:* a number from 0 through 59

  Enter `15` to start the task at 15 minutes past every hour, `0,30` to start the task every 30 minutes, or `10-20` to start the task every minute from 10 to 20 minutes past the hour.

- *Hour:* a number from 0 (midnight) through 23 (using the 24-hour clock)

  Enter `12` to start the task at midday, `06,18` to start the task at 6 A.M. and at 6 P.M., or `14-18` to start the task once an hour every hour from 2 P.M. through 6 P.M.

- *Day of the Month*: a number from 1 through 31

  Enter `15` for the first day of every month, `5,15` for the 5th and 15th day of every month, and `1-31` for every day of the month. Note that `31` is always interpreted as the last day of the month, even if the month has 28, 29, or 30 days. If you define the day twice, once here and once in "Day of the Week," the scheduled action is started twice.

- *Month:* a number from 1 (January) through 12 (December)

  Enter `4,5` for April and May, and `6-8` for June, July, and August.

- *Year:* the year in which the scheduled task should run

  Enter `2009` for year 2009. Note that the number must include four digits. If you want to signify year 2009, you must enter `2009` and not only `09`.

- *Day of the Week:* a number from 0 (Sunday) through 6 (Saturday).

  Enter `1,2,3` for Monday, Tuesday, and Wednesday, or `4-6` for every day between (and including) Thursday and Saturday. If you define the day twice, once here and once in "Day of the Month," the scheduled action is started twice.

Symptom QCCR1A154855
Editing a node fails if the HBP interval is specified as 00h10m00s

The Administration UI fails to save the node after editing it if the HBP interval has two zeros in the hours field.

Solution

To solve this problem, replace `00` with `0`.

Symptom QCCR1A134422
The operator Responsibility Matrix is not properly displayed in IE 8

When accessing the operator Responsibility Matrix in Internet Explorer 8 only the first nine out of 19 rows are visible. Because the vertical scroll bar is also not displayed, users cannot see the rest of the rows.

Solution

To solve this problem, enable the IE8 Tools-> Compatibility View settings.

QCCR1A159356
AdminUI "Find-Locate" functionality in AdminUI in IE9 aborts

When performing "Find" operation in the AdminUI opened in Internet Explorer 9 on Windows 7, the error messages similar to the following appear:

```
No pipeline matched request: -BES-index-RAW-/en/ at <map:mount> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:520:101 at <map:serialize type="xml"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:375:42 at <map:transform> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:330:90 at <map:transform type="xinclude"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:637:41 at <map:transform type="divIdgen"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:636:41 at <map:generate> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:634:88 at <map:serialize type="html"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:372:43 at <map:transform type="encodeURL"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:360:64 at <map:transform type="i18n"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:357:38 at <map:transform> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:330:90 at <map:transform
type="midasWidgetsTransformer"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:994:84 at <map:transform
type="urlParameterTransformer"> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/global.xmap:990:83 at <map:mount> -

file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/sitemap.xmap:363:74
```

Solution

To solve this problem, enable the IE8 Tools-> Compatibility View settings.

Symptom QCCR1A157968
Add option to modify assigned policy version for policy groups recursively

When a checkbox that denotes a subgroup inside a policy group is selected in the Administration GUI, and then the option "Modify assigned Version…" from the drop-down list is used to select, for example, "LATEST" as the new chosen policy version, an exception error is thrown.

It should be possible to change the policy version of all policies inside the selected policy group, as well as the policies from included subgroups.

Solution

Change the policies recursively by using the command line. The output should look similar to the following:

```
# opcpolicy -list_group pol_group=TestPolicySubGroup1
Retrieving information for 'POLICY_GROUP_DETAILS' from the HPOM database failed.

# opcpolicy -list_groups | grep Test
```

```
policy group: /TestPolicyGroup
policy group: /TestPolicyGroup/TestPolicySubGroup1# opcpolicy -list_group
pol_group=/TestPolicyGroup/TestPolicySubGroup1
--------------------------
policy group: /TestPolicyGroup/TestPolicySubGroup1
assigned policy    : Test_dynamic_logfile, version 0001.0001, type name Logfile_Entry, FIX
assigned policy    : Test_forwardcheck, version 0001.0001, type name Measurement_Threshold, FIX
==================================================================

# opcpolicy -chg_assign_mode group=/TestPolicyGroup/TestPolicySubGroup1 mode=LATEST mass_upd=yes
assigned policy: Test_dynamic_logfile, version 0001.0001, FIX
to policy group: /TestPolicyGroup/TestPolicySubGroup1
assignment mode changed to LATEST
----------------------
assigned policy: Test_forwardcheck, version 0001.0001, FIX
to policy group: /TestPolicyGroup/TestPolicySubGroup1
assignment mode changed to LATEST
----------------------
2 assignments to update; all ok
==================================================================

# opcpolicy -list_group pol_group=/TestPolicyGroup/TestPolicySubGroup1
--------------------------
policy group: /TestPolicyGroup/TestPolicySubGroup1
assigned policy    : Test_dynamic_logfile, version 0001.0006, type name Logfile_Entry, LATEST
assigned policy    : Test_forwardcheck, version 0001.0002, type name Measurement_Threshold, LATEST
==================================================================
```

Symptom QCCR1A42068
Repeated logon required upon switching from the Java GUI to the Administration GUI

When switching from the Java GUI console to the Administration UI, an operator has to log on again.

Solution

Log on once more.

Symptom QCCR1A42072
Profiles assigned to an HPOM user are not displayed upon editing

When editing an HPOM user, you cannot see the assigned profiles.

Solution

Check for the assigned profiles from the Browse menu.

Symptom QCCR1A42227
Terminal type can be selected during the Windows node setup

The Virtual Terminal option is enabled on the Advanced tab when adding a Windows node. This option should be disabled for Windows nodes.

Solution

You can safely ignore this option because its value is ignored when adding a Windows node.

Symptom QCCR1A60970
Service Discovery policy is displayed in one line in the .xml file (including the raw edit)

The entire .xml output from the service discovery is displayed in one line. This applies also to the raw edit.

Solution

Editing the service discovery policy manually is not recommended and is not supported in the Administration UI.

Symptom QCCR1A61096
Certficate granting does not work even by using the Map force option

After reinstalling an HP Operations agent on Windows, a new certificate granting request is pending on the server. Granting the request is not possible even by using the Map force option in the Administration UI.

Solution

Delete the `core_id` manually from the command line as follows:

```
opcnode node_name=<node name> -del_id
```

Symptom QCCR1A100576
Some title descriptions are hardcoded

Overviews like "Orphaned Nodes" or "Unassigned Nodes" have no complete translation.

Solution

None.

Symptom QCCR1A107610
Cannot change node type for node

When changing the node type from one value to another (for example, from `MACH_BBC_LX26RPM_X86` to `MACH_BBC_HPUX_PA_RISC`) it is required to fill in these fields in the Administration UI: Label and IP address.

Because the IP address value is already specified and you are prompted to enter a host name first, it is not possible to perform a chosen selection, and therefore to edit the node.

Solution

For better IP address resolution use the "Resolve hostname" button (available with the Administration UI version 9.1.0). However, note that adding a node without the node type is not possible within the Administration UI.

Symptom QCCR1A101499
Administration UI Measurement_Threshold policy editor does not accept the comma (",") mark as a threshold.

On a Spanish platform, it is not possible to set the number with the comma (",") mark in the Administration UI policy editor because it cannot be saved.

Solution

Use full stop (".") as a separator for entering the thresholds.

Symptom QCCR1A100570
Layout problems: The hint layout of some Administration UI items is improper

Some box hints are displayed with the wrong layout. The text is not aligned to the left, as it should be.

Solution

None.

Localization

Symptom QCCR1A90000
[L10N]: JAVA_GUI: The "Certificate Management" in global filter is not translated.

This filter is uploaded along the default HPOM configuration, which is common for English, Korean, Spanish and Chinese. Name remains untranslated in default Japanese configuration files.

Solution

You can safely ignore this problem.

Symptom QCCR1A90004
[L10N]: JAVA_GUI: When login as the invalid password, the string is not translated

When you log on to Java GUI with the invalid password, an error message is displayed, but it is not translated.

Solution

To ensure that the error message displays translated, edit `/opt/OV/bin/OpC/opcuiwww.sh` by changing the locales in the call to `opcuiwww`. For example:

```
OPCUIWWW_LANG=${LANG} LANG=es_ES.UTF-8  LC_ALL=es_ES.UTF-8 \
/opt/OV/bin/OpC/opcuiwww $* >> ${LOGFILE} 2>&1
OPCUIWWW_LANG=${LANG} LANG=ja_JP.UTF-8  LC_ALL=ja_JP.UTF-8 ...
```

HP Reporter 3.80

HPOM supports HP Reporter 3.80. Consider that the same HP Reporter version is used on all HPOM supported platforms (HP-UX, Solaris, and Linux). However, reports and documentation provided with this HP Reporter version do not mention HPOM on Linux. You can safely use all the advantages of HP Reporter 3.80 on Linux, even though HPOM on Linux is not specifically mentioned.

Server Pooling

Symptom QCCR1A150555
MigrateAsymKey.sh -createNodecert does not recreate the server pooling certificate in the OVRG virt

Although the HP Operations agent documentation states that `MigrateAsymKey.sh -createNodecert` recreates the certificates of all OV resource groups, it does not recreate the server pooling certificate in the OVRG `virt`.

Solution

After creating new node certificates using `MigrateAsymKey.sh -createNodecert`, manually recreate the node certificate in the OVRG `virt`.

For example, assuming that the virtual node name is `virt.rose.hp.com`, follow these steps:

1. Remove and recreate the certificate for the OVRG `virt`:

   `/opt/OV/bin/ovcoreid -ovrg virt > /tmp/virt.coreid`

   `/opt/OV/bin/ovcert -remove `cat /tmp/virt.coreid` -ovrg virt`

   `/opt/OV/bin/ovcm -issue -file /tmp/virt.cert -name virt.rose.hp.com \`
   `-pass virt -coreid `cat /tmp/virt.coreid``

   `/opt/OV/bin/ovcert -importcert -ovrg virt -file /tmp/virt.cert -pass virt`

2. Verify that the new certificate has the correct key length:

   `/opt/OV/bin/ovcert -certinfo `ovcoreid -ovrg virt` -ovrg virt`

3. After migrating the certificates to the other server pooling node using `MigrateAsymKey.sh`, exchange the trusted certificates between the server pooling nodes again.

4. Copy `/tmp/virt.cert` and `/tmp/virt.coreid` to the other server pooling node.

5. Remove the OVRG `virt` certificate on the other server pooling node:

   /opt/OV/bin/ovcert -remove `cat /tmp/virt.coreid` -ovrg virt

6. Import the new OVRG `virt` certificate on the other server pooling node:

   /opt/OV/bin/ovcert -importcert -ovrg virt -file /tmp/virt.cert -pass virt

7. Verify that the new certificate has the correct key length:

   /opt/OV/bin/ovcert -certinfo `ovcoreid -ovrg virt` -ovrg virt

Documentation Updates

The following user documentation has been introduced or updated since the last released patches for the HP Operations management server and the Java GUI (that is, version 9.10.230):

- *Authenticating Administration UI Users Using PAM or LDAP White Paper*
- *HPOM Server Configuration Variables*
- *Custom Process Management White Paper*

Documentation Errata

The following item is listed incorrectly in the documentation.

LOCATION	*HPOM Concepts Guide*
ERROR	The information about managing disabled nodes is wrong.
CORRECTION	When managing disabled nodes, the processes are not stopped (only messages for such nodes are discarded).
LOCATION	*HP Operations Manager Installation Guide for Sun Solaris*
ERROR	The guide contains wrong information.
CORRECTION	The following information is obsolete and should not be included in the guide:
	A short hostname may not be longer than 8 characters. Whenever a host is added to `/etc/hosts`, make sure that its name is fully qualified.

Local Language Support

HPOM 9.10 is localized to Japanese, Korean, Simplified Chinese, and Spanish. HPOM can be used in multilingual environments.

Certified Encoding and Character Sets on HPOM Management Servers

Certified encoding and character sets need to be set for the HPOM management server and Oracle database host systems.

- Encoding HPOM Node Character Set: `UTF-8`

- Oracle Database Code Set: `AL32UTF8`

- Linux Language Variable `LANG`:

    — English: `en_US.UTF-8`, `en_GB.UTF-8`

    — Spanish: `es_ES.UTF-8`

    — Japanese: `ja_JP.UTF-8`

    — Korean: `ko_KR.UTF-8`

    — Simplified Chinese: `zh_CN.UTF-8`

Other locales are also supported, for example, German and French. For information about supported character sets, refer to the *HPOM Administrator's Reference*.

IMPORTANT   UTF-8 is the only encoding supported by the HPOM database.

Localized Support

HPOM 9.10 provides the localized support for the following languages:

- 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 6   **Localized Software**

Locale		English	Japanese	Korean	Simplified Chinese	Spanish
Administration UI		✔	✔			
Java UI		✔	✔	✔	✔	✔
Manual Pages		✔				
Installation		✔	✔	✔	✔	✔
HTTPS Agent Message Catalogs	Event Action	✔	✔	✔	✔	✔
	Embedded Performance Agent	✔				
Encoding/Database Character Set		UTF-8 AL32UTF8	UTF-8 AL32UTF8	UTF-8 AL32UTF8	UTF-8 AL32UTF8	UTF-8 AL32UTF8

Table 7   **Localized Documentation**

Locale	English	Japanese	Korean	Simplified Chinese	Spanish
HPOM Administrator's Reference	✔	✔			
HPOM Concepts Guide	✔	✔			
HPOM Installation Guide	✔	✔			
HPOM Java GUI Operator's Guide	✔	✔			
HPOM Software Release Notes	✔	✔			
HPOM Administration UI User Guide	✔	✔			
HPOM Administration UI Administration and Configuration Guide	✔	✔			
HPOM Administration UI Installation Guide	✔	✔			
Java GUI online help	✔	✔			
Administration UI online help	✔	✔			

NOTE	Check the following web site for the latest versions of the localized manuals:
	http://support.openview.hp.com/selfsolve/manuals

HP Software Support

You can visit the HP Software support web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

• Search for knowledge documents of interest

• Submit and track support cases and enhancement requests

• Download software patches

• Manage support contracts

• Look up HP support contacts

• Review information about available services

• Enter into discussions with other software customers

• Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract. To find more information about support access levels, go to the following URL:

http://support.openview.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to the following URL:

http://h20229.www2.hp.com/passport-registration.html

Legal Notices

Warranty.

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

Restricted Rights Legend.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices.

©Copyright 2005–2013 Hewlett-Packard Development Company, L.P.

Trademark Notices.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

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

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

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

UNIX® is a registered trademark of The Open Group.

Acknowledgements

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/.html).

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

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

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

This product includes software developed by The TM4J Project (http://sourceforge.net/projects/tm4j).

This product includes software developed by VM Systems, Inc. (http://www.vmsystemsinc.com/).

This product includes software developed by the MX4J project (http://mx4j.sourceforge.net).

This product includes DOM4J, Copyright 2001–2005 © MetaStuff, Ltd. All Rights Reserved.

This product includes ICU4C Copyright © 1995–2006 International Business Machines Corporation and others.

This product includes ICU4J Copyright © 1995–2006 International Business Machines Corporation and others.