HP Operations Manager

for the management server on the Sun SPARC Solaris system

Release Notes

Software Version: 9.11.130
Release Notes Publication Date: March 5, 2015

Edition 4

This document provides an overview of HP Operations Manager (HPOM) version 9.11.130. 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 of this document, go to: https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

This document provides information about the following topics:

- Changes with Latest Patches
- Installation
- Features, Enhancements, and Changes Introduced with HPOM 9.11.xxx
- Features, Enhancements, and Changes Introduced with 9.xx Releases
- HPOM 9.xx and Other HP Software Solutions
- Obsolescence Announcements
- Known Problems, Limitations, and Workarounds
- Local Language Support
- Documentation Updates
- Documentation Errata
- HP Software Support
- Legal Notices

Changes with Latest Patches

This section describes changes that are available with the latest HPOM patches. The following 09.11.130 patches are available:

- "HP Operations Management Server Patch" on page 2
- "Java GUI Patch" on page 3
- "Administration UI Patch" on page 3
- "HPOM Server Accessories Patch" on page 3
- "HPOM Core Server Patch" on page 4

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 09.11.130

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	Linux	Solaris
HPOM consolidated server 09.11.130	`OMHPUX_00008`	`OML_00084`	`ITOSOL_00806`

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 HP Operations management server now includes a new contrib tool, `opcsvqchk`, for dumping messages in the server queue files.

  The `opcqchk` contrib tool, which is available with the HP Operations agent, was used for server message queue files up to the HP Operations agent version 11.00, when the message format and the tag for messages changed. This resulted in losing the possibility to use `opcqchk` for HP Operations management server message queue files (content was displayed as hex dump).

- A new server configuration variable `OPCUIWWW_NO_LDAP` is now available. If set to `TRUE`, `opcuiwww.sh` uses the regular `opcuiwww` utility instead of `opcuiwww.ldap`.
- HPOM now uses the current time as the annotation time in message operations.

  A new server configuration variable `OPC_USE_ACTION_TIME_FORW_ANNO` is now available. If set to `TRUE`, you can use the old behavior to use the time as reported by the agent.

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

New Support Announcement

HPOM 9.11.130 now supports Oracle database version 12c. For the installation procedure, see "Installing HPOM with Oracle Database 12c" on page 5.

Java GUI Patch

The following Java GUI patch is available:

Table 2 Java GUI Patch 09.11.130

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	Linux	Solaris
Java GUI 09.11.130	OMHPUX_00009	OML_00085	ITOSOL_00807

You can now specify a timeout after which opcuiwww disconnects the Java GUI and exits (in case there are no other users with the same name). This prevents stale sessions from happening, when the Java GUI is disconnected because of a VPN disconnection. You can configure the timeout by using a new server configuration variable OPCUIWWW_DISCONNECT_TIMEOUT.

For example, to set the timeout to two minutes, run the following command:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPCUIWWW_DISCONNECT_TIMEOUT 120
```

Administration UI Patch

The following Administration UI patch is available:

Table 3 HPOM Administration UI Patch 09.11.130

Patch Name	
HPOM Administration UI 09.11.130	OMUADMINUI_00013

HPOM Server Accessories Patch

The following server accessories patch is available:

Table 4 HPOM Server Accessories 09.11.130

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	Linux	Solaris
HPOM Server Accessories 9.11.130	OMHPUX_00016	OML_00092	ITOSOL_00814

This patch contains the following shared component packages:

- HPOvJREB (HP Software JRE) 01.07.025
- HPOvTomcatB (HP OpenView TomcatB Servlet Container) 07.00.056
- HPOmWs (HP Operations Manager Web Service) 09.10.062

- HPOprWsInc (HP Operations Manager Incident Web Service) 09.10.062

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 written in the Special Installation Instructions section of the patch description.

HPOM Core Server Patch

The following core server patch is available:

Table 5 HPOM Core Server 09.11.130

Patch Name	Management Server Platform		
	HP-UX on HP Integrity	Linux	Solaris
HPOM Core Server 09.11.130	OMHPUX_00014	OML_00090	ITOSOL_00812

This patch contains the following packages:

- HPOvOprEl (HP Operations Embedded Licensing) 02.12.103
- HPOvSecCS (HP Software Certificate Management Server) 11.05.015 and 11.14.014
- HPOvJxpl (HP Software Cross Platform Component Java) 11.05.015 and 11.14.014
- HPOvJsec (HP Software Security Core Java) 11.05.046 and 11.14.014
- HPOvJbbc (HP Software HTTP Communication Java) 11.05.047 and 11.14.049

IMPORTANT Before installing HPOM Core Server patch, make sure you get familiar with the section "HPOM Core Server Patch Installation Notes" on page 7.

Installation

This section contains the information about installing and deinstalling HPOM 9.11.xxx, as well as the installation notes that apply for all the HPOM 9.xx releases.

Installing HPOM with Oracle Database 12c

To install the Oracle database version 12c for use with HPOM 9.11.130, follow these steps:

1. Get familiar with the installation requirements described in the *HPOM Installation Guide for the Management Server,* and also with the Oracle 12c requirements provided with the Oracle documentation.
2. Install Oracle 12c following the instructions for installing Oracle 11g Database Release 2 Enterprise Edition (64-bit) (you can find them in the “Installing and Verifying an Oracle Database” section of the *HPOM Installation Guide for the Management Server)* up to Step 14 that states the following:

   “If you use the Oracle Database Release 2, consider that starting with relational database management system (RDBMS) 11g R2, Oracle no longer provides the `libclntsh.so` and `libnnz11.so` 32-bit client libraries together with the 64-bit versions of their database server or the client.

   HPOM 9.xx on HP-UX 11i v3 and HPOM 9.xx on Sun Solaris 10 are built as 32-bit applications, so these libraries are needed for the proper operation."

NOTE Replace all instances of `11.2.0` with `12.1.0`.

3. As the `root` user, type:

   ```
   umask 022
   mkdir -p /opt/oracle/product/12.1.0/lib32
   chown oracle:oinstall /opt/oracle/product/12.1.0/lib32
   chmod 755 /opt/oracle/product/12.1.0/lib32
   ```
4. Install or uncompress Oracle instant client 12c and copy all its files to `/opt/oracle/product/12.1.0/lib32/`.
5. Set the `LD_LIBRARY_PATH` variable globally to `/opt/oracle/product/12.1.0/lib32`.

   To do so, type the following:

   ```
   crle -v -E LD_LIBRARY_PATH=/opt/oracle/product/12.1.0/lib32
   ```
6. Run `ovoinstall` and follow the installation prompt until the following text appears:

   ```
   Installation successfully finished
   NOTE: Before continuing with the server configuration, you can manually install available server patches.
   Do you want to automatically continue with Server configuration [exit,back,?,y|n,"y"] ?
   >
   ```
7. Install the Consolidated Server Patch 9.11.130.

   The patch includes the `ovoracle` and `omu500` scripts in the `newconfig` directory.

NOTE The fixed scripts can be customized, therefore it is required to copy or merge them from the `newconfig` directory into the final destination. If you did not do any modifications, you can copy them as follows:

```
cp /opt/OV/newconfig/OpC/etc/init.d/ovoracle /etc/init.d/ovoracle
```

8. Proceed with the HPOM installation by answering **y** to the rest of the installation prompts.

IMPORTANT To be able to use Oracle 12c in remote database environments, make sure you perform the following:

- Add the `unlimited tablespace` grant in “Configuring Users, Passwords, and Rights Manually” subsection (Step 5) of both Oracle database configuration scenarios described in the *HPOM Installation Guide for the Management Server* (“Setting Up HPOM with a Remote/Manual Oracle Database” and “Setting Up HPOM in an Oracle Real Application Clusters (RAC) Environment”) as follows:

  ```
  grant unlimited tablespace to opc_op;
  ```

- When setting the initialization parameters following the Oracle database configuration scenario described in the *HPOM Installation Guide for the Management Server* (“Setting Up HPOM with a Remote/Manual Oracle Database”, Steps 6-8) make sure the following is done in addition to setting the initalization parameters:

  — On Memory tab, set Memory Size to 500 MB

  — On Sizing tab, set Block Size to 16384 bytes and Processes to 200.

  Failing to set these parameters properly on these two tabs could result in problems during the database creation.

Installing HPOM 9.11.xx Patches

HPOM 9.11.xxx patches are installed either on top of the HPOM 9.10 release (with or without 9.10.xxx patches) or on top of any HPOM 9.1x.xxx patch. For more details about patches and enhancements, see “Changes with Latest Patches” on page 2.

NOTE For additional information about installing HPOM 9.xx, see “HPOM 9.xx Installation Notes” on page 9. For more details, see the *HPOM Installation Guide for the Management Server*.

Installation Steps

To install HPOM 9.11.xxx, follow these steps:

1. *If you have HPOM 9.10 or higher and HPOM Administration UI 9.1.0 or higher installed, ignore this step.* Install HPOM 9.10 by running the latest `ovoinstall` script that you can find at the following location:

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

   After you install HPOM, make sure to install HPOM Administration UI 9.1.0.

For the HPOM installation details, see the *HPOM Installation Guide for the Management Server* version 9.10. For the Administration UI installation details, see the *HPOM Administration UI Installation Guide* version 9.1.0.

2. Before continuing with the server configuration install the 9.11.xxx consolidated management server patch.

   This patch, as well as other HPOM 9.11.xxx patches, can be obtained from the following location:

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

   Install the patch as described in the patch information file that is also available on this site.

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

   After the agent depot packages installation is completed, 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
   ```

4. Install the rest of the HPOM 9.11.xxx patches as described in the respective patch information files. For more information about the patches, see “Changes with Latest Patches” on page 2.

IMPORTANT Before installing HPOM Core Server patch, make sure you get familiar with the section “HPOM Core Server Patch Installation Notes” on page 7.

Installing all the HPOM 9.11.xxx patches is mandatory if you plan to use IPv6-based communication or CAC authentication.

IMPORTANT If you plan to use CAC technologies to authenticate and authorize users, you must have the HPOM Accessories patch 9.10.230 or later installed before you enable CAC. For more information about the HPOM Accessories patch, see “HPOM Server Accessories Patch” on page 3.

HPOM Core Server Patch Installation Notes

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 written in the Special Installation Instructions section of the patch description.

When installing this patch, 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` 11.14.014, `HPOvJxpl` 11.14.014, `HPOvJsec` 11.14.043 and `HPOvJbbc` 11.14.049 are installed if the HP Operations agent version installed on the management server is 11.10 or higher.
- The `HPOvSecCS` 11.05.015, `HPOvJxpl` 11.05.015, `HPOvJsec` 11.05.046 and `HPOvJbbc` 11.05.047 packages are installed if the HP Operations agent version installed on the management server is 11.0x 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 11.14.014 (or 11.05.005, 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 11.05.015 and HP Operations agent 11.0x combination is required if you want to keep the HP Operations agent version 11.0x and autogranting is used.

NOTE With HPOvSecCS 11.14.014, 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 (HP Operations Manager Installation 10):

```
/opt/OV/bin/OpC/opcsvcertbackup -backup -passwd <password> -file \
/backup/cert_backup
```

NOTE After you install the new core patch, exchange trusted certificates as described in the *High Availability Through Server Pooling White Paper*. For both servers to work with the 1024 and 2048 certificates, follow the procedure by Step 7.

Keep in mind that the old agents work only with the 1024 certificate, whereas the new agent that registers on the server works with the new 2048 certificates keys. Therefore, if you want to upgrade the certificate to 2048 on the old agents so that they can work with both RSA keys, make sure that you perform also Step 8 of the exchange trusted certificates procedure.

Deinstalling HPOM 9.11.xxx

To deinstall HPOM 9.11.xxx, follow these steps:

1. Deinstall HP Operations management server 9.11.

   To do so, you must deinstall all HPOM 9.11.xxx patches as described in the patch information files that are available at the following location:

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

2. Complete the HP Operations management server 9.1x deinstallation.

For the instructions for deinstalling HPOM 9.1x, see the *HPOM Installation Guide for the Management Server* version 9.10.

HPOM 9.xx 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.

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 8.1x/9.xx, MSES and TIBCO SPI, and Infrastructure SPIs 2.0.
To use these products, you must also purchase a valid license. In addition, you receive AlarmPoint Express. AlarmPoint is an interactive alerting application, designed to capture and enrich events and route those events to the right person on any communication device, and give that person the ability to solve, escalate, or enlist others to resolve.

The AlarmPoint integration allows the appropriate technician to be notified directly using voice, email, pager, BlackBerry or other devices. Information about the failure is presented to the event resolver and decisions about how to handle the event can be made in real-time.

NOTE HP only distributes the AlarmPoint Express media, and does not provide support. AlarmPoint Express support and information may be obtained directly from AlarmPoint at:

http://express.alarmpoint.com/hp

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 "HPOM 9.11" on page 55 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.

For information on Oracle 11g Release 2 operating system requirements, see the Oracle documentation.

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/b32313/toc.htm

- **For Oracle 11.2:**

  http://docs.oracle.com/cd/E11882_01/install.112/e24349/toc.htm

- **For Oracle 12.1:**

http://docs.oracle.com/database/121/SSDQI/toc.htm#i1010738

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: Obtaining the libclntsh.so and libnnz11.so Libraries
- Task 5: 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 `/export/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 12 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:

https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=

Obtaining the libclntsh.so and libnnz11.so Libraries Oracle no longer provides the 32-bit `libclntsh.so` and `libnnz11.so` client libraries together with the 64-bit versions of the Oracle database server or client. Because HPOM on SunSolaris 10 is built as a 32-bit application, you must obtain these libraries for Oracle to work properly.

To obtain the `libclntsh.so` and `libnnz11.so` libraries, follow these steps:

1. Download the Oracle 11g Release 2 32-bit database client from the Oracle download page, and then uncompress it.

2. As the `root` user, set `umask` to allow users to access the Oracle binaries by running the following command:

   `umask 022`

3. Create the `lib32` subdirectory in the `ORACLE_HOME` directory by running the following command:

   `mkdir -p /opt/oracle/product/11.2.0/lib32`

4. Assign permissions to the `lib32` subdirectory by running the following commands:

   `chown oracle:oinstall /opt/oracle/product/11.2.0/lib32`

   `chmod 755 /opt/oracle/product/11.2.0/lib32`

5. Create a new Oracle home directory by running the following command:

   `mkdir -p <new_oracle_home_directory>`

For example:

```
mkdir -p /opt/oracle/product/11.2.0-32
```

6. Assign permissions to the new Oracle home directory.

   For example, run the following commands:

   ```
   chown oracle:oinstall /opt/oracle/product/11.2.0-32
   chmod 755 /opt/oracle/product/11.2.0-32
   ```

7. As the `oracle` user, export `ORACLE_HOME=<new_oracle_home>`, and then run the Oracle Universal Installer.

   During the Oracle client installation, in the Select Installation Type window, select **Instant Client**.

8. When the installation is finished, copy `libclntsh.so.11.1` and `libnnz11.so` from the newly created `ORACLE_HOME` directory to the `lib32` subdirectory in the old `ORACLE_HOME` directory.

   Run the following commands:

   ```
   cp /opt/oracle/product/11.2.0-32/libclntsh.so.11.1 /opt/oracle/product/11.2.0/lib32/
   cp /opt/oracle/product/11.2.0-32/libnnz11.so /opt/oracle/product/11.2.0/lib32/
   ```

9. Navigate to the `lib32` subdirectory of the old `ORACLE_HOME` directory by running the following command:

   ```
   cd /opt/oracle/product/11.2.0/lib32/
   ```

10. In the `lib32` subdirectory of the old `ORACLE_HOME` directory, create the following links:

    ```
    ln -s libclntsh.so.11.1 libclntsh.so
    ln -s libclntsh.so.11.1 libclntsh.so.10.1
    ```

    The new file structure of the old `ORACLE_HOME\lib32` directory must be the following:

    ```
    lrwxr-xr-x libclntsh.so -> libclntsh.so.11.1
    lrwxr-xr-x libclntsh.so.10.1 -> libclntsh.so.11.1
    -rwxr-xr-x libclntsh.so.11.1
    -rwxr-xr-x libnnz11.so
    ```

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/lib
      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/lib32/libclntsh.so libclntsh.so
      ln -s /opt/oracle/product/11.2.0/lib32/libclntsh.so libclntsh.so.1.0
      ln -s /opt/oracle/product/11.2.0/lib32/libclntsh.so libclntsh.so.10.1
      ln -s /opt/oracle/product/11.2.0/lib32/libclntsh.so libclntsh.so.11.1
      ln -s /opt/oracle/product/11.2.0/lib32/libclntsh.so libopcora.so
      ln -s /opt/oracle/product/11.2.0/lib32/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`).

Preparing the New Oracle Database to Be Used with the Administration UI To prepare the new Oracle database to be used with the Administration UI, follow these steps:

1. Stop and clean the Administration UI as follows:

   ```
   /opt/OV/OMU/adminUI/adminui clean
   ```

2. Update the `ORACLE_HOME` variable in the `midas_env.sh` file.
3. Update the following configuration files with the appropriate Oracle JDBC connection string:

   ```
   /opt/OV/OMU/adminUI/conf/ovoinstall.properties
   /opt/OV/OMU/adminUI/conf/ovoconfig.properties
   /opt/OV/OMU/adminUI/conf/opccfg.properties
   /opt/OV/OMU/adminUI/conf/ovoappl.properties
   ```

   Each of these configuration files contains a JDBC connection string which could, for example, look as follows:

   `ovodb.url=jdbc:oracle:thin:@<`*`SERVER`*`>:<`*`PORT`*`>:<`*`SID`*`>`

   The connection string should be in one line, without line feeds and without blanks inside it.

NOTE To obtain the correct Oracle JDBC connection string, check the `$ORACLE_HOME/network/admin/tnsnames.ora` file.

4. Start the Administration UI as follows:

   ```
   /opt/OV/OMU/adminUI/adminui start
   ```

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

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.

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

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 The default management server deployment includes HP Operations agent version 8.60. However, as of August 31, 2013, HP Operations agent 8.60 is no longer supported and must therefore be replaced with a supported version, namely version 11.0x or 11.1x.

NOTE To communicate with IPv6-enabled servers, you must have HP Operations agent version 11.13 installed. For more information on how to configure your HPOM environment for using IPv6, see the *HPOM IPv6 Support White Paper*.

To update HPOM to a supported agent version, request the agent media for version 11.0x or 11.1x from HP and install the agent on the management server. The agent installation and deployment is described in the HP Operations agent documentation, which is available from https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

In addition, download and install the latest HP Operations agent patches from HP Software Support Online at http://www.hp.com/go/hpsoftwaresupport.

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 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.

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.

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 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 https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword= 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.

NOTE Self-signed certificates created during the Administration UI installation can be replaced with the custom CA certificates. For more information, see “Replacing Self-signed Administration UI Certificates with Custom Certificates” on page 26.

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*.

Features, Enhancements, and Changes Introduced with HPOM 9.11.xxx

This section contains the support announcements, features, and enhancements that are introduced with HPOM 9.11.xxx.

HPOM 9.11.110

New Variables

```
AGENT_REQ_NUM_WARNING
AGENT_REQ_NUM_CRITICAL
OPC_API_NO_NODE_DEL_ACK
```

New CLI

An option `-timestamp` for the `opccfgupld` utility is available. This option preserves the timestamps of source instrumentation and executable files that need to be uploaded. The `-timestamp` option can be used only together with the `-add` and `-replace` options.

The `opccfgdwn` utility always preserves the timestamp of instrumentation and executables.

Java GUI

- Java GUI automatically triggers configuration reload upon both Major and Minor configuration synchronization if the following configuration settings are defined:
  - `OPCUIWWW_DISABLE_NOTIF_ONLY_AUTO_RECONNECT` is set to `TRUE`
  - `OPCUIWWW_DISABLE_ONLINE_CONFIG_SYNC` is set to `DISABLE_NOTIF_ONLY`
- Java GUI displays a message group label instead of a name in the message group column. If there is no label for a message group, Java GUI displays its name.

Administration UI

- Specific Trap condition edit form (available from Edit policy -> Tab conditions -> Edit condition) is no longer a mandatory field.
- By default, Administration UI allows Simultaneous Session Logons (that is, one user can have simultaneously more than one session on one system (by using different browsers) or on different systems.)

  You can turn off this function by appropriately editing the following properties in the `/opt/OV/OMU/adminUI/conf/auth.properties` configuration file:

  - `userauth-filter.concurrentSessionsEnabled`

    Restricts users from logging on more than once (`true|false`).
  - `userauth-filter.concurrentSessions`

    Shows how many concurrent sessions per user is allowed.
  - `userauth-filter.inactivityTimeout`

    Configures inactivity period.

- `userauth-filter.automaticLogout`

  Performs automatic logout if the number of allowed concurrent sessions is exceeded.

Miscellaneous

- The `opchamgr` utility performs retries for the `ping` check. To configure this, override the defaults from the `/etc/opt/OV/hamanager/hamanager.conf` file with the following settings:
  - `PING_RETRIES`
    Number of `ping` retries if `ping` fails (default is 3)
  - `PING_RETRY_DELAY`
    Delay in seconds before retrying `ping` (default is 5).
- The `opcmomchk` command reports warnings in case several operations are listed in the same `MSGOPERATION` section.
- The error message that is displayed when a managed node does not resolve to the new IP address of an IP Address Change Event (IPCE) from the agent is more specific, as follows:

  “`Name resolution for Node <node name> is not (yet) in sync for new IP address <IP> as sent in IP change event from the agent.`”
- HP Operations agent upgrade works if a managed node that hosts the agent is behind proxy.
- The `opcnode -add_node` command fails in case a managed node with network type `NETWORK_IP` cannot be resolved and `ip_addr` is not specified. The nodes that cannot be resolved from topology synchronization (for example, from HP Operations Manager for Windows) are added with the machine type `non-IP/other/other`.
- Nodes added through topology synchronization from HP Operations Manager on Windows are added properly in case the node can be resolved by the name service.
- It is possible to configure HPOM so that no message changes are sent to the Incident Web Service if a message is in the history. To enable this feature, use the following command:

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

  You must restart the server processes for this change to take effect.

HPOM 9.11.100

New Variables

`DISABLE_SITESCOPE_NODE_MODIFICATION`	`OPC_USE_PAM_RESET_COUNTER_AND_DELAY`

New CLI

The `opcmsgsrpt` utility has a new option, `-l`, for setting a long output format that allows having up to 999 characters in a line. You can define a default page size if this option is not used by using the following configuration settings:

`OPC_RPT_COLUMNS_PER_LINE` Number of columns per line (default: 86, range: 80–999)

`OPC_RPT_LINES_PER_PAGE` Number of lines per page (default: 55)

Administration UI

- Selected drop-down menu options are executed after choosing the >> action.

- When performing the Download to local computer action, the SaveAS window that enables you to save or open a file or cancel an action appears.
- In the list of regroup conditions, all nodes of a regroup condition are displayed regardless of the number of nodes.
- Port and certificate values are properly managed during the patch deinstallation process.

IMPORTANT Because the `unpatch` command is deprecated, the Administration UI is deinstalled by using the `deinstall` command.

However, you should use the `unpatch` command for the deinstallation of the Administration UI patch versions earlier than 9.11.100.

Miscellaneous

- HPOM does not send CMA change events anymore if the duplicate counter was increased and text or severity was changed. The only events that HPOM sends are the following: a modify severity event when the severity is changed, a modify text event when the text is changed, and a CMA modify event when the CMAs are changed.
- If you want `opcpolicy` to check only the server policy type, set the `OPC_API_DONT_USE_AGT_?OLTYPE` server configuration variable to `TRUE`. This means that you can have a log file policy and Windows event log policy with the same name. By default, `opcpolicy` does not allow having the same policy name and agent policy type.
- `opc_node_change.pl` correctly changes IPs and hostnames for both IPv4 and IPv6 nodes.
- It is not possible to create a node or a virtual node if a node group with the same name already exists. Trying to use the same name for the node or the virtual node and the node group results in an error message on both the management server (if using `opcnode`) and Administration UI sides.

Support Announcements

The HP Operations management server patch 09.11.100 introduces support of the following:

- HPOM is supported on Tomcat web server version 7. This enables you to use all the advantages of the Common Access Card authentication feature supported on Tomcat 7. For details, see the *Common Access Card Authentication White Paper*.
- IPv6 is supported with server pooling. For detailed information, see the *Enabling IPv6-based Communication in an HPOM Environment White Paper* and the *High Availability Through Server Pooling White Paper*.
- The HA Manager supports IPv6 addresses. For detailed information, see the *High Availability Manager White Paper*.
- Java GUI:
  - The Java GUI is supported on Windows 8 and 8.1.
  - `ITO_OP` online pages, which you can access through `http://<`*`HPOM_server`*`>:8081/ITO_OP/` or `https://<`*`HPOM_server`*`>:8444/ITO_OP/`, contain the support information for Mac OS X.

HPOM 9.11

The HPOM 9.11 release introduces the following:

- **CAC authentication**

  HPOM supports CAC technologies to authenticate and authorize users. By configuring HPOM for CAC authentication, access to HPOM user interfaces is allowed only to operators who possess a valid CAC with a valid certificate. Therefore, security is increased and access procedures are simplified.

  IMPORTANT If you plan to use CAC technologies to authenticate and authorize users, you must have the HPOM Accessories patch 9.10.230 or later installed before you enable CAC. For more information about the HPOM Accessories patch 9.11.100, see the *HPOM Software Release Notes* version 9.11.100.

  For more information about CAC authentication, see the *HPOM Common Access Card Authentication White Paper.*

- **IPv6-based communication**

  HPOM supports communication over the network based on the IPv6 internet protocol.

  IMPORTANT To communicate with IPv6-enabled servers, you must have HP Operations agent version 11.13 installed.

  For more information on how to configure your HPOM environment for using IPv6, see the *HPOM IPv6 Support White Paper*.

IMPORTANT To be able to use CAC authentication or IPv6-based communication, you must have all the HPOM 9.11 patches installed. For more information about the patches and the installation details, see the *HPOM Software Release Notes* version 9.11.100.

New Variables

```
OPC_REPLACE_KNOWN_NODE_NAME_BEFORE_MSI
OPCUIWWW_DISABLE_NOTIF_ONLY_AUTO_RECONNECT
OPC_POLICY_LIST_ITEMS_PER_PAGE
OPC_POLICY_LIST_WIDGET_SIZE
JGUI_API_ENABLED
OPCUIWWW_APP_C_SORT
OPC_JGUI_TIMEOUT
STARTUP_MESSAGE_VISIBLE
OPC_USE_ADVANCED_RAW_EDITOR
```

New CLIs

A new script, `OvSvcDiscTroubleShooter.sh`, is available. This script parses through the `SvcDiscServer.log` file and provides suggestions on how to fix any problems. The usage syntax is as follows:

```
OvSvcDiscTroubleShooter.sh [-file <logfile>] [-report] [-analyze] \
[-debug ON|OFF <size in MB>]
```

The `OvSvcDiscTroubleShooter.sh` script accepts the following parameters:

`-report` Prints errors only.

`-v` Displays verbose output.

`-analyze` Checks the errors against the local model.

`-file`	Uses the specified file rather than the `OvSvcDiscServer.log` file specified in `/var/opt/OV/shared/server/log`.
`-debug`	Turns on or off verbose logging and sets the size of the log file to the specified size in MB.

CAUTION The `-debug` option automatically restarts the OvAutoDiscovery server service.

Java GUI

You can set up a message filter in the Java GUI history message browser based on CMA pattern matching.

Administration UI

- Autocomplete is disabled when logging on to the Administration UI. Therefore, when you type the first letter or letters of a user name, a password, or a display station name, the application does not predict one or more possible words as choices. By autocomplete being disabled, security is increased.
- The Administration UI cookies are modified so that they comply with the security standards (that is, they are secure, non-persistent, inaccessible from other domains, and so on).
- You can use the Administration UI from within the Internet Explorer standard mode. You can edit user responsibility matrixes, execute conditions pattern tests and use the Administrative menu.

Enhancements

The following CLIs are enhanced with the HPOM 9.11 release:

- `itochecker`
  The names of HPOM patches are properly displayed in the `itochecker` report.

  The `itochecker` option `-help` is also updated. There are no more false error reports for the node check. The Administration UI patches and hotfixes are added to the report.
- `opccfgdwn` and `opccfgupld`
  These utilities wait for each integration to finish or until a configured timeout occurs, which can be set by using the `OPC_CFG_INTEG_TIMEOUT` configuration variable.
- `opcsvcam`
  `opcsvcam` so far did not reconnect if the connection to `opcscm` was lost. this utility exits if the connection to `opcsvcm` is lost. In this case, `ovcd` restarts `opcsvcam`, and the newly started `opcsvcam` connects to `opcsvcm` again.

  This scenario applies also for `opccustproc1`, and is performed in the service API. When the connection is lost, the only processes that stop are the ones listed in `OPC_SVCAPI_KILL_PROCESSES_CONN_LOST` (by default, `opcsvcam` and `opccustproc1`). This way stopping the custom applications that use the service API is avoided.
- `opcdbpwd`
  All special characters in passwords are accepted except the quotation marks (`"`). However, special characters `` ` ``, `$`, `\`, and `"` cannot be handled by `ovoconfigure` and `opcdbsetup`, so they need to be excluded from the password when running these scripts. You can add these characters later to the password by using the `opcdbpwd` utility.

For more information about the enhanced CLIs, see the manual pages.

Support Announcements

The HPOM 9.11 release introduces support of the following:

- Java GUI:
  - The Java GUI is supported on Windows 2003 Server (64-bit) and Windows 2008 R2 (64-bit).
  - You can use the cockpit view on Linux RHEL/Firefox and Mac OS X/Safari, both with latest JRE 7 version and Flash plugin. The supported Flash versions are 10 and 11.
  - The Java GUI supports JRE 1.7.0_25.

Features, Enhancements, and Changes Introduced with 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 78.

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.

NOTE Self-signed certificates created during the Administration UI installation can be replaced with the custom CA certificates. For more information, see “Replacing Self-signed Administration UI Certificates with Custom Certificates” on page 26.

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 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 73.

Replacing Self-signed Administration UI Certificates with Custom Certificates

Replacing self-signed certificates created during the Administration UI installation with the custom CA certificates includes the following tasks:

- Task 1: Backing up the Current Keystore and Truststore
- Task 2: Replacing the Certificates

Backing up the Current Keystore and Truststore Make sure that you back up the current keystore and truststore in a directory outside the Administration UI (for example, the `/tmp` directory). To do so, run the following commands:

```
cp /opt/OV/OMU/adminUI/conf/servicemix/keystore_webapp.jks <directory>
```

```
cp /opt/OV/OMU/adminUI/conf/servicemix/truststore_webapp.jks <directory>
```

Replacing the Certificates To replace self-signed certificates created during the installation with custom CA certificates, follow these steps:

1. Make sure that your certificate is available in the PKCS12 format.
2. Remove all old certificates from the keystore and the truststore of the WebApp by following these steps:
   a. Check the contents of the keystore and the truststore by running the following command:
   ```
   /opt/OV/OMU/adminUI/adminui ant -f run.xml https_list_webapp
   ```
   b. Remove the certificates by running the following commands:
   ```
   /opt/OV/OMU/adminUI/jre/bin/keytool -delete -alias <alias_name> -keystore \
   /opt/OV/OMU/adminUI/conf/servicemix/keystore_webapp.jks
   ```
   ```
   /opt/OV/OMU/adminUI/jre/bin/keytool -delete -alias <alias_name> -keystore \
   /opt/OV/OMU/adminUI/conf/servicemix/truststore_webapp.jks
   ```
   When running these commands, you must provide the correct passwords. The default ones are `password`. However, check the `"password"` and `"trustPassword"` properties respectively in the `/opt/OV/OMU/adminUI/conf/jetty.xml` file to see if the default passwords were changed. In this case, make sure to use the changed ones.

   c. Verify that the certificates are removed by running the following command:
   ```
   /opt/OV/OMU/adminUI/adminui ant -f run.xml https_list_webapp
   ```
   An output similar to the following one should appear:

```
... Your keystore contains 0 entries ...
```

3. Import the p12 files to the keystore by running the following command:

   ```
   /opt/OV/OMU/adminUI/jre/bin/keytool -importkeystore -deststorepass <dest_store_pass> \
   -destkeypass <dest_key_pass> -destkeystore /opt/OV/OMU/adminUI/conf/servicemix/\
   keystore_webapp.jks -srckeystore <store_name>.p12 -srcstoretype PKCS12 -srcstorepass \
   <src_store_pass> -alias <alias_name>
   ```

   In this instance, the default passwords for both *<dest_store_pass>* and *<dest_key_pass>* are `password`. However, check the `"password"` and `"keyPassword"` properties respectively in the `/opt/OV/OMU/adminUI/conf/jetty.xml` file to see if the default passwords were changed. In this case, make sure to use the changed ones. The default password for *<src_store_pass>* is the one entered when the `p12` file was created.

   Use the `-alias` option only if it was used when creating the `p12` file.

NOTE If you do not use the `-destkeypass` option, the value of the `"keyPassword"` property in the `/opt/OV/OMU/adminUI/conf/jetty.xml` file should be entered as the value for *<src_store_pass>*.

   If you have the Administration UI and HPOM Server Accessories 9.10.230 patches installed (or higher), you can use `/opt/OV/nonOV/jre/b/bin/keytool` instead of `/opt/OV/OMU/adminUI/jre/bin/keytool`. However, it is recommended to use the latter one because in this case you can deinstall the Administration UI patch and revert to version 9.1.0 after you complete replacing the certificates.

4. Import the crt file to the truststore by running the following command:

   ```
   /opt/OV/OMU/adminUI/jre/bin/keytool -import -alias <alias_name> -keystore \
   /opt/OV/OMU/adminUI/conf/servicemix/truststore_webapp.jks \
   -storepass <store_pass> -file <crt_name>.crt
   ```

   In this instance, the default value for *<store_pass>* is `password`. However, check the `"trustPassword"` property in the `/opt/OV/OMU/adminUI/conf/jetty.xml` file to see if the default value was changed. In this case, make sure to use the changed one.

   Use the `-alias` option only if it was used when creating the `crt` file.

5. Check the contents of the keystore and the truststore by running the following command:

   ```
   /opt/OV/OMU/adminUI/adminui ant -f run.xml https_list_webapp
   ```

IMPORTANT Make sure that the entry types are `PrivateKeyEntry` in the keystore and `trustedCertEntry` in the truststore.

6. Restart the Administration UI by running the following commands:

   ```
   /opt/OV/OMU/adminUI/adminui clean
   ```

   ```
   /opt/OV/OMU/adminUI/adminui start
   ```

New Policy Types

HPOM templates are 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 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:

https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=

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 Java GUI instances 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:

https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=

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.

ZFS File System Support

HPOM can be installed on one or more Solaris ZFS file systems. Veritas Cluster Server versions 5.0 and 5.1 as well as Sun Cluster versions 3.2 and 3.3 are supported on the ZFS file systems.

A ZFS file system is created in a ZFS pool and is automatically mounted when created.

For more information about ZFS, see http://www.oracle.com/us/sun/index.htm.

Solaris Zones Support

HPOM can be installed on Solaris global and non-global zones. A global zone is created when you install the Solaris operating system. Zones hosted by a global zone are known as non-global zones. There are two types of non-global zones: Sparse Zones and Whole Root Zones. HPOM 9.xx supports only Whole Root Zones.

Remote Database Support in a Solaris Non-Global Zone

The following remote database scenarios in which the Oracle server is installed in a Solaris full-root non-global zone, either on the same machine as the HP Operations management server or a different one, are supported:

- HPOM and Oracle on different machines, with Oracle in a non-global zone
- HPOM and Oracle on the same machine, both in non-global zones
- HPOM and Oracle on the same machine, HPOM in a global zone, Oracle in a non-global zone

NOTE This environment has some limitations because the HP Operations server in the global zone can detect the processes that run in non-global zones. Because of that there cannot be any other HP Operations management server or agents running in the non-global zones.

- HPOM on a cluster node in global zones, Oracle on a cluster node in a non-global zone

Logical Domains Support

HPOM can be installed on Solaris Logical Domains (LDoms). ZFS file systems within LDoms are also supported.

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

Cluster Support

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

- Sun Cluster 3.2 and 3.3
- Veritas Cluster Server 5.0 and 5.1

New CLIs

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

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

For more information, see the corresponding manual pages.

New Variables

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

DISABLE_SITESCOPE_NODE_MODIFICATION
OPC_ACK_DUPLS_IF_NORMAL_MSG
OPC_ALLOW_DUPLICATE_IP
OPC_ALWAYS_KEEP_CURRENT_POLICY_STATUS
OPC_CFGDWN_OMIT_VIRTUAL_GROUP_DOWNLOAD
OPC_CFGUPLD_BLOCK_RETRY
OPC_CSA_ALLOW_IP_MISMATCH
OPC_CSA_LINUX_X64_PLATFORM
OPC_CSA_USE_OS_BITS[a]
OPC_CFGUPLD_ONLINE_SVC_UPDATE
OPC_DEPLOY_IF_CALLBACK_FAILS
OPC_DIST_OMIT_ERROR_AGT_NOT_INST
OPC_DONT_EMPTY_NS_CACHE
OPC_DONT_LOG_REUSED_COREIDS
OPC_EMPTY_NS_CACHE
OPC_ENABLE_FWDCHAIN_FWDSENDER_CMA
OPC_FILTERS_BY_LAYOUT_GRP_LABEL
OPC_FORWARD_READONLY_MSGS
OPC_HBP_DOUBLE_CHECK_DELAY
OPC_HBP_DOUBLE_CHECK_DELAY_BUFFER
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
OPC_MSGKEY_MODIFY_TEXT
OPC_NAMESRV_EXPIRE_MODE
OPC_NAMESRV_TTL
OPC_NO_ACK_VIA_CORR_IF_OWNED
OPC_OVHARG_START_LOCAL_AGENT
OPC_PING_SIZE
OPC_REJECT_CMA_DELETIONS
OPC_SERIALIZE_SERVICE_MODEL
OPC_SOURCE_FORW_NOTIF_TO_TT
OPC_SUPPRESS_IF_NO_CORRELATION
OPC_SUPPRESS_IF_NO_CORRELATION_MSGAPPLICATION
OPC_SUPPRESS_IF_NO_CORRELATION_MSGGROUP
OPC_SUPPRESS_IF_NO_CORRELATION_MSGOBJECT
OPC_TRUNC_MSG
OPC_XPL_SQL_TRACE
OPCRAGT_MAX_THREADS_TOTAL
OPCRAGT_OMIT_ERROR_AGT_NOT_INST
OPCRAGT_START_TIMEOUT
OPCRAGT_STOP_TIMEOUT
OPCRAGT_TIMEOUT
OPCUIWWW_KILL_APP
OPCUIWWW_KILL_APP_TIMEOUT

[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 APIs

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

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

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 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.
  - Service Actions are executed on user selected nodes only if there are no predefined nodes in service `.xml` file for these actions.
- 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 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`.
  - The Export button that you can use for exporting or writing messages to a file without using a printer is 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.

  - Changing labels for Message Browser columns in the Customize Message Browser Columns window results in changing the corresponding message attributes in the Message Properties window.
- Miscellaneous
  - Java GUI filtering 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 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
    ```
  - The HTTPS protocol is 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 Java GUI installation 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
```

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.

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.

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 severity order: unknown, normal, warning, minor, major, and critical.

For example:

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

In this instance, the severity labels are changed as described in Table 6.

Table 6 Severity Label Change

Default Severity Label	New Severity Label
unknown	this
normal	is
warning	new
minor	custom
major	severity
critical	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,?
```

In this instance, each occurrence of the `?` character is ignored and the default severity label is loaded.

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.

If you want to restore the default severity labels, delete the corresponding server configuration variable. For example:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opc -clear OPC_JGUI_SEV_EN
```

IMPORTANT For the changes to take effect, **File->Reload Configuration** must be selected.

Enhanced Message Forwarding in Flexible Management Environment

Message forwarding in flexible management environment is enhanced as follows:

- Server-to-server message forwarding between HPOM8.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 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`
- `opcremsyschk`
- `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. You can 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 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 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 be skipped on the passive cluster node by adding the p option to other options (for example, itochecker -12345p).
- The service engine 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.
- You can assign an instrumentation category to a policy group, not only to a policy.
- You can 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:
  - — `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 HA Manager–related changes are 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 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.
- The following two new options can 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`.
- 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 licensing-related changes are available:
  - The All Nodes and the Selected Node reports 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 30.
  - 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.
- The `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.

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 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

Variable	HPOM 8.xx Default	HPOM 9.xx Default
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. 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 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 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

Changed License Passwords

The HPOM 9.xx management server license password is different from the HPOM 8.xx management server license password. If you plan to upgrade from HPOM 8.xx to HPOM 9.xx, you must request a new license password from the Password Delivery Center (https://webware.hp.com/welcome.asp). HPOM 9.xx is not able to run with a HPOM 8.xx management server license password. All other HPOM 8.xx license passwords, such as agent license passwords, can be re-used and might be migrated to the new IP address. For details, refer to the *HPOM Installation Guide for the Management Server*.

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 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 Sun Solaris.

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 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).

- You can 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
  ```

- You can 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
  ```

HPOM 9.xx and Other HP Software Solutions

Integration

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

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

- HP Operations agent 11.0x
- HP Operations agent 11.1x
- HP Performance Manager 8.2x and HP Performance Manager 9
- 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
- Business Service Management (BSM) 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 9.1x from HPOM 8.xx.

Obsolete Management Server Platforms

The following Solaris management server platforms are obsolete:

- Sun Solaris 8
- Sun Solaris 9

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
- 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 25.

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 documents 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*
- *HPOM Administration UI Release Notes*

  Note that the information contained in this document can be found in the present *HPOM Software Release Notes*.

Miscellaneous

- 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.

Known Problems, Limitations, and Workarounds

HPOM 9.11

Management Server

Symptom QCCR1A173284
opcmsgm stops if LANG is not set to UTF8

opcmsgm occassionally stops if $LANG is not set to an UTF8 value.

Solution

With HPOM 9.x the HP Operations management server processes are required to run with the $LANG value set to UTF8, the character set used also by the database.

To make sure the server processes are always started with this character set, enable setting $LANG before starting HPOM processes, as follows:

```
ovconfchg -ns ctrl.env LANG en_US.UTF-8
```

Symptom QCCR1A157983
The opcpolicy check=yes command does not warn in case there are conditions with duplicate descriptions

In case there are conditions with same descriptions in the same policy, the following error message appears in the Administration UI:

```
The following errors have been detected (marked with !):
Condition descriptions must be unique. Duplicate condition description on conditions number: 1, 2
Please, correct them and try saving again.
```

The opcpolicy and opccfgupld commands should detect this as a syntax error.

Solution

Manually change the condition descriptions.

Symptom QCCR1A168210
Manual page for opcdata lists the wrong attribute OPCDATA_APP_IP_STRING

When manual page for opcdata is run, the OPCDATA_APP_IP_STRING attribute is listed instead of OPCDATA_IP_STRING.

Solution:

Use OPCDATA_IP_STRING instead of OPCDATA_APP_IP_STRING.

Symptom QCCR1A168974
Sometimes MANAGER and MANAGER_ID variables are not set after the 9.11 HPOM and HP Operations agent 11.13 installations. This affects Service Discovery.

After installing the HPOM patch 9.11.030 and HP Operations agent version 11.13.07, variables MANAGER and MANAGER_ID fail to be set. As a result, Service Discovery server does not get data for Infra Spi. This problem cannot be always reproduced.

Solution

If the MANAGER and MANAGER_ID variables are missing in the sec.core.auth namespace, set them as follows:

1. To set the MANAGER variable, run:

   ```
   /opt/OV/bin/ovconfchg -ovrg server -ns sec.core.auth -set MANAGER <full_name_of_server>
   ```

   To set the MANAGER_ID variable, follow these steps:

   a. Get node ID by using the following command:

   ```
   /opt/OV/bin/OpC/utils/opcnode -list_id node_name=<full_name_of_server>
   ```

   ID field appears on the screen.

   b. Run the following command:

   ```
   /opt/OV/bin/ovconfchg -ovrg server -ns sec.core.auth \
   -set MANAGER_ID <ID_from_previous_command>
   ```

2. Restart the agent as follows:

   ```
   /opt/OV/bin/ovc -restart AGENT
   ```

Symptom QCCR1A168997
Installation of the IPv4 remote agent (11.13.007) fails if variable IsIPV6Enabled set to TRUE

In the IPv6 environment the IsIPV6Enabled variable should be set to TRUE. However, if this variable is set to TRUE, the IPv4 remote agent (11.13.007) installation fails.

Solution

Before installing the IPv4 agent, temporarily set the IsIPV6Enabled variable to FALSE, as follows:

```
ovconfchg -ns sec.cm.server -set IsIPV6Enabled FALSE
```

Symptom QCCR1A169126
HP Operations agent 11.12 cannot detect Redhat High Availability Addon 6.3 (RH cluster suite)

The ovclusterinfo command is throwing exception in the HP Operations agent 11.12 Linux cluster box.

Solution

Use HP Operations agent 11.10.

Java GUI

Symptom QCCR1A138045/QCCR1A172931
Java GUI displays a message group name instead of a label in message browsers

In the Java GUI message browsers, the message group name is displayed instead of its label.

Solution

None.

Symptom QCCR1A121738
Messages cannot be acknowledged in the Java GUI

The attempt to acknowledge messages in the Java GUI, by using opc_adm or any other user fails.

Solution

This issue is caused by the bulk message insertion mechanism (default with HPOM 9.xx).

For performance reasons, the bulk message insertion mechanism inserts messages only in opc_act_messages without checking. If the message with the same ID is already in opc_act_messages, it is rejected because of the primary key violation. However, if the message with the same ID is in opc_hist_messages, it is not detected.

To avoid the problem, disable the bulk insert by setting it to:

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

Since there are already some messages with the same ID in `opc_act_messages` and also in `opc_hist_messages`, it is recommended to download all history messages to exclude the old messages. For example:

```
opchistdwn -older 0s -file <filename>
```

Symptom QCCR1A162458
The JavaGUI on 64-bit Windows 7 Enterprise does not find IE10

An attempt to use the Java GUI in Internet Explorer 10 produces the following warning:

```
Warning: Internet Explorer libraries not found on a system. ActiveX web browser options are
disabled.
```

Solution

Use an older version of Internet Explorer.

Symptom QCCR1A165183
Detached windows in the Java GUI do not work properly

It is not possible to attach the window back by using the Attach Window icon. Also, the following error message is displayed when selecting File > Close:

```
ERROR MSG, 1:39:35 PM, com.hp.ov.it.ui.OvEmbMainMenu$FileMenu$1: This menu item should be
available only for detached windows!
```

Solution

Use JRE 6.

Administration UI

Symptom QCCR1A171445
After upgrading the Administration UI to version 9.11, the connection with HPOM is lost

After upgrading the Administration UI to version 9.11.040, the following settings in the `$adminui/conf/ovoinstall.properties` configuration file are not recognized:

```
ovoinstall.useOpenSSH=true

ovoinstall.sshOptions=StrictHostKeyChecking\=no,BatchMode\=yes
```

As a consequence, the Administration UI fails to deploy the `midas-beovocfg` assembly and therefore the connection with HPOM is lost.

Solution

Perform the following steps:

1. Stop the Administration UI as follows:

   ```
   /opt/OV/OMU/adminUI/adminui stop
   ```

2. From the `/opt/OV/OMU/adminUI/conf/ovoinstall.properties` configuration file, remove the following settings:

   ```
   ovoinstall.useOpenSSH=true

   ovoinstall.sshOptions=StrictHostKeyChecking\=no,BatchMode\=yes
   ```

3. Start the Administration UI as follows:

   ```
   /opt/OV/OMU/adminUI/adminui start
   ```

Symptom QCCR1A124391
Administration UI browser fails if a host name contains an underscore

The Administration UI does not support underscores in hostnames, therefore the connection to the database fails.

Solution

This problem cannot be resolved by HP because it is related to the 3rd party product for which HP does not have ownership.

Symptom QCIM1A167210
Adding a node in the Administration UI results in an error being displayed

When performing Node Bank -> Add Node ..., the following error message appears:

```
An internal error occurred:
```

```
Duplicate widget id "1__ms____x86____winnt" detected at fd:group - file:
/opt/OV/OMU/adminUI/webapps/midas/work/webapp/content/ovo/nodeedit/forms/ \
edit-node-model-<SERVER>.xml:XXXX:YYY. Container widget "node-type-platform-sel" at fd:union -
file:/opt/OV/OMU/adminUI/webapps/midas/work/webapp/content/ovo/nodeedit/forms/ \
edit-node-model-<SERVER>.xml....
```

This error indicates that the `AgentPlatform` file appears more than once on the HP Operations management server. The `AgentPlatform` file should be unique for all platforms, but sometimes multiple `AgentPlatform` files are added for one platform with one or more agent hotfixes.

Solution

Check your system for any duplicates at the location where the problem is found. Considering the error message text, these duplicates are probably located inside the following directory:

```
/var/opt/OV/share/databases/OpC/mgd_node/vendor/ms/x86/winnt
```

Perform the following steps:

1. Upgrade the Administration UI to the latest patch version (at least 9.10.240).
2. Clean the Administration UI:

   ```
   /opt/OV/OMU/adminUI/adminui clean
   ```

3. Generate new machine types:

   ```
   /opt/OV/OMU/adminUI/adminui machtypes
   ```

4. Regenerate Web assemblies:

   ```
   /opt/OV/OMU/adminUI/adminui webassemblies
   ```

5. Start the Administration UI:

   ```
   /opt/OV/OMU/adminUI/adminui start
   ```

Symptom QCCR1A165161
Category with a white space in its name cannot be uploaded

When uploading a category that contains a white space in its name, no errors are reported. However, a message appears stating that an upload was successfully performed but the category is not uploaded.

The problem is not reproduced by using the `opccfgdwn` and `opccfgupld` commands.

Solution

Remove the white space from the category name.

Symptom QCCR1A165292
Internal error occurs if an SQL file with the same name already exists

When adding an SQL report file with the name that already exists, an internal error is displayed instead of the message about the existing file name.

Solution

Avoid using the existing file names.

Symptom QCCR1A165471
Event Correlation Composer policy cannot be copied by using the Administration UI

When copying Event Correlation Composer policy by using the Administration UI, the following error is displayed:

```
... edit-ecc-policy-model.xml (No such file or directory (errno:2))
```

Solution

You can copy the policy contents from the Content tab by using the keyboard.

Symptom QCCR1A168276
Internal error occurs when editing a node added as non IP -> other -> other

When editing a node with the IP address assigned in DNS or in the `/etc/hosts` file, and added as `non IP -> other -> other` in the Administration UI, an internal error occurs.

Solution

Do not select `non IP -> other -> other` node type for nodes with IP addresses.

Symptom QCCR1A168550
Adapt the Administration UI CSS for the IE Standard Mode

When operating with the Administration UI in the Internet Explorer standard mode some buttons are not properly displayed. In addition, some spaces are wrongly positioned and the text area with three rows has too big scroller arrows.

Solution

Run the Administration UI in the Internet Explorer compatibility mode.

Symptom QCCR1A165429
Policy SNMP ECS Traps cannot be copied by using the Administration UI

It is not possible to copy the SNMP ECS Traps policy by using the Administration UI.

Solution 1

Run the following command:

```
opcpolicy -copy_pol pol_name='SNMP ECS Traps' pol_type=trapi \
pol_name_to='copy_of_SNMP ECS Traps'
```

Solution 2

Set a number value for the Specific Trap field in every condition.

Symptom QCCR1A171106/QCCR1A171107
Administration UI aborts when the password expires for Active Directory logon if PAM integration is used

If you use PAM integration for Active Directory logon, the Administration UI aborts upon the user password expiration.

Solution

Use LDAP instead of PAM for Active Directory integration in the Administration UI.

HPOM 9.xx Releases

Installation

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 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>]
   ```

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 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 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 QCCR1A92608
Database creation on Solaris 10 may fail even if DISABLE_NUMA is set to TRUE and exported

The creation of the database on Solaris 10 may fail with the following errors even if the `DISABLE_NUMA` environment variable is set to `TRUE` and exported:

```
ORA-12853: insufficient memory for PX buffers
ORA-04031: unable to allocate ... bytes of shared
```

Solution

Increasing `memory_target` solves this problem.

To increase `memory_target`, modify `/opt/OV/bin/ovdbsetupo1_opc.sh` by changing the following line:

```
memory_target = 500M
```

to

```
memory_target = 750M
```

IMPORTANT This change must be made after installing the HPOM software and the latest server patch (if applicable), but before calling `ovoconfigure` or `opcdbsetup`. `memory_target` can be set to an even higher value, if needed.

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 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 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.UTF-8
```

Restart the processes by running the following commands:

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

Symptom QCCR1A109200
Modified category instrumentation files are not deployed to agent if a system time zone is eastern than UTC

Category instrumentation files that were deployed and afterwards modified on the management server, cannot be deployed again to the agent due to miscalculated file timestamp when TZ is more than UTC (TZ>UTC.)

Solution

Deploy all instrumentation files with a force option, for example:

```
# opcragt -distrib -instrum -force <node_name>
```

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 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=solaris \
   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 QCCR1A61275
During ovoremove, an error occurs while removing HPOvCtrl or some other package

During server removal using the ovoremove script, a message similar to the following appears:

```
HPOvCtrl     (6.10.025) . . . . FAILED
ERROR:  Error occurred while removing HPOvCtrl package
Please check /var/opt/OV/log/OpC/mgmt_sv/installation.log.error for details
```

After checking the installation log files, you find that the reason for this problem is package dependency.

Solution

This package cannot be removed because some other packages depend on it. For this reason, use skip to continue. This will skip package removal, and the package will stay on the system. For example:

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

Symptom QCCR1A110770
Oracle aborts on systems with a lot of CPUs

On a Solaris system with a lot of CPUs, Oracle may abort. The amount of SGA memory that Oracle needs depends on the number of CPUs. Oracle may need more memory to work properly.

Solution

Increase the memory_target initialization parameter. For example, increase it to 1024MB as follows:

1. Exit all GUIs and shut down the HP Operations management server processes as follows:

   ```
   # ovc -kill
   ```

2. Switch to the oracle user as follows:

   ```
   # su - oracle
   ```

3. Make sure that `ORACLE_HOME` and `ORACLE_SID` are set correctly.
4. Log on to `sqlplus` as DBA by running the following:

   ```
   $ sqlplus "/ as sysdba"
   ```

5. If Oracle is not currently running, start it to the nomount state as follows:

   ```
   SQL> startup nomount;
   ```

6. Check the current value of `memory_target` as follows:

   ```
   SQL> show parameter memory_target
   ```

7. Increase memory_target in the spfile to 1024M as follows:

   SQL> alter system set memory_target = 1024M scope = spfile;

8. Restart Oracle as follows:

   ```
   SQL> shutdown;
   SQL> startup;
   SQL> exit
   ```

9. As the `root` user, start HP Operations management server processes as follows:

   ```
   # ovc -start
   ```

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

When you install HP Performance Manager 8.2x 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 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 QCCR1A145210
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 QCCR1A157490
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 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 QCCR1A127613
Small stack size causes opcuiwww to core dump

`opcuiwww` core dumps if the `OPC_USE_JB_MSGS_GET` configuration variable is set to `TRUE` and a pattern node matching several physical nodes exists. The problem appears because of the small stack size (8192).

Solution

Extend the stack size by adding the following command into the `opcuiwww.sh` script before the `opcuiwww` command:

```
ulimit -s 32767
```

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 QCCR1A55909
Java GUI cannot Connect when the ito-e-gui Service is in Maintenance State

If Java GUI cannot connect to the HPOM management server running on Solaris 10, it is possible that the `ito-e-gui` service is in maintenance state.

On Solaris 10, `inetd.conf` is obsolete, and `ito-e-gui` must be registered as a service. This service is responsible for starting the `opcuiwww.sh` script when Java GUI starts connecting to the HPOM Management Server.

If something goes wrong with `opcuiwww`, `ito-e-gui` switches into maintenance, and manual intervention is needed to put the service back online. When the service is in maintenance state, it is not possible to make a connection from the Java GUI.

Solution

To get the current service status, use the following command:

```
svcs | grep ito
```

If the `ito-e-gui` service status is maintenance, switch it back online using the following command:

```
svcadm clear /network/ito-e-gui/tcp
```

The Java GUI should be able to connect to the HPOM Management Server.

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 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

The default behavior of the Java UI when reloading configuration is to set all service maps to the default view in the Preferences dialog. If the service maps are saved in the Console Settings file, they retain their view setting.

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 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.

Administration UI

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 QCCR1A61096
Certificate 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 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 ...
```

Symptom QCCR1A100576
Some title descriptions are hardcoded

Overviews like “Orphaned Nodes” or “Unassigned Nodes” have no complete translation.

Solution

None.

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
   ```

Local Language Support

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`
- Solaris 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 9.11 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 7 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 8 Localized Documentation for HPOM 9.10

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[a]	✔	✔			
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	✔				

[a] The *HPOM 9.11 Software Release Notes* document is not localized.

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

https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=

Documentation Updates

Since the last release for the HP Operations management server and the Java GUI (that is, version 9.11.110), only the *HPOM Server Configuration Variables* document has been updated.

The *HPOM Server Configuration Variables* document is enhanced to exclude the `nodeinfo`, `opcsvinfo`, `opcinfo`, and `OVO7` references.

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.
LOCATION	*HPOM Administration UI Help*
ERROR	The information about the proper archive name format is missing.
CORRECTION	The following text should be added: The Administration UI configuration upload works only if the name of an archive starts with `opccfg_`. You cannot use the Administration UI menu to upload the configuration with an archive name different from `opccfg_XXXXXXX`.

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.

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.