HP Operations Manager for UNIX 9.10

for the UNIX operating system

Administration UI

Software Version: 9.1.0

User Guide

Legal Notices

Administration UI includes software developped by various open-source projects and organizations as listed below. The corresponding files and components are copyright to the corresponding organization or vendor and all rights reserved. The software files and components distributed under the open-source licenses are distribted on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the license of the corresponding project for specific rights and limitations under the license. Depending on the license, any product derived from the products may not be called with the name of the project nor may the name of the project appear in their name, without prior written permission. For written permission, please contact the corresponding project owner by visiting the corresponding project home page as listed below.

We greatly appreciate the work of those projects and try to contribute as much as possible to some of those projects in order to compensate their contributions.

This product includes software developed by the Acegi System for Spring Project (http://acegisecurity.org/)

This product includes software developed by the ActiveMQ project

(http://activemq.org/)

This product includes software developed by the Ant-Contrib project

(http://sourceforge.net/projects/ant-contrib)

This product includes software developed by the Antlr project

(http://www.antlr2.org)

This product includes software developed by the Apache Software Foundation

(http://www.apache.org/). These are "Ant", "Batik","BCEL", "Cocoon", "Commons", "Derby", "Excalibur", "FOP", "Forrest", " FTPServer", "Jasper", "Log4j", "Lucene", "ORO", "POI", "Solr", "Tuscany", "Velocity", "Xalan", "Xerces" and "XML RPC", "XML Security".

This product includes software developed by the Baekmuk project (http://kldp.net/projects/baekmuk/)

This product includes software developed by the BSF project (http://jakarta.apache.org/bsf/)

This product includes software developed by the dnsjava project (http://www.dnsjava.org/)

This product includes software developed by the Docbook project (http://www.docbook.org/)

This product includes software developed by the dom4j project (http://dom4j.org/)

This product includes software developed by the Drools project (http://drools.codehaus.org/)

This product also includes software developed by the dsmltools project (http://www.dsmltools.org/)

This product also includes software developed by the EditArea project (http://www.cdolivet.com/editarea/)

This product also includes software developed by the Exist project (http://www.exist-db.org/)

This product also includes software developed by the Fins project (http://cocoondev.org/main/117-cd/29-cd.html)

This product also includes software developed by the Fireflysung project (http://www.study-area.org/apt/firefly-font/)

This product also includes software developed by the Groovy project (http://groovy.codehaus.org/)

This product also includes software developed by the GWT project (http://code.google.com/webtoolkit/)

This product also includes software developed by the ICU4C project (http://www.ibm.com/software/globalization/icu/)

This product also includes software developed by the ICU4J project (http://www.ibm.com/software/globalization/icu/)

This product also includes software developed by the j2ssh project (http://sourceforge.net/projects/sshtools/)

This product also includes software developed by the Janino project (http://www.janino.net/)

This product also includes software developed by the Jasper project (http://tomcat.apache.org/)

This product also includes software developed by the Jaxen project

(http://jaxen.org/)

This product also includes software developed by the Jaxup project
(http://klomp.org/jaxup/)

This product also includes software developed by the JDOM project
(http://www.jdom.org/)

This product also includes software developed by the Jencks project
(http://jencks.org/)

This product also includes software developed by the Jetty project
(http://jetty.mortbay.org/jetty/)

This product also includes software developed by the JFreeChart project
(http://www.jfree.org/jfreechart/)

This product also includes software developed by the JPam project
(http://jpam.sourceforge.net/)

This product also includes software developed by the mimeutil project
(http://sourceforge.net/projects/mime-util/)

This product also includes software developed by the jRegistryKey project
(http://sourceforge.net/projects/jregistrykey/)

This product also includes software developed by the Jsch project
(http://www.jcraft.com/jsch/)

This product also includes software developed by the Jsdifflib project
(http://snowtide.com/jsdifflib)

This product also includes software developed by the Jython project
(http://www.jython.org)

This product also includes software developed by the MX4J project
(http://mx4j.sourceforge.net)

This product also includes software developed by the Netbeans CVS project
(http://javacvs.netbeans.org/library)

This product also includes software developed by the openadaptor project
(http://www.openadaptor.org)

This product also includes software developed by the Oracle JDBC project
(http://www.oracle.com)

This product also includes software developed by the Prefuse project
(http://prefuse.org)

This product also includes software developed by the Quartz project
(http://www.opensymphony.com/quartz)

This product also includes software developed by the Rhino project
(http://www.mozilla.org/rhino)

IV

This product also includes software developed by the Sazanami project (http://sourceforge.jp/projects/efont)

This product also includes software developed by the ServiceMix project (http://www.servicemix.org)

This product also includes software developed by the ServingXml project (http://servingxml.sourceforge.net)

This product also includes software developed by the Spring project (http://www.springframework.org)

This product also includes software developed by the StaX project (https://sjsxp.dev.java.net)

This product also includes software developed by the TM4J project (http://www.tm4j.org)

This product also includes software developed by the util.concurrent project (http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html)

This product also includes software developed by the VMTools project (http://www.vmsystems.net/vmtools)

This product also includes software developed by the Wrapper project (http://wrapper.tanukisoftware.org)

This product also includes software developed by the XBean project (http://xbean.org)

This product also includes software developed by the XIA project (http://www.jeckle.de/freeStuff/xia/)

This product also includes software developed by the XML Ant Task project (http://www.oopsconsultancy.com/software/xmltask/)

Trademark Notices

Firefox ® a registered trademark of the Mozilla Foundation.

Internet Explorer ® is a U.S. registered trademark of Microsoft Corporation.

Java™ a U.S. trademark of Sun Microsystems, Inc.

Microsoft ® a U.S. registered trademark of Microsoft Corporation.

Mozilla ® a registered trademark of the Mozilla Foundation.

Oracle ® a registered U.S. trademark of Oracle Corporation, Redwood City, California.

OSF, OSF/1, OSF/Motif, Motif, and Open Software Foundation are trademarks of the Open Software Foundation in the U.S. and other countries.

SQL*Plus ® a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX ® a registered trademark of the Open Group.

Zip and UnZip are U.S. registered trademarks of Info-ZIP.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online 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 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 web 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 a support contract. To register for an HP Passport user ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

(intentionally left blank)

Table of Contents

Conventions

Font Style	Explanation
Boldface	Words in boldface type represent programs and commands.
Capitalization	Capitalized first letters represent company or product names.
`Computer font`	Words in computer font represent file or path names, command syntax statements, prompts or messages that appear on your screen or text you should type on your workstation or terminal.
Italics	Words in italics represent variables in syntax statements or words that are emphasized in the text.
{ }	Represents required elements in a syntax statement. When several elements are separated by the | symbol you must select one of the elements.
[ ]	Represents optional elements in a syntax statement.

In all examples the default installation path of Administration UI

on HP-UX, Sun Solaris, Linux is displayed. It is

```
# /opt/OV/OMU/adminUI/
```

(intentionally left blank)

1   Intended Audience

Overview

Your company's business success relies on high-quality IT services and IT infrastructure agility. To keep your IT services available and well performing, you need a proven operations management solution that gives you control over your ever-changing IT infrastructure. That solution is HP Operations Manager on UNIX (OMU), SOLARIS (OMS) or LINUX (OML).

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

For a general overview about OMU, OMS and OML feature set, refer to the HP Operations Manager Concepts Guide, which is available in PDF format on the HP product manual website (see below).

About this Document

This User Guide provides instructions on the usage of the Administration UI software.

For more information on configuration, maintenance or troubleshooting, please see the main "Administration & Configuration Guide".

For questions regarding the installation process, please consult the separate "Installation Guide".

This manual applies both to Administration UI for OMU, OMS and OML and any reference throughout this manual to HPOM includes all three versions. System specific specialities are highlighted accordingly.

Please note, that as a result of regular program updates, some information in the printed manual may vary from that found in the online help. For the same reason, there may be slight differences in the presentation of the program's interface. Most screenshots in this manual have been taken during development and may not reflect final content.

Useful Links & Contact Information

Check the following web site periodically for the latest versions of this and other HPOM manuals:

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

Select "Operations Manager for UNIX" and version 9.0.

HPOM patches can be downloaded from the following website:

http://support.openview.hp.com/patches/patch_index.jsp

It is recommended also to check the current HPOM 8/9 SUMA (support matrix):

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

2   First Steps

Overview

This section is intended for those who use the Administration UI for the first time. It will cover the following subjects:

- Access & Access Troubleshooting: Access and Login on page 4

After that the main layout of the web interface, navigation and basic functionality will be explained:

- How Does The Interface Work? on page 6

- Menu Overview on page 8

- Navigation of HPOM Classes and Objects on page 9

Access and Login

To access the web interface of the Administration UI, please follow the steps below:

1) Open your browser and point it to the address where HPOM is installed. For HTTP the default port is 9662 and for HTTPS it is 9663.

- for unencrypted access use   `HTTP://HP-OM-Server:9662`

- for encrypted access use   `HTTPS://HP-OM-Server:9663`

In your browser you should see the user interface (Figure 1 on page 4).

2) Enter your login name and password which has been provided to you by your MIDAS Administrator.

If you access the web interface for the first time as the administrator himself, please use the following credentials:

- The initial user name is   **admin**

   and the default password is **secret**

TIP 1: Depending on the hardware and server load, the startup of the web interface can take a few seconds to 2-3 minutes.
TIP 2: Please be patient. The login screen will be displayed before the actual XML user database is ready!
If you try to login too soon, you will receive a message that the user name/password is incorrect. Simply wait a little longer and the login will be successful.

Figure 1 Login Screen

After a successful login you will be presented with the main front page of Administration UI (see Figure 2 on page 5).

Figure 2 Main front page
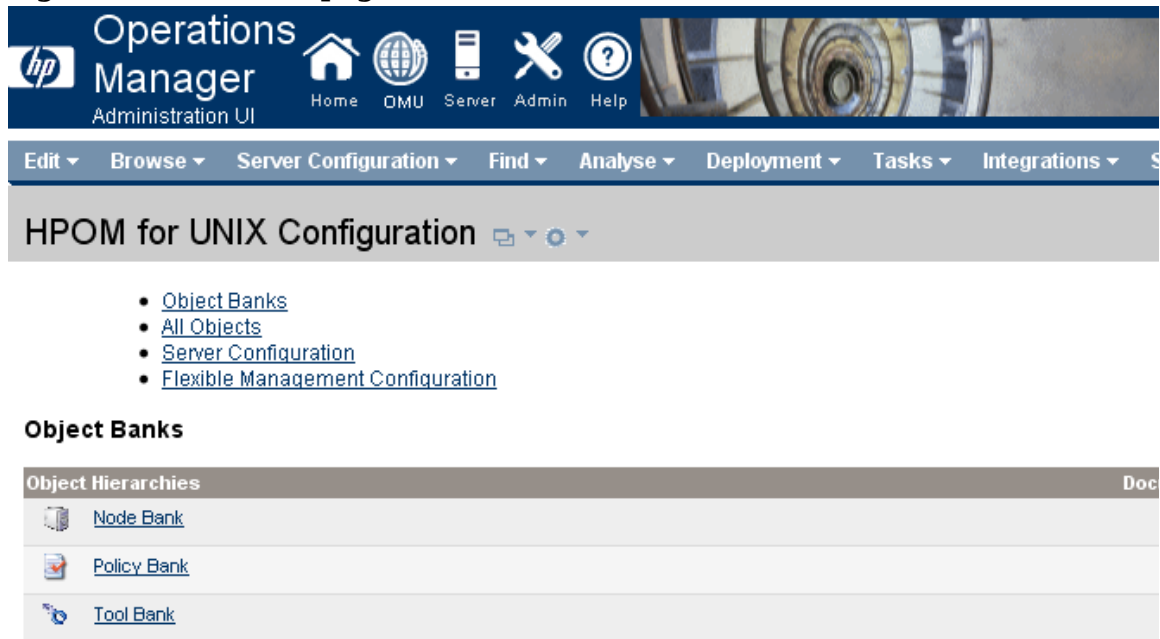
Help, I cannot login!

If the correct web interface shows up, but your login and password is rejected, that as a result you receive the following error message (Figure 3 on page 5), please try the troubleshooting tips in section Login Problems on page 117

Figure 3 Login Error

In case you are *not* presented with the main web interface in Figure 1 on page 4, but see some other error screen or some sort of directory listing, please consult the Administration UI Installation Guide chapter "Installation Troubleshooting"-> "Web Interface Problems" for further advice.

How Does The Interface Work?
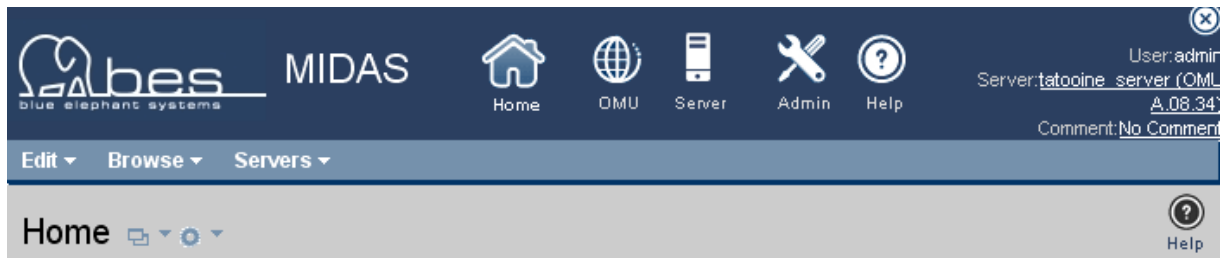
This provides an overview of and insight into IT management information by making configuration data accessible to Administrators and Application Managers. You can use it to administer your IT environment by tracking changes to configuration data and generating snapshots of the data, which you can store, publish, and re-use.

The interface works like any other modern internet website or web based application using hyperlinks and Java script (for additional functionality). Therefore, the usage should be rather straight forward in regard of operation.

Please note, that there is generally **no** "right mouse button" context menu available, as it exists e.g. in the Java GUI.

The only exception is within the responsibility matrix editor.

All (also context) menus and functions throughout the Administration UI are generally accessed using the **left** mouse button.

Nevertheless, it is possible to use the right mouse button in order to open a link in a new window or in a new browser tab. But this is the standard right mouse button menu of your web browser and not of Administration UI. Example (Figure 4 on page 7)

Figure 4 Context Menu of Web Browser
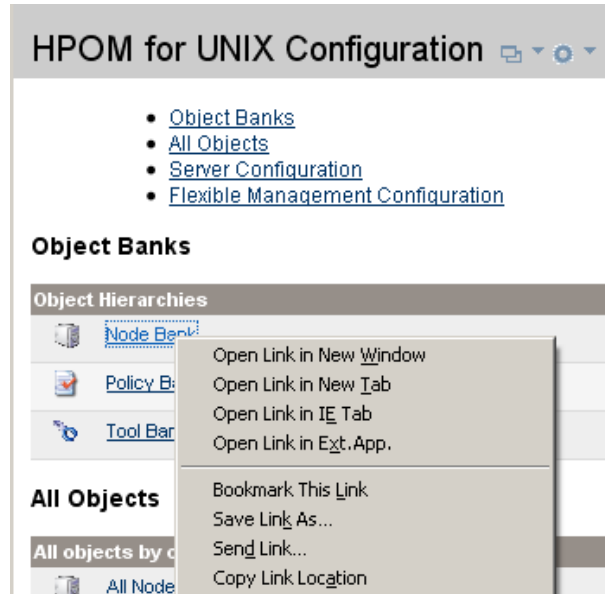
> It is recommended to use the "Open Link in New Tab" function of your web browser. Doing so you can have multiple configuration views open or continue working in one windows, while waiting for an operation to finish in another window.
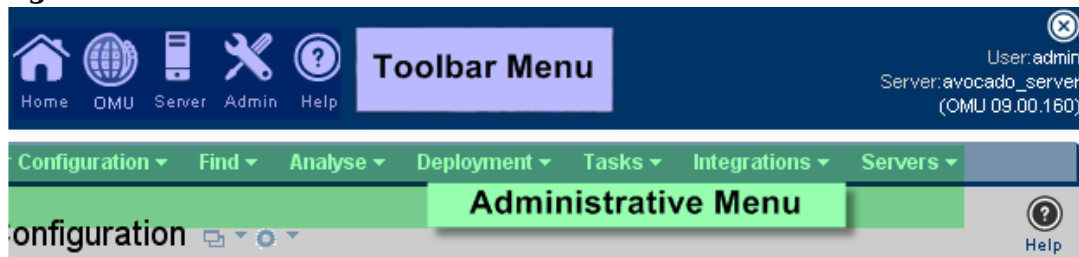
Menu Overview

Toolbar and Administrative Menu

In order to give you an overview of the interface structure the two immediately visible menus are those two on the top of your screen. These are the (see Figure 5 on page 8)

- **Toolbar Menu**, and

- **Administrative Menu**.

These two menus are always visible at the top of your screen.

Figure 5 Toolbar and Administrative Menu

The Toolbar Menu allows you switch between the main Administration UI components.

The icon you select in the Toolbar Menu defines what functions will be offered in the Administrative Menu below it:

- **Toolbar Menu** - Switch between HPOM ("OMU") and the different Administration UI components ("Home","Server", "Admin" and "Help"):

  — **Home** – returns you to the Administration UI start page

  — **OMU** – lists all HPOM objects which you can view, change assignments or perform editing tasks

  — **Server** – allows you to add new jobs, manage tasks or browse logfiles of the Administration UI server component

  — **Admin** – in this section you can manage user access into Administration UI

  — **Help** – access to the online-help system

- **Administrative Menu** - Once the main context has been defined via the Toolbar Menu the Administration Menu will list all accessible configuration objects.

By default the OMU server icon is selected and therefore the Administrative Menu lists all HPOM configuration objects ("Edit", "Browse", etc.).

On the right hand side of the Toolbar Menu (Figure 6 on page 9) you can see the following information:

- User: This is the username with which you are currently logged in.

- Server: Lists the name and version of the HPOM system you are connected to.

Figure 6Login and Server Information

Navigation of HPOM Classes and Objects

Via the Administrative Menu all HPOM objects can be accessed. From "Browse" you can select all main objects (e.g. Node Bank, Policy Bank, etc).)

Tip: Once you are inside a HPOM section (e.g. "All Policies"), it is possible to create a bookmark in your web browser, for later easy access.

Lab:

- In order to introduce you to the main navigational functions used inside any HPOM object listing, please select either the direct link "Policy Bank" on the main page or select from the Administrative Menu: "Browse" -> "Policy Bank".

This should give you a result similar to the picture below (Figure 7 on page 10). Please note, that we used a filtered result in the screenshot, in order to keep the listing small.

Figure 7   List, Browse, Action Menus

Apart from the already mentioned Toolbar and Administrative Menu more menus are available once a HPOM object class has been selected:

- **Browse Menu** - here you will be offered useful context based information, e.g. show the parent policy group, show node assignments of this policy, message catalog, node group, users responsible for a node, etc.

- **Action Menu** - as the title suggests different actions can be performed here for an object. Example: Edit, copy or delete a policy or a node; run a policy comparison.

- **List Menu** - operations can be performed at once for multiple objects.

- **Global Browse and Action Menu** - same as the context based Browse and Action Menu but on global level. Once a HPOM object is viewed, the global menu will switch to a context based Browse and Action Menu for that particular object (see below).

- **Context sensitive Help** button - it will display help information for the section or HPOM object currently being viewed.

The content of the Browse, Action and List Menus will change depending on the HPOM object class you are in.

More details on the Browse and Action Menu are available here: Browse & Action Menu on page 13

Sorting Options

In regard of the presentation of the different HPOM objects, the interface offers different filtering, listing and sorting options. These are designed to help you in finding the desired object quickly.

Generally, all objects will be presented in an alphabetical order. Depending on the HPOM object class different columns exist:

Type, Name, Label, Description, Smart Plug-in, Categories etc.

Administration UI can help you in several ways finding the required object (see Figure 8 on page 11) once you are inside a HPOM object class:

- Custom filter function (usage - see next page).

- Full listing via the "Show all" function (the listing can take a few moments!).

- Find all items starting with a particular letter.

- Use the forwards or backwards icon or jump to page No. xx.

- Instead of an alphabetical listing via the Name or Label column it is also possible to select another column header (e.g. type, name, description) to define the order of the listing.

Figure 8 Sorting Options

There will be 20 results shown on each page (cannot be increased). If there are more results, the page forwards/backwards function will be available. Showing 1-20 of XXX will inform you about the total amount of matching results.

Please note, it is also possible to combine different filter methods. For example to list all policies starting with the letter "e" and then to use the "show all" function.

Custom Filter Function

With the filter function you can define filter yourself. This filter function is available for all HPOM object classes.

Lab:

In order to test this filter function please perform the following steps:

* From the Administrative Menu select "Browse" -> "All Policies"

* Click on the "Filter" field (Figure 9 on page 12)

Figure 9 Filter
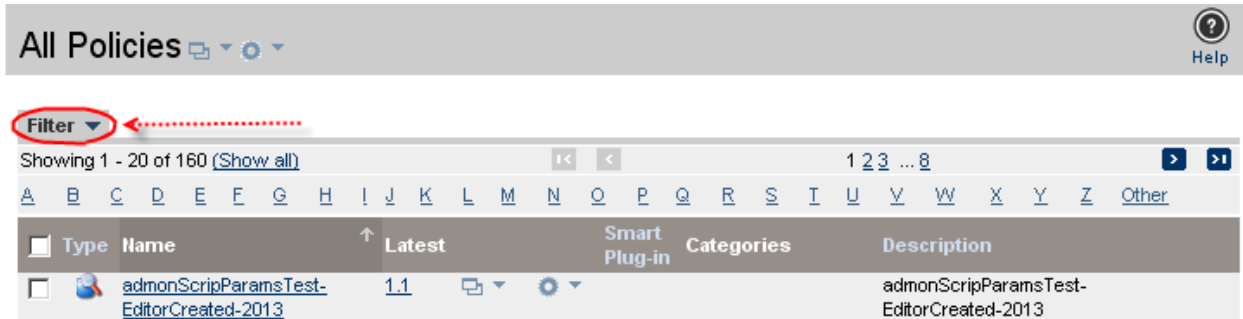
This will open the filter (see: Figure 10 on page 12)

* Simply enter "bad" in the name field and press "Apply Filter" or hit the <RETURN> key on your keyboard.

Figure 10 Filter "bad"

This should give you some result like Figure 11 on page 13 below.

The filter function also exists on a global level. It can be accessed via the Administrative Menu: "Find" -> "Locate".

The Locate function is discussed in greater detail in section:Locate on page 72

Figure 11 Filter Result "bad"

Browse & Action Menu

The Browse and Action Menu are probably the two menus which will be used most.

The Browse Menu helps the administrator to display existing relationships of an object or to perform an impact analysis. Generally it would have been difficult or impossible to perform these operations in the previous Motif GUI or using the shell.

The Action Menu helps each user to quickly perform tasks like editing, assignments or deployments.
The content of these two menus depend on the HPOM object class you are in. Both menus will be discussed exemplarily below for nodes and policies.

If one of these menus is only partially visible, especially when accessed close to the bottom of your browser (see Figure 12 on page 13), use the mouse wheel (if available) and scroll down, so it is completely visible (Figure 13 on page 13).

Figure 12 Partial Window   **Figure 13**

Browse Menu

The Browse Menu for a **policy** will give you access to the following information:

- List the parent policy group.
- List all nodes (groups) where this policy is directly assigned to.
- List all nodes on which the policy will end through direct or indirect assignments (via node group or policy group).
- List the Instrumentation directory `/var/opt/OV/share/databases/OpC/mgd_node/instrumentation/`
- List of all categories (logical classifications of policies) that exist for the policy.
- Policy type displays the policy type details.
- Smart Plug-ins list all SPIs that exist for the policy.

Figure 14 Policy Browse Menu
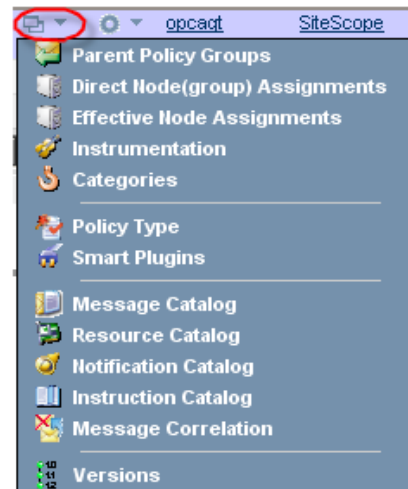
- Message Catalog shows all messages created by the match conditions of a policy or policy group.
- Resource Catalog shows all logfiles and monitor programs or scripts of a policy or policy group.
- Notification Catalog shows a list of template conditions that are forwarded to notification interfaces or trouble ticket systems for a policy or policy group.
- Instruction Catalog displays a list of instruction texts for all conditions of a policy or policy group.
- The Message Correlation page displays a list of the messages correlated on the selected node; the information displayed includes the name of the policy that generated the message, the condition triggered, the message key, and the resulting correlation. The list shows all correlations between policy conditions based on the message key and message-key relation attributes for a policy or policy group.
- Versions lists all versions of the policy in the version control system.

The Browse Menu for a **node** will offer the following menus:

Figure 15 Node Browse Menu

- List all direct policy (group) assignments for this node.

- List all direct and indirect assignments to a node, thus listing all policies which will end on this node.

- List the assigned sub-agents.

- List all node groups the node is in.

- List node defaults (e.g. machine type, heartbeat polling status & interval...).

- List layout groups for the node.

- Users lists the users configured to work on this node.

- Profiles lists the according user profiles.

- Categories lists the logical classifications that exist for that particular node.

- Instrumentation lists the directory `/var/opt/OV/share/databases/OpC/mgd_node/instrumentation/`

- The Flexible Management Configuration menu option opens a page which displays a summary of the active flexible-management configuration for the HPOM environment.

- Message, Resource, Notification, Instruction Catalog and Message Correlation (see above).

Action Menu

The Action Menu for a **policy** enables the user to perform the following operations:

- View lists the policy and conditions in a graphical refined way.

- Raw View of the policy.

- Edit will open the policy editor (there is a separate section on it).

- Edit Raw Mode is available through an inbuild editor that supports simple syntax highlighting.

- Assign operations can be executed to policy groups or nodes (groups).

- Copy will open an exact copy of the selected policy in the policy editor.

- Assign Categories can be used to define a logical classification for this policy or a node.

Figure 16 Policy Action Menu
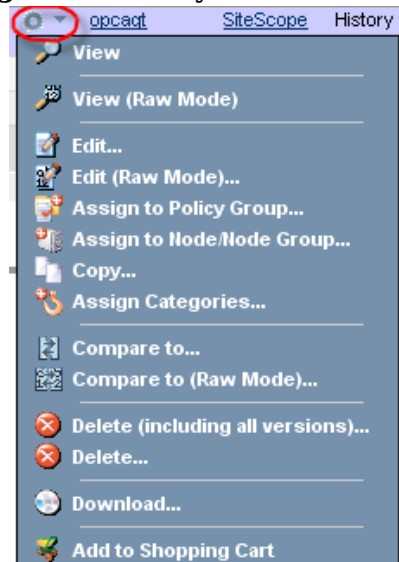
- Compare enables the user to compare this policy against another one. (explained in detail in another section below).

- Delete (including all versions) will remove the policy altogether, also from the version control system.

- Delete removes this version of the policy, leaving other versions and those inside the version control system intact.

- Download will download the policy to the Administration UI clipboard, from where it can be processed further (details can be found in a section below).

- Shopping Cart is a virtual "shopping" basket which can be used to store temporarily items which can be then e.g. downloaded altogether in a second step.

-

Global Action Menu

The global Action Menu inside an object class can be used for a complete download of this class (Figure 17 on page 17). The global Browse Menu is currently not used.

Figure 17 Global Action Menu
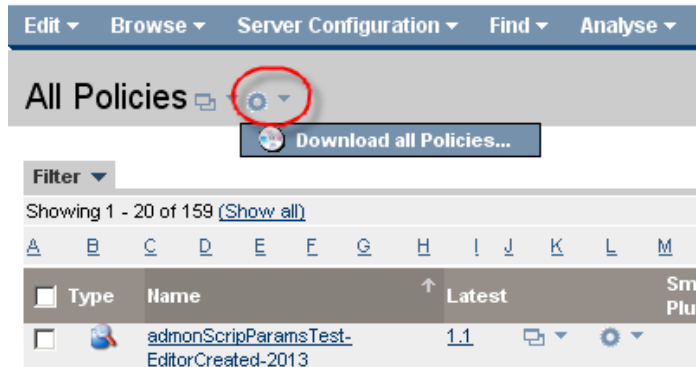
Global Browse and Action Menu in the View Operation

Once a HPOM object is viewed the Global Browse and Action Menu will change its function and become a context based Browse and Action Menu.

Lab: In order to test this please perform the following steps:

• From the Administrative Menu select "Browse" -> "All Nodes"

• In order to view a node (or policy, policy group, tool, etc.) you can either click on the name of the system. Example "avocado" or "avocado.bes-intern.com".
Or you can select from the Action Menu: "View" (see Figure 18 on page 17)

Figure 18 View

Inside the View (data will be displayed in read-only mode), the global Browse and Action Menu will now offer all context typical browse and action functions, see Figure 19 on page 18.

Figure 19 Global Browse and Action Menu in the View Operation
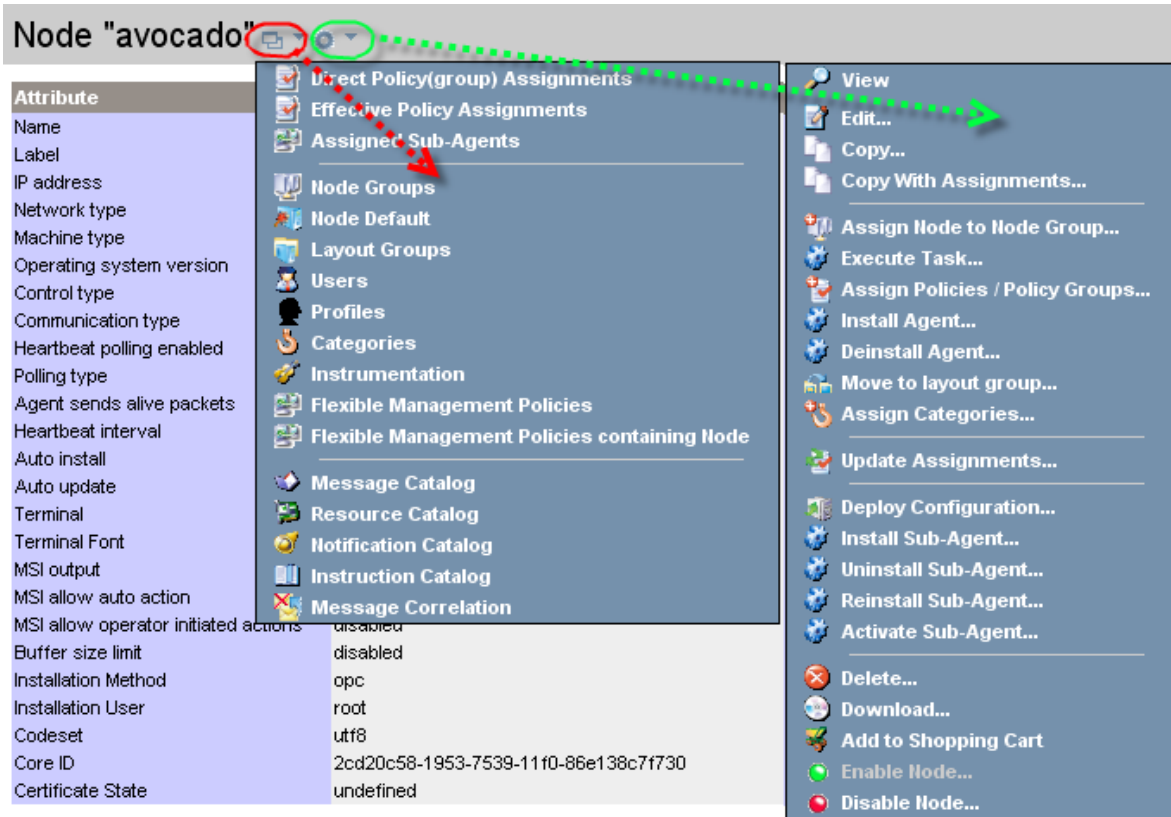
✏️ Please note, that there is a dedicated Chapter 6, Access to all Areas which discusses how to reach all available functions, which are available in the Administration UI web interface.

3 Editors & Selectors

This chapter will show how objects (e.g. policies) can be edited using the different editors and how to use selectors to select nodes, policies, etc.

Moreover, the existing locking mechanism inside the Administration UI application will be explained. It warns users and stops them editing objects which are currently edited by another user.

The individual sections are:

- Editors - Introduction on page 20

- Selectors on page 35

Editors - Introduction

There are basically two forms of editors existing in Administration UI. A fully GUI based one with enhanced functionality and a simple RAW file editor.

But before these two are covered in more detail two "workflow" tips exist, that should be observed in order to avoid confusion. After the different editor invocation methods are shown:

- How to Exit an Editor on page 20

- Renaming an Object on page 20

- Editor Invocation on page 22

How to Exit an Editor

Though no editor example was given yet, it is actually more important how an editor screen is closed than opening it.

To exit any editor please use either the SAVE or to quit the CANCEL button! Please do **not** use the "<-" back button (Go back one page) of your web browser.

Inside Administration UI a locking mechanism exists. As soon as the edit function is used a lock is created for this object. This helps to prevent other users from accidently modifying this object as well.

The locking mechanism and how to unlock objects is explained in a separate section: Locks on page 33

SAVE or CANCEL will automatically remove this lock.

Since any standard web browser can be used to access and operate Administration UI its back button functionality isn't a full integrated part of the application. Therefore, if an editor is exited using the browser's own back button, the edit process for an object will remain open, thus the lock on it as well. As a result if you or other users come back wanting to edit this object again, a warning message will be displayed, that this item is still locked.

For all details on this subject see: Locks on page 33

Renaming an Object

Before the different editors and their features are discussed, there is a another simple but important advice, which can, if it is not followed, lead to user irritation.

When you want to **RENAME** a HPOM object, it is important from where (which HPOM object listing) the edit and rename operation is initiated.

Please use the edit function from within an object class listing and NOT when viewing the object itself (in read only mode)!

The following process flow should demonstrate it, followed by an example:

Correct: HPOM object listing -> edit -> initial HPOM object listing is displayed.

Not recommended:
HPOM object listing -> view object(!) -> edit (inclusive policy/user rename) -> two messages will be displayed. Success on edit but also an ERROR message. There will be no HPOM object listing! For a screenshot of such a result, please see Figure 20 on page 21.

> The process logic behind any edit is that the user will be transferred back to the initial screen after the edit operation is completed (by SAVE or CANCEL), from where the edit operation was initiated. Generally this will be some (filtered) HPOM object class listing (e.g. policies, users).

Example: You use a policy filter, that lists all policies where "bad" is part of the name. If you select "Edit" from the Action Menu for one of these policies, change the policy and press "SAVE" or "CANCEL" you will be sent back to the previous results page with the filter "bad" still enabled.

Even with a complete rename of a policy ("bad"->"good") during the edit operation, you will be still transferred back to the previous results page listing all policies with "bad" in their name somewhere. Naturally the renamed policy "good" is no longer visible since it does not match the "bad" filter which is still enabled.

But what happens if this workflow is used:
HPOM object listing -> view object(!) -> edit (inclusive policy/user rename)

From what we said above the user will be brought back to the initial screen in which the edit operation was initiated. In this example the edit was triggered while viewing the object itself! But since the object was renamed the URL mechanism used to bring the user back to his initial listing, will **fail** to list the HPOM object under its **old** name, see Figure 20 on page 21.

Figure 20
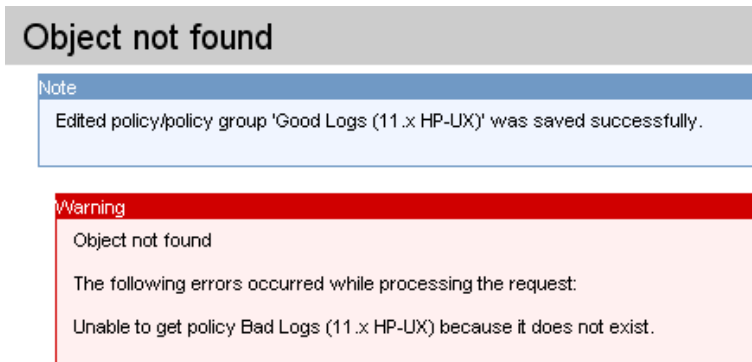
For rename operations it is therefore recommended, to trigger these from a common object listing, and not from within a view of that object.

Again to make it very clear, there is no technical problem with the rename operation itself. If the not recommended process is used as explained above, the previous object view listing will simply fail, which might be irritating for the end user.

Editor Invocation

Once you have located the HPOM object you want to edit, through one of the filtering or sorting techniques (explained here Custom Filter Function on page 12) or through the locate function (which is explained in Locate on page 72, two options exist.

- For the listed object select "Edit" from the Action Menu.

- While viewing the object select "Edit" from the Global Action Menu.
  This is NOT recommended for rename operations as already explained.

- New, not existing objects can be added via the Administrative Menu: "Edit" -> "Add Node", "Add Policy", "Add Policy Group", etc.

- Or once you are inside a particular object class, e.g. a node or policy group, it is possible to use the List Menu: "Add Policy", "Add Policy Group" etc.
  The advantage here is that the hierarchical context you are in, will be taken into account. Therefore, if a policy is added in such a way it will be added within this policy group.

# GUI Based Editors

Introduction

With Administration UI HPOM objects can be added and modified inside your standard web browser. This section will introduce you to all editor basics.

The policy editor will also be shown in detail since it offers some unique features (e.g. condition copy across policies).

Previous Motif Gui users will find the same fields in all editor screens. Administration UI is using tabs for the different areas, see Figure 21 on page 22.

- Fields which are compulsory are marked with a blue *.

- Field based help information is available via the ? icon

Figure 21 Edit Tabs
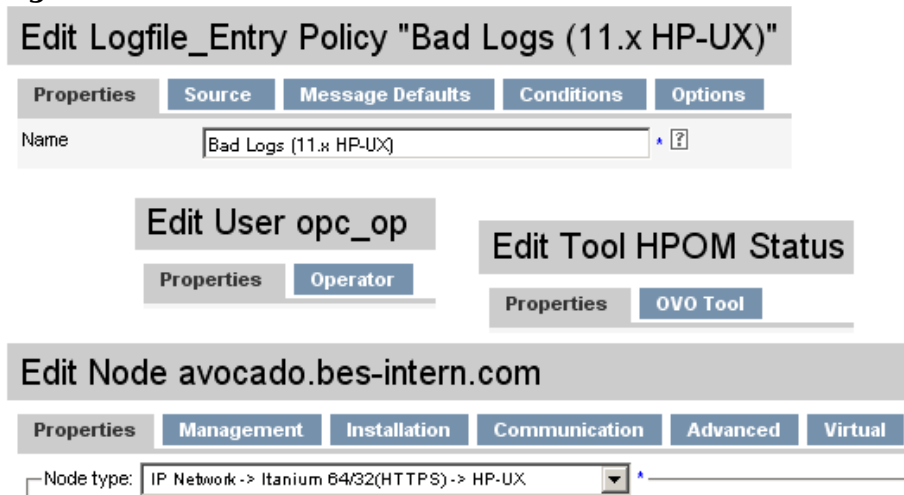
At the bottom of each editor screen you will find a SAVE, CANCEL and RESTORE button, see Figure 22 on page 23:

- SAVE will save all modifications (a syntax check is performed also) to HPOM.

- CANCEL - quit the editor without saving.

- RESTORE will reset any modified fields to their original state when the editor was opened for that object.

Figure 22
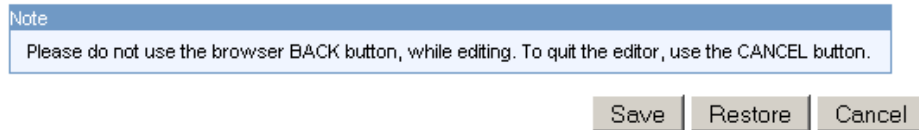
Field and Syntax Checks

With each SAVE there will be a syntax check performed, if all compulsory fields are correctly filled and if there is there is a syntax somewhere. If such a problem is found, there will be a red ! mark on the tab containing the empty or incorrect field entry. A warning message will also be displayed why this operation was not successful, see Figure 23 on page 23:

Figure 23 Syntax Check Warning
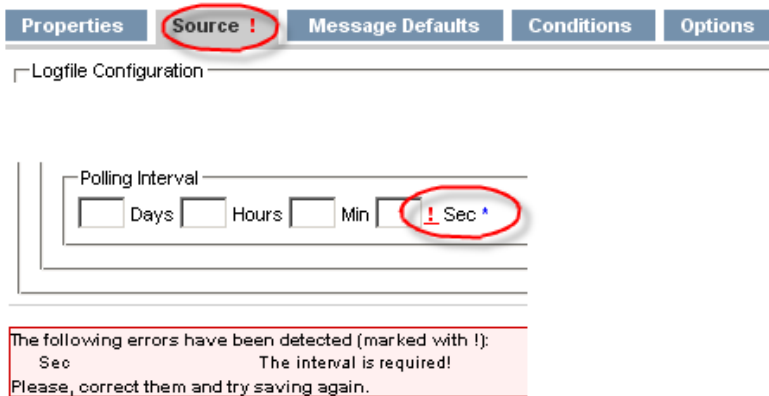
Policy Editor

The GUI based policy editor offers some enhanced functions, that include copy & paste operations for conditions or a filtering function to quickly locate a condition in a bigger policy.

In order to run through all major functions, please follow the lab instructions below.

Lab:

• From the Administrative Menu select: "Browse" -> "All Policies".

• Select for any of these "Edit" from its Action Menu.

The content of the policy will be listed under different tabs (example Figure 24 on page 24):

— **Properties** contains the name and description. Also the version handling can be defined here.

— **Source** contains, for example the monitor, logfile location, polling interval, etc. This tab is only available if a policy has such a source.

— **Message Defaults** lists all message attributes fields; sub-tabs exist in this section for Instructions, Correlation.

— **Conditions** enables the user to edit, add, move or copy conditions. It also enables the user to test patterns.

— **Options** local logging & unmatched messages

The contents should be self-explanatory under each tab. For conditions there are some special features available. You can reorder conditions, duplicate a condition with the copy function and even copy condition(s) from policy A to policy B (more on that later).

• Please select the tab "Conditions" to view its contents.
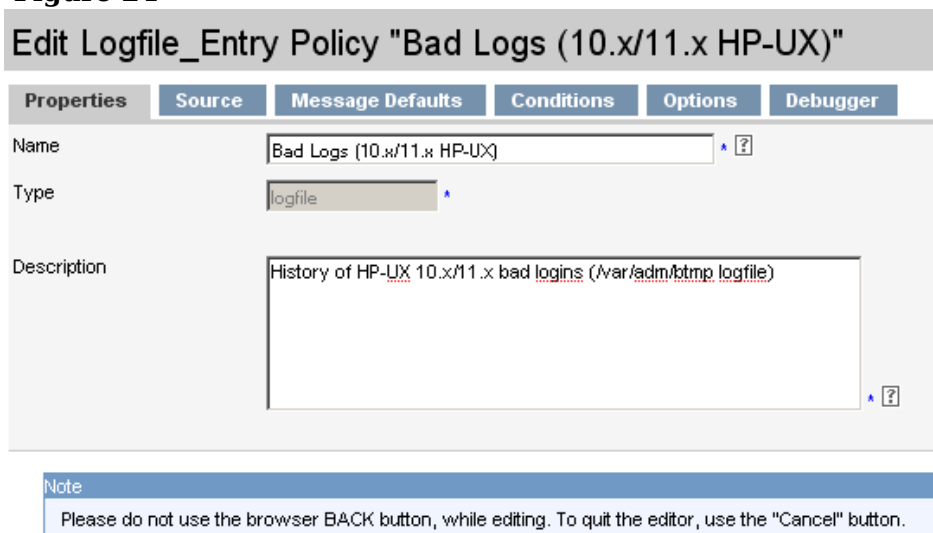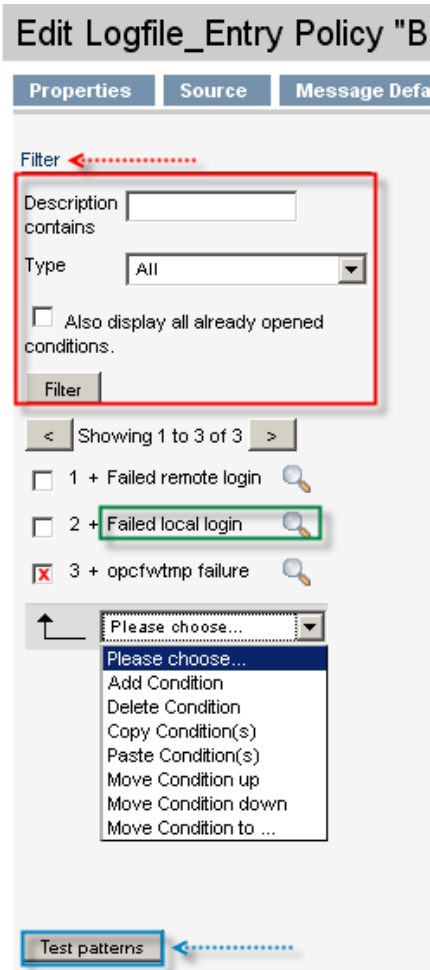
Figure 24

Figure 25 Edit Conditions

On the top there is a Filter function available. Once selected the filter box opens (marked in red).

On the left hand side all the conditions are listed No. 1-x. They are listed in blocks of 50. If there are more than 50 conditions, please use the "<" and ">" to list the next block.

The condition contents is not listed by default. Each contents is only listed (and fetched from HPOM) once you click on the magnifying glass or the condition name itself. (marked green)

Via the checkboxes and using the available commands from the drop down menu it is possible to add, delete, copy, move conditions.

At the bottom it is possible to test the conditions patterns via the "Test patterns" button (marked blue).

In order to list more than 50 conditions at once, please perform these two steps:

• Access the filter function, without entering anything in the description field.

• Press the "Filter" button.

Once a condition is selected, the conditions contents is listed on the right hand side of the screen, see Figure 26 on page 26.

Each condition will have its own condition number in the upper left hand corner.

Inside the condition you will also find several tabs to access the various configuration areas.

Figure 26 List Condition
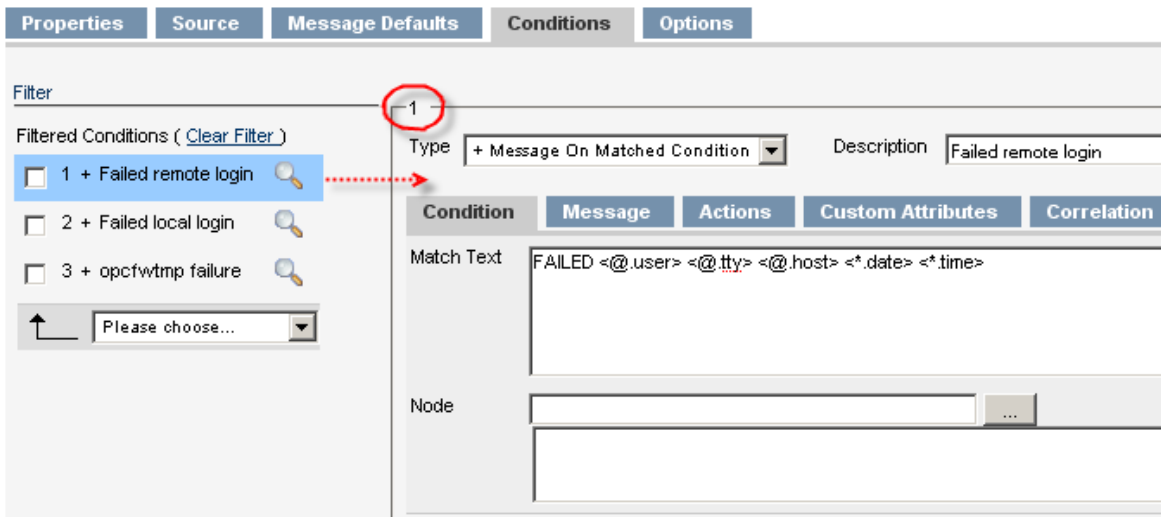
Add, Copy & Move Conditions

• In order to add a new condition simply select "Add Condition" from the drop down menu. A completely empty condition will be opened.

• If an existing condition should be deleted, enable its checkbox and select "Delete Condition" from the drop down menu.

• Sometimes it can be very helpful to simply copy and re-work an already existing condition instead of creating it from scratch.

  In order to do so, please enable the checkbox of one condition you want to create a copy from and select from the drop down menu "Copy Condition(s)". This will add the condition to the very end of the condition list. Example: If condition 1 is copied and there are 251 conditions, the newly copied condition will become 252. .

Multiple conditions can be copied & pasted. Also they can be copied from one policy into another one, see the next page.

• To move a condition one slot up or down use the appropriate command.

  Generally it is recommended to use the "Move Condition to" function instead of manually performing this over and over again. When "Move Condition to" is used a pop up window will appear in which the target condition ID can be entered.

Chapter 3: Editors & Selectors

Copy Condition(s) Across Policies

The process to copy one or more conditions from one policy to another one is actually very simple.

- Use the edit command on the source policy.
- Tick all checkbox(es) of the condition(s) you want to copy.
- Select from the drop down menu: "Copy Condition(s)".
- Quit the source policy via the CANCEL button.
- Use the edit command on the target policy.
- Inside the conditions tab select from the drop down menu: "Paste Condition(s)" This will add the condition to the very end of the condition list.

Pattern Testing

The pattern testing window enables you test pattern-matching rules used in HPOM Administration UI log file policies which are used to monitor application log files.

Please note, that pattern testing is **only** available with **HPOM 8.29** and above.

The pattern testing window allows you to test the strings before a policy is actually distributed to any managed node.

Adding pattern matching to conditions enables you to target much more accurately the really important log file entries which will be monitored.

When editing a policy you can find inside the tab "Conditions" the button "Test patterns"(see Figure 27 on page 28)

Please allow pop up windows for the Administration UI server to be opened! Otherwise the pattern testing window cannot be displayed.

Generally it is possible to test just one condition, several or all. Simply tick (enable) all those checkboxes of those conditions you want to test.

If no checkbox is selected ALL conditions will be tested.

Please note, that once the pattern testing window is open, it is NOT possible to go back into the policy editor. Only after clicking OK or CANCEL inside the pattern testing window you will be brought back into the main policy editor window.

In case the pattern testing window does not open correctly, there is an "Enable editor" button in the middle of the locked editor window, which will unlock the editor.

Figure 27 Test Patterns
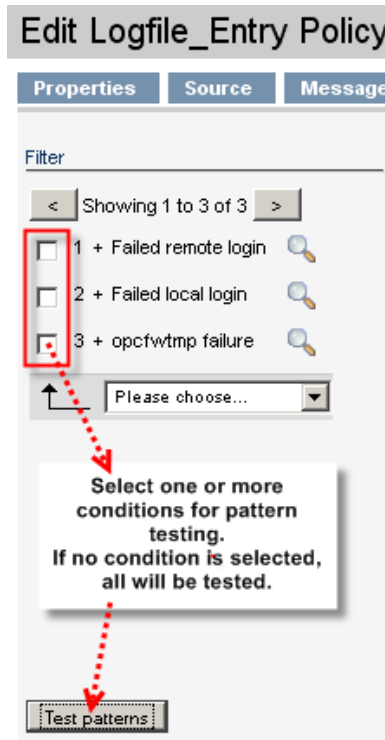
Once the pattern testing window is open, you can see all previously selected conditions or all conditions (Figure 28 on page 29).

- RESET - Load the original conditions from the policy. Useful if you have made changes to the patterns in the conditions and want to revert back to the original state of the policy.

- VALIDATE - Test the new or modified patterns for syntax errors. Indicates condition and character which caused the error. More detailed information is available in a tool-tip, which is displayed when you hover the mouse over the condition with the indicated error.

- TEST - Run a test of the patterns on the data in the Test Data text area. If a file has been uploaded in order to test its contents (see below), please notice, that the test is performed only on that part of the file that is visible in the Test Data text area. It is by default 20 lines, but can be extended to 50 lines or a maximum of 100 lines.
  Testing a line stops as soon as the test mechanism finds a match condition. The test results are shown under the tab "Result Table".

  It is possible to make changes to the test data in the textarea in order to test what-if cases. But please ensure, that not too much or too little matches. You can make changes to the file to test what-if cases (to ensure that not too much or too little matches). However, the changes you make to the data in the textarea, are lost as soon as you page away from the changed lines or you shut the editor.

- It is also possible to use test data from a logfile from your own local workstation (it must be in a text format!). To do so select from the drop down menu "Upload file from local Computer". A pop up box will open through which you can select the file. Please note, the maximum file size for uploads is 10mb.

Figure 28 Pattern Testing Window
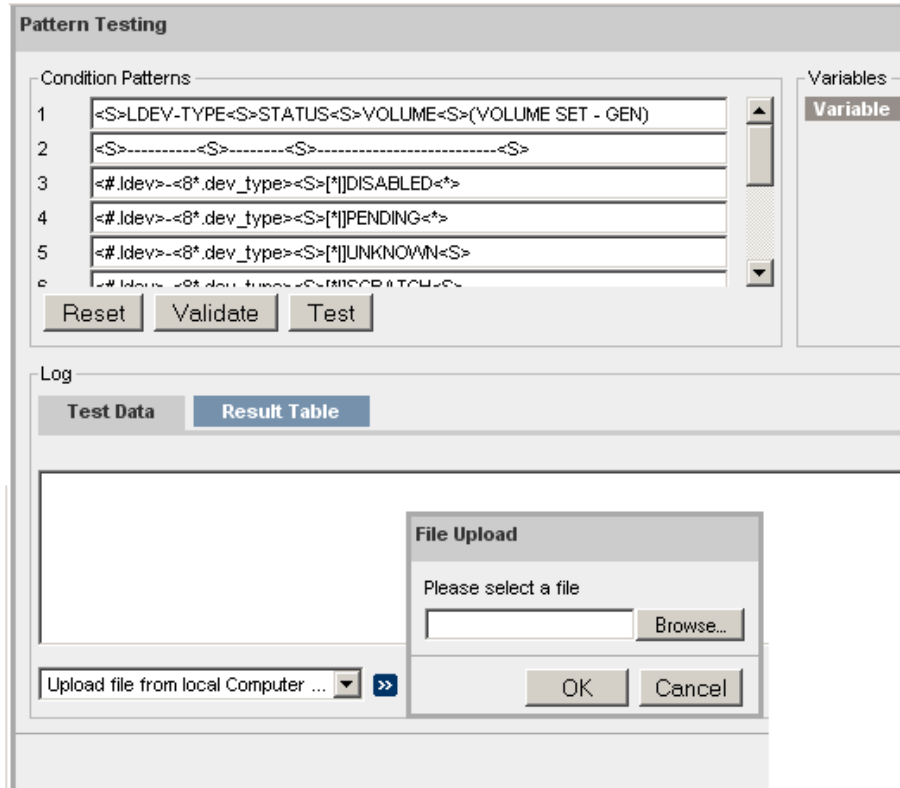
Result Table (see Figure 29 on page 30)

Shows the results of the pattern-matching tests by indicating which text lines matched (or didn't match) the patterns specified in the rules you are defining.

The results show the line where the match occurred, the content that matched, and the condition that triggered the match.

If you uploaded a file you can use the [<] and [>] buttons to move through the file. Depending on your selection 20, 50 or 100 lines are shown.

Please use the [|<] and [>|] buttons in order to jump to the beginning or the end of the file.

Select a line in the result table (it will be highlighted in blue) to display the variables (if any) that matched in the selected line and the value of the variable that matched. You can use the information displayed in the result table to fine tune the condition to more accurately match the log-file entries.

If there is no match at all this will be indicated by a "-".

Figure 29 Test Patterns

If you change a pattern, this pattern will be highlighted in blue in the pattern listing.

Figure 30 Test Patterns

In order to copy this pattern back into the policy, you have to click on OK. When inside the policy editor again, it is necessary to press SAVE next to save all changes in the HPOM database.

If CANCEL is used, all pattern changes will not be copied to the policy conditions and therefore will be lost.

- Please leave the pattern test window by pressing "CANCEL".

- Please leave the editor by pressing "CANCEL".

Raw Editors

Raw Editors are available for policies and files/scripts. They offer some basic syntax highlighting.
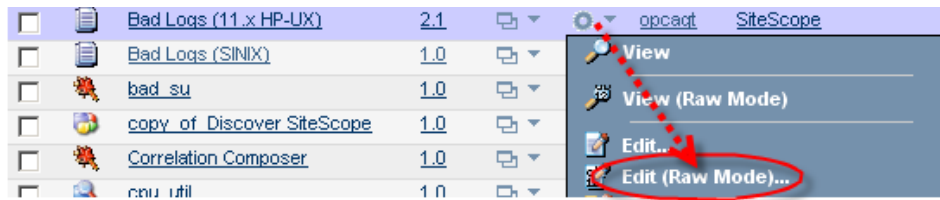
On the basis of the policy raw editor this will be demonstrated next.

Lab:

In order to test this feature please perform the following steps:

- From the Administrative Menu: select "Browse" -> "All Policies"

- For any policy (in the example below we use "Bad Logs (11.x HP-UX)" select from its Action Menu: "Edit (Raw Mode)", see Figure 31 on page 31

Figure 31 Action Edit Raw Mode

This will open the raw editor. Two tabs exist: "Properties" and "Content".

For a policy the raw editor is GUI based for the properties part, see Figure 32 on page 31.

Figure 32 Policy Raw Edit - Properties
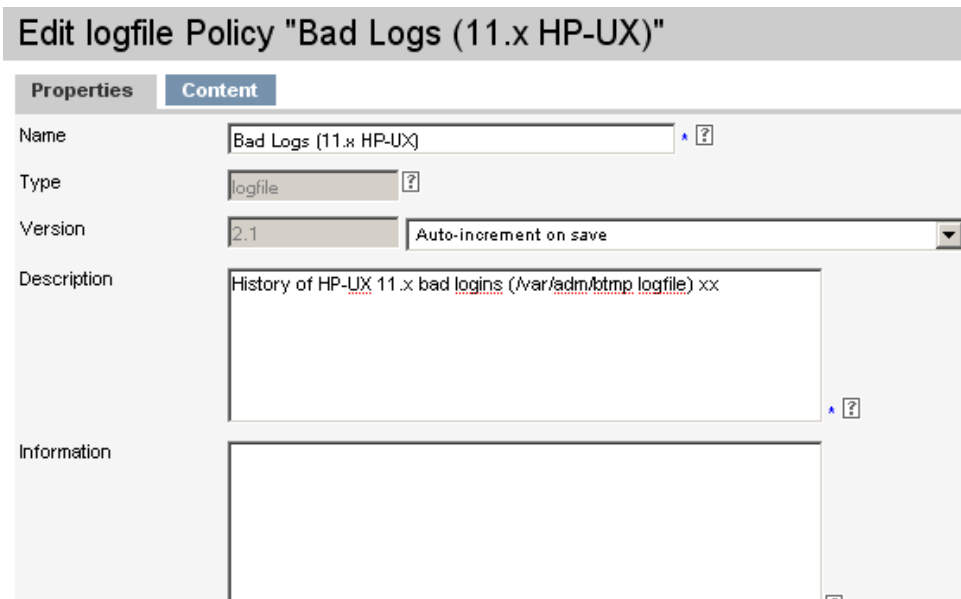
The content itself will be displayed in the raw format. It is possible to enable, disable or reset the syntax highlighting.

From the syntax selector another syntax can be defined. By default HPOM is selected.

A search function and go to line function is also offered. See Figure 33 on page 32.

Figure 33 Policy Raw Edit - Content

- Please leave the editor by pressing "CANCEL".

Locks
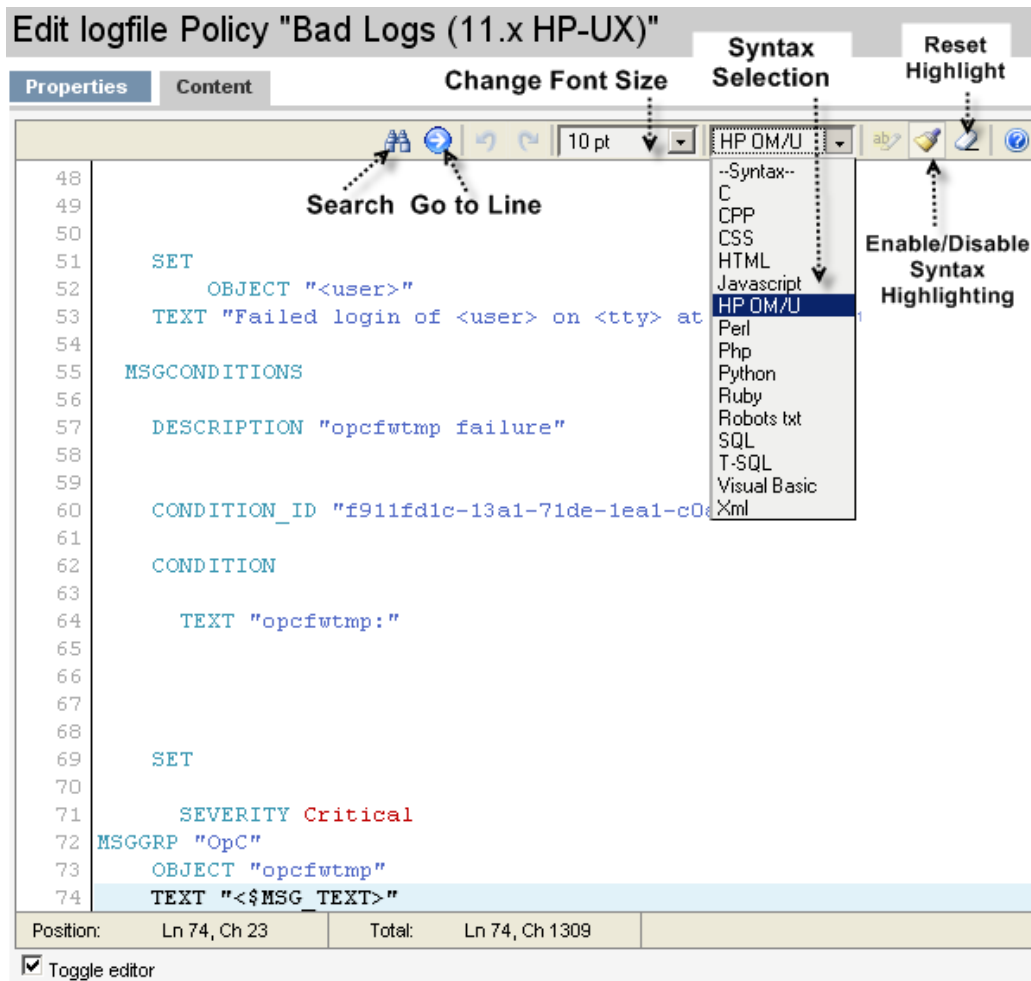
This section will explain the locking mechanism behind Administration UI. As soon as a user uses the "Edit" function on any HPOM object, Administration UI will create a lock on this item. These locks are stored in Administration UI. If another user tries to edit this item as well, he will be presented with a warning message and is asked what he wants to do next, see Figure 34 on page 33.

This warning message also shows the name of the other user currently accessing this object. In Figure 34 on page 33 the HPOM object has already been opened by the same user.

Most of the time the lock is existing because a user left the edit window by closing it or using the back button of the web browser, instead of using the "CANCEL" or the "SAVE" button.

There are two similar warning window offering up to three possibilities:

- **Open editor in read-only mode**. No changes can be done nor saved!
- **Open the editor in full edit mode.** This simply boils down to this: The last user pressing the save button will win. The modifications of the other user(s) will be lost.
- **Cancel the whole operation.**

When editing and saving might cause the others users configuration to be overwritten another warning message will be displayed whether this operation should be performed or not.

Figure 34 Lock Warning
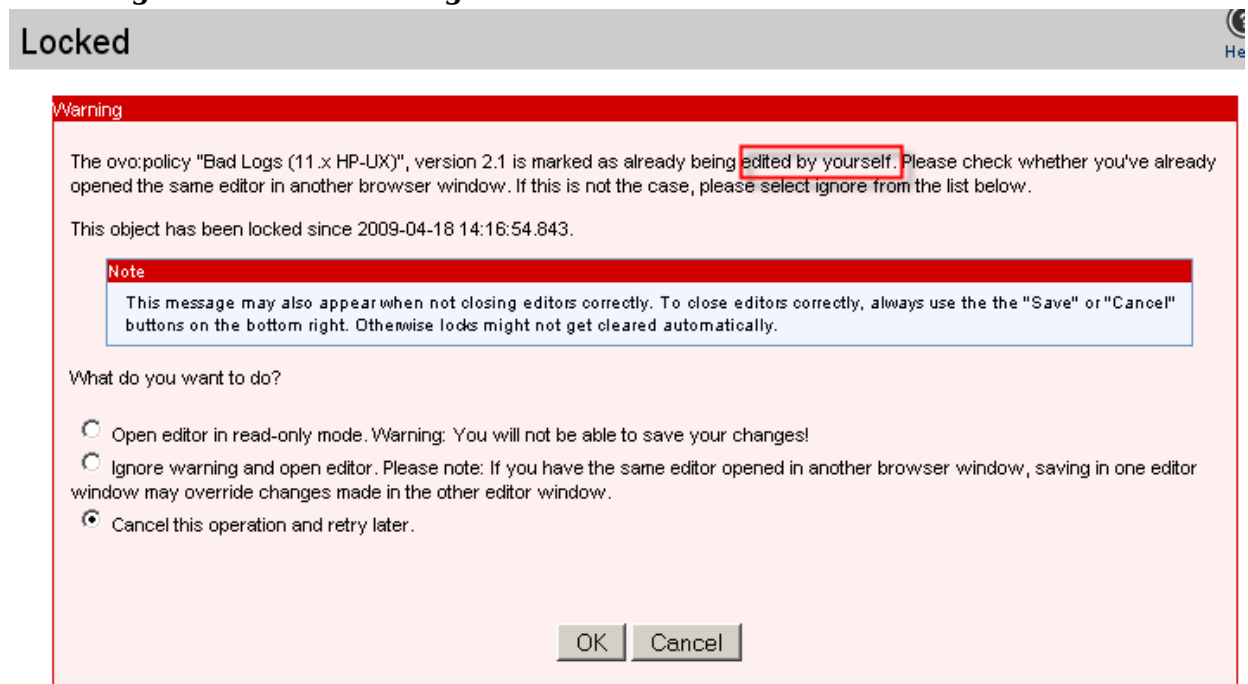
Lock Removal

It is also possible to remove some or all locks. This can be useful, e.g. Monday morning when you can be sure no one has logged in yet.

In order to remove those lock files manually please run through these steps:

- Select the "Admin" icon from the Toolbar Menu
- From the Administrative Menu: "Browse" -> "List Locks"

This should display you all locks similar to the screenshot below (Figure 35 on page 34).

- Enable all checkbox(es) of those locks you want to remove.
- Afterwards select from the List Menu: "Delete Lock"

TIP: When you want to remove all locks simply press the top checkbox (next to name) this will enable all other checkboxes.

Figure 35 Lock Removal

Selectors

Selectors are used in different forms throughout Administration UI for assignment operations or to fill in a required field in an editor.

A good example to demonstrate a selector is the selector which is used when you want to assign a policy or policy group to a node.

Lab:

In order to test this please perform the following steps:

- From the Administrative Menu select: "Browse" -> "All Nodes".

- For a node of your choice select from its Action Menu: "Assign Policies / Policy Groups", see Figure 36 on page 35.

Figure 36

This will open the selector window, see Figure 37 on page 36.

There are two types of selectors:

Figure 37 Selector

simple (only a CLOSE button) and **multiple** object selectors (with an OK and a CANCEL button).

In this example this is a multiple objects selector.

A simple mouse click will be selected (highligthed in blue). Multiple selections are possible.

Use the top menu to use an individual "Filter", or browse "Policy Bank", "All Policy Groups", or even "All Policies"(this listing can take a while).

- Since we do not want to assign anything yet, press CANCEL to close the selector window.
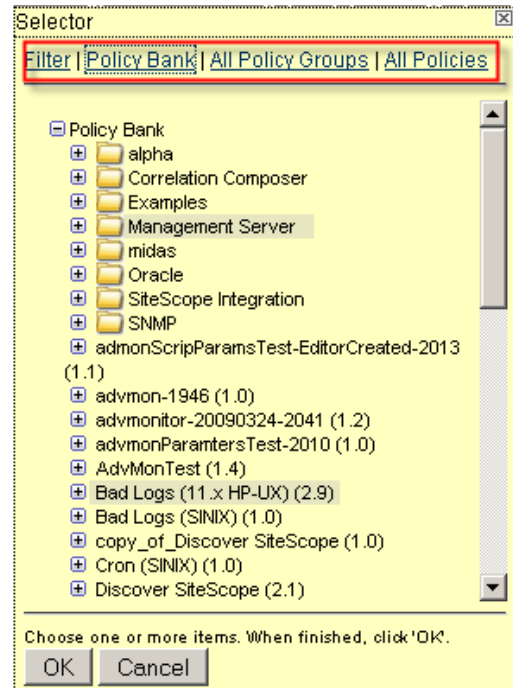
If the selector window isn't fully visible use the following TIP:

TIP: If needed you can move the yellow selector boxes. Simply hover with your mouse pointer the top section of the window (colored green) and the mouse pointer will change to a cross. While holding the left mouse button you can re-position the window according to your needs.

Figure 38

Simple Selector

In order to demonstrate also this type please run through the following Lab:

- From the Administrative Menu select: "Browse" -> "All Policies".

- For a policy of your choice select "Edit" from the Action Menu.

- Inside the policy editor select the tab " Message Defaults".
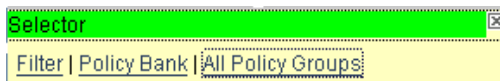
- For the field "Message Group" press the [...] browse button.
  This will open the selector.

  In this example it is a simple selector. Only single objects and be selected by a double-click. See the hint highlighted in green (Figure 39 on page 37).
  With the double-click the item will be inserted in the corresponding editor field.

- Press CLOSE to close the selector.

- Quit the policy editor by using the CANCEL button.

Figure 39 Simple Selector

(intentionally left blank)

4 Administration UI Shell Commands

This chapter discusses the most commonly used Administration UI shell commands.

For an in-debth listing of all available shell commands, please consult the Administration UI "Administration and Configuration Guide". That guide also lists advanced scripts which can be used to perform port or hostname changes inside the Administration UI configuration itself.

This chapter is split into two sections. The first one will list the most important and commonly used commands, so you can print or use this overview as a reference.

The second section will discuss these commands in greater detail and does include also examples from the screenoutput you will receive during the command execution.

Overview

Stop, Start, Restart

```
# /opt/OV/OMU/adminUI/adminui start
# /opt/OV/OMU/adminUI/adminui stop
# /opt/OV/OMU/adminUI/adminui restart
```

In case of some file corruption or login problems, a "clean" restart might help.

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

With HPOM 9 Administration UI is fully integrated in the HPOM startup. Here you can also use:

```
# ovc -start adminui
# ovc -stop adminui
# ovc -restart adminui
```

Status

Check the application status using this command. Basically it boils down to this: If you receive Build Successful, the application is up, otherwise down.

```
# /opt/OV/OMU/adminUI/adminui status
```

Version

In order to find out what version of Administration UI is installed, please use:

```
# /opt/OV/OMU/adminUI/adminui version
```

Patch Installation

Regular patches for Administration UI will be delivered as ZIP files (do not unpack them!), which have to be installed using:

```
# /opt/OV/OMU/adminUI/adminui patch /tmp/<patch.zip>
```

Analyze

When facing problems and before contacting Support use this command. The configuration will be displayed and all log files are checked for common errors. If one of these is detected a troubleshooting tip will be given.

```
# /opt/OV/OMU/adminUI/adminui analyze
```

Support.zip

In case of technical problems Support will require detailed information about the individual configuration of Administration UI. The support command helps to collect and pack all required log & configuration files.

```
# /opt/OV/OMU/adminUI/adminui support
```

Save & Reload

Different backup methods exist. See the main "Administration and Configuration Guide" for a detailed explanation. Very flexible is the following one:

```
# /opt/OV/OMU/adminUI/adminui save
```

```
# /opt/OV/OMU/adminUI/adminui reload /tmp/<save.zip>
```

Command Details

This section will give more details in regard to the commands listed in the previous section.

- Start, Stop, Restart Details on page 41

- Clean Details on page 42

- Status Details on page 43

- Version Details on page 44

- Patch Details on page 44

- Analyze Details on page 45

- Support Details on page 46

Start, Stop, Restart Details

The start, stop and restart command is tightly integrated with the HPOM 9 `ovc` command. Therefore, there two options exist to start and stop the application:

• via `/opt/OV/OMU/adminUI/adminui start|stop|restart`

• or using the `ovc` command

Via the adminui command:

The `stop` sub-command stops the complete application on the local system:

```
# /opt/OV/OMU/adminUI/adminui stop
stopping via ovc integration...
```

The `start` sub-command starts the application on the local system:

```
# /opt/OV/OMU/adminUI/adminui start
starting via ovc integration...
```

The restart sub-command will stop and restart the application:

```
# /opt/OV/OMU/adminUI/adminui restart
stopping via ovc integration...
Restarting in 30 seconds ...
starting via ovc integration...
```

IMPORTANT: The start command returns to the shell prompt immediately, however is still starting up. Depending on the speed of the local system, the start-up may take a few minutes.

Via the `ovc` command:

To start the application via ovc:

```
# ovc -start adminui
```

To stop the application via ovc:

```
# ovc -stop adminui
```

To restart the application via ovc:

```
# ovc -restart adminui
```

Also here the start command returns immediately to the shell prompt, whereas the startup itself hasn't completed yet.

TIP: To check the start-up progress, use

```
# tail -f /opt/OV/OMU/adminUI/logs/wrapper.log
# tail -f /opt/OV/OMU/adminUI/logs/servicemix.log
```

Logging starts in wrapper.log, then servicemix.log.

By rule of thumb if no more logging takes place inside the wrapper.log & servicemix.log the application startup is complete.

Clean Details

The `clean` sub-command will remove all (!) log files below `/opt/OV/OMU/adminUI/logs` and also the `/opt/OV/OMU/adminUI/work` directory. The work directory's function is similar to a cache. At application startup all service assemblies will be unpacked in this directory. Any following application startup will benefit from this. At the same time file corruption can sometimes occur inside the work directory at runtime. In case of starting problems it is recommended to first run the `analyze` followed by the `clean` sub-command.

Please note that after a `clean` the Administration UI application is **not** automatically started. This has to be done manually either by executing `./adminui start` or `./ovc -start adminui` command.

Example:

```
[root@deli:/opt/OV/OMU/adminUI/] ./adminui clean
stopping via ovc integration...
[...]
Buildfile: /opt/OV/OMU/adminUI/run.xml
clean:
intern.copy_wahttp:
BUILD SUCCESSFUL
Total time: 3 seconds
```

Combine the restart and clean command (see below).

It is possible to "combine" the sub-command `start|restart` with a "clean":

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

Here the application will be stopped, a clean will take place and the Administration UI will be started again.

But it is also possible if the Administration UI is currently not running to have a clean performed before the application startup. To achieve this the command is:

```
# /opt/OV/OMU/adminUI/adminui start -clean
```

Status Details

The sub-command `status` displays the status of the processes including connection status and whether the server assembly is correct or not.

Example (extract):

```
# ./adminui status
[...]
intern.status_service:
     [echo] sending status request to service ovconfig...
     [copy] Copying 1 file to /opt/OV/OMU/adminUI/work/20090325104339
   [reqpost] sending request to http://deli.bes-intern.com:9661/
midas_client/
[...]
     [echo] status of backend deli.bes-intern.com_server
     [echo]
     [echo]     Server:  deli.bes-intern.com_server
     [echo]     Service: auth
     [echo]       Name:        User Authentication Filter
     [echo]       Status:      connected
     [echo]       Error count: 0
     [echo]       Status:      unlicensed
     [echo]
     [echo]     Server:  deli.bes-intern.com_server
     [echo]     Service: backend
     [echo]       Name:        Local Backend Server
     [echo]       Status:      connected
     [echo]       Error count:
     [echo]       Status:      unlicensed
[...]
BUILD SUCCESSFUL
Total time: 25 seconds
```

If the application isn't correctly running a BUILD FAILED message will be received.

In addition you can use the `ovc` command :

```
# ovc -status
```

or

```
# ovc -status adminui
```

The output should look like:

```
[root@deli:/opt/OV/OMU/adminUI/] ovc -status
ovcd        OV Control                      CORE         (2004)   Running
ovbbccb     OV Communication Broker         CORE         (2005)   Running
ovconfd     OV Config and Deploy            COREXT       (2301)   Running
ovcs        OV Certificate Server           SERVER       (2009)   Running
ovtomcatB   OV Tomcat(B) Servlet Container WEB           (2497)   Running
opcactm     OMU Action Manager              SERVER,OPC   (2067)   Running
opcbbcdist  OMU BBC Config Adapter          SERVER,OPC   (2151)   Running
opccsad     OMU Cert. Server Adapter        SERVER,OPC   (2129)   Running
opcdispm    OMU Display Manager             SERVER,OPC   (2025)   Running
opcforwm    OMU Forward Manager             SERVER,OPC   (2113)   Running
opcmsgm     OMU Message Manager             SERVER,OPC   (2081)   Running
opcmsgrb    OMU Message Receiver (HTTPS) SERVER,OPC      (2053)   Running
opcsvcm     OMU Service Engine              SERVER,OPC   (2165)   Running
```

```
opcttnsm     OMU TT & Notify Manager    SERVER,OPC    (2095)    Running
ovoareqsdr   OMU Request Sender         SERVER,OPC    (2039)    Running
opcuihttps   OMU HTTPS Communication ProxySERVER,OPC (2211)    Running
opcsvcam     OMU Svc. Nav. Action Manager SERVER,OPC  (2225)    Running
opcsvcdisc   OMU Service Discovery Server SERVER,OPC  (2241)    Running
coda         OV Performance Core        COREXT        (2507)    Running
opcmsga      OVO Message Agent          AGENT,EA      (2508)    Running
opcacta      OVO Action Agent           AGENT,EA      (2509)    Running
opcmsgi      OVO Message Interceptor    AGENT,EA      (2510)    Running
adminui      OMU Administration UI Server SERVER,OPC,UI (5463) Running
```

Version Details

Via the sub-command `version` you can display the version & build.

```
# /opt/OV/OMU/adminUI/adminui version
```

Example:

```
[root@deli:/opt/OV/OMU/adminUI/] ./adminui version
[...]
[http://exist-db.org/ant:exist] Checking collection: xmldb:exist://
deli.bes-intern.com:9662/exist/xmlrpc/db/backends
version:
     [echo] installed product = HP Operations Manager for Unix
Administration UI (OMU Administration UI)
     [echo] OMU Administration UI version = 9.0.0
     [echo] OMU Administration UI build number = 288
     [echo] OMU Administration UI build date = 20090317
     [echo] OMU Administration UI install date = 3/17/09 12:07 PM
     [echo] OMU Administration UI installation directory = /opt/OV/
OMU/adminUI/
     [echo] installed OMU Administration UI products:
     [echo]   OMU Administration UI Documentor Backend
     [echo]   OMU Administration UI Configurator Backend
     [echo]   OMU Administration UI Light Web Application
BUILD SUCCESSFUL
Total time: 1 second
```

Patch Details

Use the `patch` sub-command to install future Administration UI fixpacks
(=servicepack/patches). Their format will be *.zip.

To install such a fixpack file copy the ZIP file either into the installation directory
`<AdminUI_HOME>` or any other location (e.g. `/tmp`). **Do not unzip it!** This will be done
by the patch mechanism itself. To install a fixpack execute

```
# /opt/OV/OMU/adminUI/adminui patch /tmp/<fixpack>.zip
```

or if the fixpack zip file is located inside `<AdminUI_HOME>` it is sufficient to use:

```
# /opt/OV/OMU/adminUI/adminui patch <fixpack>.zip
```

In order to offer a roll back mechanism the configuration files will be backup to a
new folder inside `/opt/OV/OMU/adminUI/<old-version>`. E.g. `/opt/OV/OMU/`
`adminUI/9.1.0`

The `unpatch` sub-command removes a previously installed fixpack. You must specify the ID of the fixpack to be de-installed as shown in the following example:

```
# /opt/OV/OMU/adminUI/adminui unpatch 9.1.0
```

The ID is defined by the directory name in which the backup files are located in.

Analyze Details

The `analyze` sub-command gives you a short overview of your system's configuration values and most common error messages in log files. Furthermore, all log files are checked for common errors. If one of these is detected a troubleshooting tip will be given. Before contacting Support it is useful to run this command first and check the result.

Example:

```
# ./adminui analyze
...
Configuration values
====================
  Installation:
    Version                     9.0.0 (build: 288)
    OEM Version                 cvpl
    Installation Directory      /opt/OV/OMU/adminUI/
    Installation Type           full
  Server:
    Hostname                    deli.bes-intern.com
    Platform                    unix
    Backend Identifier          deli.bes-intern.com_server
  Communication:
    JMX Port                    9660
    Server Port                 9661
    HTTP Port                   9662
    HTTPS Port                  9663
  XMLDB:
    XML DB User                 midas
  ORACLE:
    Oracle Home                 /opt/oracle/product/11.1.0.6
    Oracle Major Version        11
    Oracle Host                 deli.bes-intern.com
    Oracle Port                 1521
    Oracle SID                  openview
    Oracle User                 opc_op
  Operations Manager:
    Version                     900
    Codeset                     UTF-8
  Licenses:
    License Type                licensed through OMU

  Errors in Logfiles
  ==================
```

Support Details

In case of technical problems Support will require detailed information about the individual configuration of Administration UI.

With the support sub-command it is possible to quickly collect all required log & configuration files.

```
# /opt/OV/OMU/adminUI/adminui support
```

The shell output should look like this:

```
[root@deli:/opt/OV/OMU/adminUI/] ./adminui support
[...]
support.zip:
     [echo] collecting support information ...
     [echo] collecting version info ...
     [echo] collecting installed files ...
     [echo] collecting Java properties ...
[propertyfile] Creating new property file:
[...]
intern.checksum_check:
     [echo] checking checksums ...
     [echo] creating support zip ...
      [zip] Building zip: /opt/OV/OMU/adminUI/
support_20090325162209.zip
[echo] cleaning up ...
[echo] send the file /opt/OV/OMU/adminUI/support_20090325162209.zip
to support
BUILD SUCCESSFUL
Total time: 2 minutes 30 seconds
```

At the end of the output you see the support filename's name and location. Please send this file to Product Support.

5 Maintenance

This chapter discusses typical situations where the Administration UI configuration must be updated, when certain parameters are changed within your HPOM environment.

Currently two scenarios exist:

- Password Change of Oracle Database User on page 48

- Change of Oracle OMU Database Settings (Port, URL). on page 49

Password Change of Oracle Database User

Administration UI uses a direct connection into the OMU Oracle database. From this connection all data is fetched which is used for the typical object listings (list all nodes, policies, policy bank).

By default the Administration UI installer suggests during the installation process to use the "opc_op" user for that connection. The installer also requests the opc_op users's password, which will be saved in encrypted form in the Administration UI configuration.

If the password of this user is changed (for example due to security rules), it is important, that this password is also updated inside Administration UI.

In order to do so please perform the following steps:

- Update the password inside Administration UI:

  ```
  # /opt/OV/OMU/adminUI/adminui password -u ovodb -a -p <new_password>
  ```

- Restart Administration UI using this command:

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

Change of Oracle OMU Database Settings (Port, URL).

If any of the existing OMU Oracle database settings is changed it is also important to update the corresponding configuration entries inside Administration UI. Otherwise, Administration UI will not be able to connect to Oracle and any HPOM object class listing request will fail (for example list policy bank).

Possible Oracle change which will impact Administration UI are:

- Hostname change of a remote Oracle server.

- Change of HPOM Oracle database port.

- Change of HPOM Oracle database SID.

- Communication of Oracle is changed: secure (oci) ./. unsecure (TCP).

If any of these configuration items is changed, it is necessary also to update this information in all required Administration UI configuration files.

All Oracle related information is stored in three configuration files which are:

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

Each configuration file contains an url with the relevant Oracle connectivity information. It could look like this for example:

```
ovodb.url=jdbc:oracle:thin:@avocado.hp.com:1521:openview
```

The syntax and fields which could require modification are:

```
ovodb.url=jdbc:oracle:{thin|oci}@{Oracle_host}:{port}:{SID}
```

Most items should be self-explanatory:

- `{Oracle_host}` - Oracle server hostname which hosts the HPOM database.

- `{port}` – Oracle port.

- `{SID}` – OMU database instance name (SID).

- `{thin|oci}` – Oracle can operate using unencrypted (thin) or encrypted communication (oci).

These settings can be checked manually by using one of the following commands. $ORACLE_HOME needs to be correct:

```
$ORACLE_HOME/bin/tnsping {oracle_server}
or
$ORACLE_HOME/bin/lsnrctl status
```

The output of the latter command could look like this:

```
[...] Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=openview)))
Services Summary [...]
```

(PROTOCOL=TCP) stands for unencrypted communication.

(PROTOCOL=ICP) indicates that you need to enable "thin" inside the mentioned configuration files of Administration UI.

If ICP and TCP are both are both used we recommend to use an unsecure Oracle connection.

If only secure Oracle communication is allowed but normal communication via TCP/IP should be added, this can be achieved by modifying the listener.ora file on the target system like this:

BEFORE

```
===
LISTENER =
  (ADDRESS_LIST =
        (ADDRESS=
           (PROTOCOL=IPC)
           (KEY= openview)
        )
  )
STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10
LOG_DIRECTORY_LISTENER = /appl/ora/product/10.1.0/network/log
LOG_FILE_LISTENER = listener
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME=openview)
      (ORACLE_HOME=/appl/ora/product/10.1.0)
    )
 )
```

AFTER

```
LISTENER =
  (ADDRESS_LIST =
        (ADDRESS=
           (PROTOCOL=IPC)
           (KEY= openview)
        )
              (ADDRESS =
                (PROTOCOL = TCP)
                (HOST = abcdefg1)
                (PORT = 1521)
              )
  )

STARTUP_WAIT_TIME_LISTENER = 0
CONNECT_TIMEOUT_LISTENER = 10
LOG_DIRECTORY_LISTENER = /appl/ora/product/10.1.0/network/log
LOG_FILE_LISTENER = listener
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME=openview)
      (ORACLE_HOME=/appl/ora/product/10.1.0)
    )
  )
```

(intentionally left blank)

6 Access to all Areas

Introduction

Before usage of individual functions is discussed, this chapter wants to give an overview on the main components that can be accessed via the Toolbar Menu (Home, OMU, Server, Admin, Help) and their relative Administrative Menus.

Once a Toolbar Menu icon has been clicked, the Administrative Menu will list all available configuration objects in this section via its drop down menus

- **Home** - Click the Home icon in the Toolbar Menu to return to the HP Operations Manager for Unix Administration UI start page.

- **OMU** - In the OMU context, you manage all OMU related objects, for example: nodes, policies, tools, agent installations, etc.

- **Server** - The information in the Server section describes the user interface displayed when you are working in the server data context inside the Administration UI application. Here you can manage tasks, and browse details of logfiles on the local server.

- **Admin** - In the Admin context, you can configure and manage the users who log in to HPOM Administration UI. Based on user roles you can define who can do what inside the Administration UI web interface.

- **Help** - Click the Help icon to display the online-help system. Once you have set the data context, for example: OMU, click the Help icon at the top-right of the page you are viewing to display context-sensitive help about the objects displayed..

Note that the rights and responsibilities granted to the user in whose name you log in determine the access you have to the displayed objects.

Home Icon

The available functions offered by the Administrative Menu can be seen in Figure 41 on page 52.

- **"Edit" -> "My User Settings"**
  Here the user information and password of the user currently used to log in can be modified/updated.

- **"Edit" -> "Logout"**
  To logout also the white X in the top right hand corner can be used, see Figure 40 on page 52, which is generally quicker.

  Figure 40 Logout
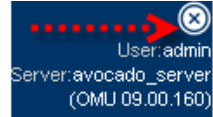
- **"Browse" -> "Shopping Cart"**
  The shopping cart is a convenient location where you can keep configuration-data items temporarily before downloading them to a file. The shopping cart menu provides options that allow you to browse or delete the current contents of your shopping cart. Please note, that the contents of the shopping cart is lost when you log out of OMU Administration UI.
  Convenience links also exist in the OMU module: Administrative Menu: "Browse" -> "Shopping Cart"

- **"Browse" -> "Notifications"**
  List all the notification messages sent to the user running the current browser session.

- **"Servers"** shows which OMU server is currently selected and active. With Administration UI there is only one HPOM server available.

Figure 41
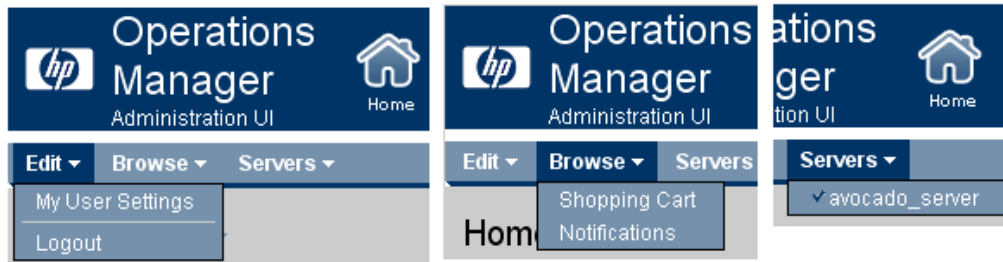
On the next page all functions accessible through the Administrative Menu inside the OMU icon will be explained.

OMU Icon
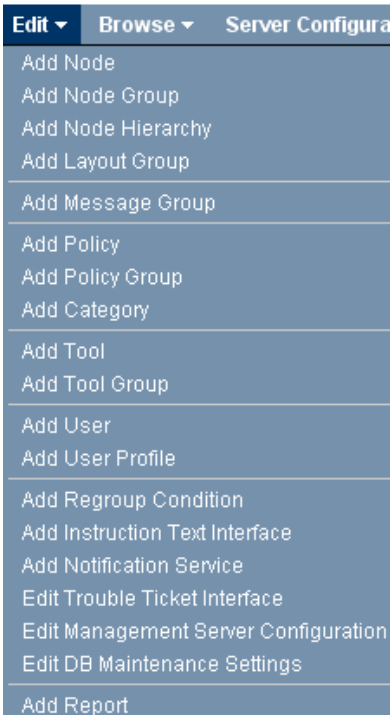
Figure 42

- **"Edit" -> "Add Node"**
  The add node page displays options that enable you to define new managed nodes and add them to your OMU environment.
  You define a managed node by selecting the node type and entering information in fields in various property tabs. The number and type of tabs which require you to enter information is determined by the type of node you choose to create.

- **"Edit" -> "Add Node Group"**
  The add node group page displays parameters for new OMU managed node groups and allows you to define the node group quickly and completely.

- **"Edit" -> "Add Node Hierarchy"**
  The add node hierarchy page allows you to define all parameters for new a OMU node hierarchy bank.

- **"Edit" -> "Add Layout Group"**
  Node layout groups are collapsible hierarchies that allow you to restrict the number of displayed nodes to those that exist in a particular level or hierarchy. Layout groups allow you to organize large numbers of managed nodes into more manageable groups. Use the add layout group page to create new node layout groups.

- **"Edit" -> "Add Message Group"**
  This function allows you to define new message groups. New message groups are assigned to OMU users in order to ensure that the right users receive the correct messages. Use the Add Message Group page to create new node message groups and add them to your OMU environment.

- **"Edit" -> "Add Policy"**
  Browse the policy types listed in the Type column and click the policy type that you want to add. The type column in the all policies table uses a variety of different icons to indicate the type of policies that are available.

- **"Edit" -> "Add Policy Group"**
  Use this option to create a new policy group.

Figure 43

- **"Edit" -> "Add Category"**
  Use the new category page to create new policy categories and add them to your OMU environment. Categories are logical classifications of policies or nodes. You can use categories to associate policies with instrumentation, nodes, and with user profiles. If you associate policies with instrumentation using categories, you can ensure that the appropriate instrumentation is deployed at the same time as the policy it is associated with.

- **"Edit" -> "Add Tool"**
  The add tool page displays parameters for new OMU tools and allows you to define the tools completely. Use this page to create new tools and add them to your OMU environment.

- **"Edit" -> "Add Tool Group"**
  Use this page to create new tool groups and add them to your OMU environment.

- **"Edit" -> "Add User"**
  OMU users include e.g. operators and administrators, who are responsible for the nodes managed by the OMU management server. The number and type of tabs which require you to enter information is determined by the type of user you choose to create or modify.

- **"Edit" -> "Add User Profile"**
  OMU user profiles can be applied to new users (such as operators and administrators) that you add to the OMU management servers.

- **"Edit" -> "Add Regroup Condition"**
  The add regroup condition page displays parameters that you can use to change the message group to which a message belongs. After the message has been integrated and filtered by OMU, you can instruct OMU to move the matched messages to a new message group on the management server, for example: to new and customized message groups specifically suited to an operator's tasks and responsibilities. Regrouping messages means you do not have to change individual conditions in the message-source policy itself and you do not have to redistribute the policies to move messages from one message group to another. You create the new message groups and move the messages to the new groups after they arrive on the management server.

Figure 44

- **"Edit" -> "Add Instruction Text Interface"**
  The add instruction text Interface page displays the parameters you need to use to provide instruction text to HPOM users by means of an external application such as web browser when a message condition matches and a message is generated. Use this page to create a call to the external applications that you want to use to display instruction text for your HPOM operators in order to help them fix problems.

- **"Edit" -> "Add Notification Interface"**
  The add notifications page allows you to specify an external notification service such as an email or a Short Messaging Service (SMS) to inform OMU operators of important events. You can schedule different notification services at different times of the day. Example: SMS during the day and pager at night.

- **"Edit" -> "Edit Trouble Ticket Interface"**
  The edit trouble ticket interface page allows you to configure a trouble-ticket interface to work with OMU. Use this page to start and stop the trouble-ticket interface and define the system call. Note that the first line of the shell script you use to start the interface must contain the statement "/#!/usr/bin/sh" or the execution of your script or program may fail.

- **"Edit" -> "Edit Management Server Configuration"**
  Use the edit management server configuration page to configure the OMU management server. You can change the type of auditing to be defined, define an external message-stream interface, or set global options.

- **"Edit" -> "Edit DB Maintenance Settings"**
  Use the edit DB maintenance configuration page to manage OMU message storage and maintenance. For example, you can specify the maximum number of active, pending, and history messages that OMU keeps in the database before it sends a warning message to the message browser.

- **Edit" -> "Add Report**
  The add report page displays parameters that allow you to define the scope and contents of any new reports you want to generate for the OMU environment you are managing. Example: simple or detailed reports about message groups or managed nodes. OMU reports allow you to visualize information such a policy deployment on the managed nodes, or tool and message group assignment to user roles.

Figure 45

- **"Browse" -> "Node Bank"**
  Lists the node bank and all objects within. Hierarchies are shown below the Global Browse and Action Menu.

- **"Browse" -> "Policy Bank"**
  Lists the policy bank. Hierarchies are shown.

- **"Browse" -> "Tool Bank"**
  Lists the tool bank. Hierarchies are also shown.

- **"Browse" -> "All Nodes"**
  Gives a flat view of all existing nodes listed alphabetically.

- **"Browse" -> "All Node Groups"**
  Lists all node groups alphabetically.

- **"Browse" -> "All Node Hierarchies"**
  The all node hierarchies page displays a list of the nodes hierarchies that are configured on the OMU management server.

- **"Browse" -> "All Layout Groups"**
  The all node layout groups page displays a list of the node layout groups that are configured on the OMU management server.

- **"Browse" -> "All Node Defaults"**
  The all node defaults page displays a list of all the default configurations for the various types of managed node, including information about the machine type (Tru64 Alpha, Itanium 64/32, Sun SPARC), communication type (HTTPS), operating-system type (OSF, HP-UX, AIX, Solaris, Linux). These settings are used when a node of this type is added or discovered in the network.

- **"Browse" -> "All Message Groups"**
  The all message groups page displays a list of the HPOM message groups deployed on this OMU management server.

- **"Browse" -> "All Policies"**
  Under all policies all currently available policies are listed alphabetically. When a policy is viewed, all policy groups incl. the hierarchy will be displayed below the Global Browse and Action Menu. All links can be click for quick navigation, see Figure 46 on page 57.

Figure 46

OMU - Browse

Figure 47
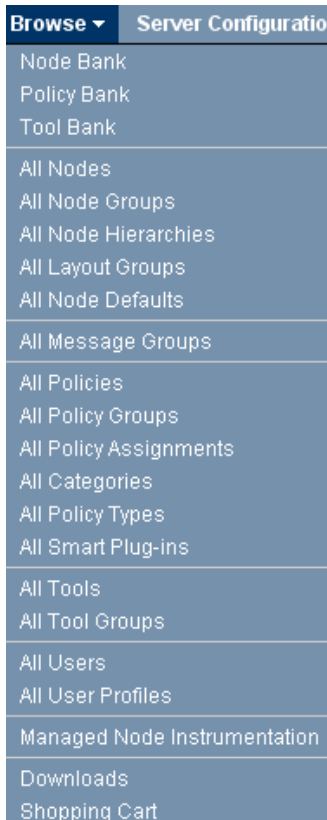
- **"Browse" -> "All Policy Groups"**
  Gives a flat alphabetical listing of all policy groups that exist on this OMU management server.

- **"Browse" -> "All Policy Assignments"**
  The all policy assignments page displays a lists of all the policies and policy groups that have been assigned to the managed nodes or node groups that belong to the OMU management server.

- **"Browse" -> "All Categories"**
  The all categories page displays a list all the categories that are currently available on this OMU server. Categories are logical classifications of policies or nodes. You can use categories to associate policies with instrumentation, nodes, and with user profiles. If you associate policies with instrumentation using categories, you can ensure that the appropriate instrumentation is deployed at the same time as the policy it is associated with.

- **"Browse" -> "All Policy Types"**
  Lists all available policy types. Based on a selected policy type a new policy can be also created from here.

- **"Browse" -> "All Smart Plug-ins"**
  The all Smart Plug-ins page displays a list of the Smart Plug-ins (SPIs) installed on the OMU server.

- **"Browse" -> "All Tools"**
  The all tools page displays a list of the tools that are available to users on the OMU server.

- **"Browse" -> "All Tool Groups"**
  Shows all tool groups that currently exist on the server.

- **"Browse" -> "All Users"**
  Shows all users setup inside HPOM.

Figure 48

- **"Browse" -> "All User Profiles"**
  Lists all existing user profiles.

- **"Browse" -> "Managed Node Instrumentation"**
  Allows you to browse all files and directories (customer, instrumentation, vendor tree) below `/var/opt/OV/share/databases/OpC/mgd_node/`. Files can be uploaded, edited and deleted through the Administration UI web interface.

- **"Browse" -> "Downloads"**
  Whenever the download function is used for an OMU object or a whole object class the downloaded item will be placed inside the downloads folder. It can be found in the file system here: `/opt/OV/OMU/adminUI/data/clipboard/`. Any item in here can be archived (zip/tar), transferred manually to another server or uploaded into the OMU server, if it was copied into this folder.

- **"Browse" -> "Shopping Cart"**
  The shopping cart is a convenient location where you can keep configuration-data items temporarily before downloading them to a file. The Shopping Cart menu provides options that allow you to browse or delete the current contents of your shopping cart. Note that the contents of the shopping cart are lost when you log out of HPOM Administration UI.

Figure 49

- **"Server Configuration" -> "Instruction Text Interfaces"**
  The all instruction text interfaces page displays a list of the instruction-text interfaces that are known to OMU. OMU allows you to use instruction text to help users solve problems; the text can be written manually or supplied by an external application.

- **"Server Configuration" -> "Regroup Conditions"**
  The list regroup conditions page displays a lists of the message conditions that have been moved from one message group to another. Regroup conditions parse the text and attributes of messages that arrive on the OMU management server and reorganize the messages from one message group or service into another. Regroup conditions enable you to organize logically related groups of messages, whose messages come from a variety of different sources but relate to the same type of event or problem.

- **"Server Configuration" -> "Notification Services"**
  This page will display a list of the notification services that are known to OMU. OMU allows you to use external services such as email, pagers, or Short Messaging Services (SMS) to notify OMU operators about important events. You can also choose to use different services at different times of the day, for example: email during working hours and pagers or SMS at night. You can use this page to modify and delete any or all existing notification services.

- **"Server Configuration" -> "Trouble Ticket Interface"**
  The trouble ticket interface page displays information about the status and availability of the trouble-ticket interface.

- **"Server Configuration" -> "Management Server Configuration"**
  The server configuration page displays an overview of the current configuration of the OMU management server, for example: the audit level, the number of allowed concurrent distributions to managed nodes, or whether the message stream interface is enabled.

- **"Server Configuration" -> "Server Policies"**
  Lists all OMU management server policies.
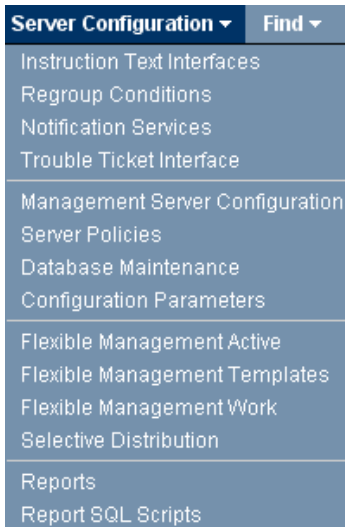
Figure 50

- **"Server Configuration" -> "Database Maintenance"**
  The database configuration page displays an overview of the current configuration of the OMU database, for example: maximum number of active, pending, and history messages that OMU keeps in the database, before it sends a warning message to the message browser, or configure the automatic download to a file of acknowledged messages.

- **"Server Configuration" -> "Configuration Parameters"**
  The all parameters page displays a complete list of the parameters that are set for the selected OMU management server, for example: the name and IP address of the HTTPS authentication server, any OMU variables such as OPC_INSTALLED_VERSION, or a list of available security certificates.

- **"Server Configuration" -> "Flexible Management Active"**
  List flexible management files shows all flexible management configuration files which are available on the currently selected OMU management server. You can use this page to display a list of the files associated with the responsible-manager (flexible management) feature in OMU, and filter the output according to various criteria, for example: the responsible-manager configuration files that are currently active, the default flexible-management "working" files, or all the available flexible-management "templates".
  `/etc/opt/OV/share/conf/OpC/mgmt_sv/respmgrs`

- **"Server Configuration" -> "Flexible Management Templates"**
  List flexible management templates shows all flexible management configuration files which are available on the currently selected OMU management server. You can use this page to display a list of the files associated with the responsible-manager (flexible management) feature in OMU, and filter the output according to various criteria. Example: the responsible-manager configuration files that are currently active, the default flexible-management "working" files, or all the available flexible-management "templates":
  `/etc/opt/OV/share/conf/OpC/mgmt_sv/tmpl_respmgrs`

Figure 51

- **"Server Configuration" -> "Flexible Management Work"**
  Lists all flexible management working files.
  `/etc/opt/OV/share/conf/OpC/mgmt_sv/work_respmgrs`

- **"Server Configuration" -> "Selective Distribution"**
  The selective distribution page displays the contents of the selective-distribution configuration file, seldist, which you use to restrict the configuration data to be distributed to particular nodes and node groups, even if the "Force Update" option is enabled during the distribution operation.
  Please note, that you can click node groups displayed in the list to display more details.
  The selective-distribution file must reside in the following location:
  `/etc/opt/OV/share/conf/OpC/mgmt_sv/seldist`.
  Notice too, that after modifying the seldist file, you have to use the opcseldist utility to reconfigure the Distribution Manager.

  In case the seldist file an error will be displayed as it can be seen below:

Figure 52Seldist Error
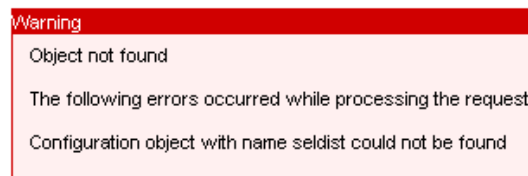
- **"Server Configuration" -> "Reports"**
  The All Reports page displays a list of the reports that are available for the OMU users configured on the currently selected management server, for example: all currently active messages, or policy deployment on managed nodes, and so on. The reports are available in the following directory on the management server:
  `/etc/opt/OV/share/conf/OpC/mgmt_sv/reports/C`.
  Please note, that the list of reports displayed in the all reports page does not include reports generated by HP Reporter.

- **"Server Configuration" -> "Report SQL Scripts"**
  Lists the contents of the /etc/opt/OV/share/conf/OpC/ mgmt_sv/reports/C/ directory. Files can be edited through the web interface or e.g. downloaded to the local computer.

OMU - Find

Figure 53

- **"Find" -> "Locate"**
  The locate configuration objects page allows you to search for and locate all types of OMU objects.

  For details on the locate function please consult the following section: Locate on page 72

OMU - Analyse

In the menu "Analyse" pre-defined queries exist that are designed to help you making sure all nodes are correctly monitored.

Figure 54
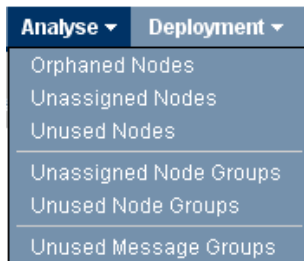
- **"Analyse" -> "Orphaned Nodes"**
  Orphaned Nodes are nodes that are not assigned to any node group.

- **"Analyse" -> "Unassigned Nodes"**
  Unassigned Nodes are nodes, that have no policies assigned (neither direct nor indirect).

- **"Analyse" -> "Unused Nodes"**
  Unused Nodes are nodes, that are not used within user responsibilities.

- **"Analyse" -> "Unassigned Node Groups"**
  Unassigned Node Groups are node groups, that have no policies assigned.

- **"Analyse" -> "Unused Node Groups"**
  Unused Node Groups are node groups, that are not used within any user responsibility matrix.

- **"Analyse" -> "Unused Message Groups"**
  Unused Message Groups are message groups, that are not used within any responsibility matrix.

OMU - Deployment

Figure 55
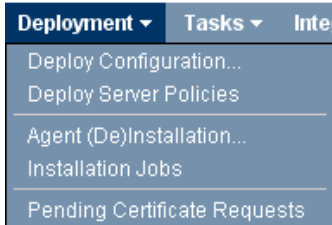
- **"Deployment" -> "Deploy Configuration"**
  The Deploy Configuration page allows you to specify the OMU instrumentation components that you want to distribute from the currently selected management server to the managed nodes and, in addition, to which managed nodes (or node groups) you want to distribute the instrumentation. For details please see: Deploy Configuration on page 81

- **"Deployment" -> "Deploy Server Policies"**
  Deploy the ECS policies, which are assigned to the OMU management server.

- **"Deployment" -> "Agent (De)Installation"**
  The agent (de)installation page allows you to install, update or remove the HPOM agent on the managed node. For details on agent (de)installation please consult Chapter 8, SSH Based Agent Installation.

- **"Deployment" -> "Installation Jobs"**
  The agent installation Logs page displays a list of the log files for the agent-installations that have completed, including status information, and where appropriate, the exit code. It lists all log files inside: `/opt/OV/OMU/adminUI/logs/agent/install/jobs/`

- **"Deployment" -> "Pending Certificate Requests"**
  The pending certificate requests page displays a list of the requests for a security certificate from HTTPS managed nodes that have not yet been granted by the currently selected management server. A HTTPS agent requests a security certificate from the certificate server when it starts up for the first time after installation; the HTTPS agent requires the certificate to communicate with the OMU management server. All requests can be managed and mapped/granted within this page.

Note on Pending Certificate Requests:

In order to list these requests, Administration UI uses the command "`opccsa -list_pending_cr`". If you are using an automated script which removes duplicate certificate requests, please use the command "`opccsa -delete`" instead. Do not use the "`ovcm -remove`" command. Requests removed with this command will still be listed via "`opccsa -list_pending_cr`".

OMU - Tasks

Via the Task menu, it is possible to view system specific log or configuration files, or even trigger certain commands. The result will be displayed in the web interface.

Figure 56
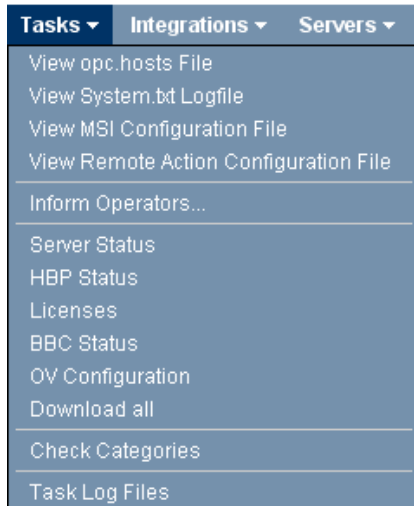
- **"Tasks" -> "View opc.hosts File"**
  If available the opc.hosts file will be displayed.

- **"Tasks" -> "View System.txt Logfile"**
  Will list the contents of the /var/opt/OV/log/System.txt file.

- **"Tasks" -> "View MSI Configuration File"**

- **"Tasks" -> "View Remote Action Configuration File"**
  Via this command the file
  `/etc/opt/OV/share/conf/OpC/mgmt_sv/remactconf.xml`
  will be shown. Additionally it can be edited or downloaded.

- **"Tasks" -> "Inform Operators"**
  The Inform all Operators page allows you to send a text message to all currently logged in OMU Administration UI users.

- **"Tasks" -> "Server Satus"**
  If the menu is selected, the output from the command "ovc" will be displayed.

- **"Tasks" -> "HBP Status"**
  Here the result of the "opchbp_list_all" command will be displayed.

- **"Tasks" -> "Licenses"**
  This will run "ovolicense_rep" and list the result in the web interface.

- **"Tasks" -> "BBC Status"**
  The output of the "bbc_stat" command is displayed here.

OMU - Tasks

Figure 57
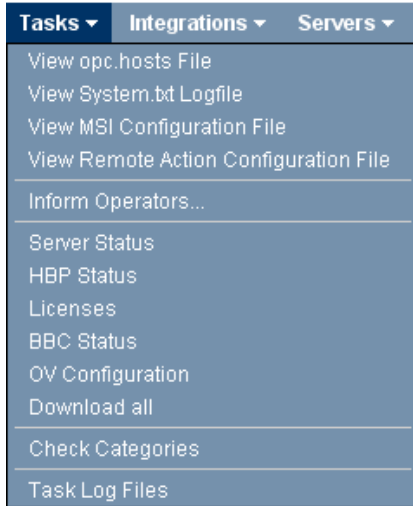
- **"Tasks" -> "OV Configuration"**
  Here the command "ovconfget" will be run and its output displayed in the web interface.

- **"Tasks" -> "Download all"**
  This will run the command "download_ovoconfig". The download can be found in the download directory, which can be accessed via "Browse" -> "Downloads".

- **"Tasks" -> "Check Categories"**
  This menu will trigger an "opcinstrumcfg_check" request. The output will be displayed in the web interface.

- **"Tasks" -> "Task Log Files"**
  Lists the directory `/opt/OV/OMU/adminUI/`logs/task/ containing all Administration UI task log files, so they can be accessed through the web interface.

OMU - Integrations

Figure 58

- **"Integrations" -> "Add-ons"**
  This page lists Add-on products which are available from blue elephant systems, who supplied the technology behind the new Administration UI.

- **"Integrations" -> "HPOM for Unix Operational UI"**
  Will start the Java GUI.

OMU - Servers

Figure 59

- **"Servers"** shows which OMU server is currently selected and active. With Administration UI there is only one OMU server available.

Server Icon

Server - Browse

Figure 60
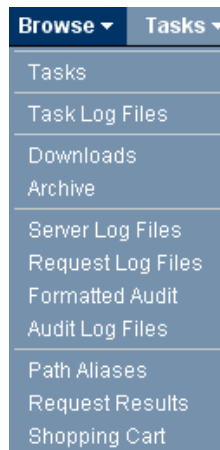
- **"Browse" -> "Tasks"**
  Lists all pre-defined tasks inside Administration UI.
  From the Action Menu they can also be executed.

- **"Browse" -> "Task Log Files"**
  This will list through the web interface the contents
  of `/opt/OV/OMU/adminUI/logs/task/`
  which contains all Administration UI task logs.

- **"Browse" -> "Downloads"**
  Here you also have access to the
  `/opt/OV/OMU/adminUI/data/clipboard/`
  directory where all downloads will be put into.

- **"Browse" -> "Archive"**
  If an item has been archived inside the downloads
  folder (zip/tar) the item will be moved to
  `/opt/OV/OMU/adminUI/data/archive/`.
  "Browse" -> "Server Log Files"
  This will list the contents of
  `/opt/OV/OMU/adminUI/logs/`
  which contain most log files of Administration UI.

- **"Browse" -> "Request Log Files"**
  Request logs from inside
  `/opt/OV/OMU/adminUI/logs/requests/`
  can be found here.

- **"Browse" -> "Formatted Audit"**
  This will list the contents of the audit log in a more
  eye friendly way.

- **"Browse" -> "Audit Log Files"**
  This lists all existing audit log files inside
  `/opt/OV/OMU/adminUI/logs/audit/`

- **"Browse" -> "Path Aliases"**
  You can display and browse through a list of aliases
  defined for file locations on the management server.
  Most aliases are pre-defined and configured during
  software installation. An alias is a link to a precise
  location in the file system, which you can display in
  your browser. The location can be either a single file,
  whose contents you want to make available to users,
  or the contents of a directory. For security reasons,
  the alias restricts access to the file or directory
  specified; you cannot browse the file system outside
  of the target specified in the alias definition. User
  roles can further restrict the type of access to the
  location specified in the path alias. Example: read
  (view), write (modify), or execute (start).

Server - Browse

Figure 61
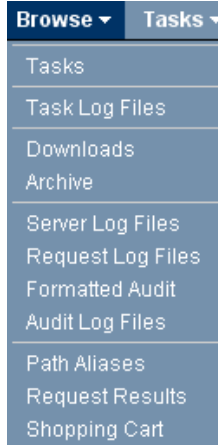
- **"Browse" -> "Request Results"**
  Here all files from within
  `/opt/OV/OMU/adminUI/logs/results/`
  are viewable without the need to use shell access,
  when request logging is enabled.

- **"Browse" -> "Shopping Cart"**
  The shopping cart is a convenient location where you
  can keep configuration-data items temporarily before
  downloading them to a file. The shopping cart menu
  provides options that allow you to browse or delete
  the current contents of your shopping cart. Note that
  the contents of the shopping cart is lost when you log
  out of OMU Administration UI.

Server - Tasks

Figure 62

- **"Tasks" -> "Generate Support Zip"**
  Instead of generating a support.zip file for Support, it
  is also possible to trigger its creation from within the
  web interface.

  Please note, the support.zip will be placed inside the
  standard download directory. To download it via the
  web interface use "Browse" -> "Downloads".

  The interface will show a link to the task log of its
  creation.

## Server - Servers

Figure 63

- **"Servers"** shows which OMU server is currently
  selected and active. With Administration UI there is
  only one OMU server available.

Admin Icon

Please also see: User Management in Administration UI on page 97

Admin - Edit

Figure 64

- **"Edit" -> "Add User"**
  The add user page displays the parameters you need to configure a new admin user quickly and completely. Users here are responsible for the management and maintenance of objects in the OMU Administration UI environment. Which objects a user is responsible for is determined by the user group to which the user belongs and the user role assigned to the user group.

- **"Edit" -> "Add User Group"**
  User groups contain users, who adopts the rights and responsibilities that the group defines by means of user roles.

- **"Edit" -> "Add User Role"**
  User roles are pre-configured user definitions which you assign to user groups in order to specify the roles and responsibilities for all the users who belong to the user group. The roles and responsibilities granted to a user determine the objects the users can see, they type of access they have to objects (create, read, modify, assign), which menu options they can see in the user interface and, as a consequence, the actions they are allowed to perform.

Admin - Browse

Figure 65

- **"Browse" -> "All Users"**
  Lists all users within the OMU Administration UI environment.

- **"Browse" -> "All User Groups**
  Lists all existing Administration UI user groups.

- **"Browse" -> "All User Roles"**
  Here all user roles are listed. They contain all granted access and modification rights to the different OMU objects.

- **"Browse" -> "Logged-in Users"**
  Here the administrator of Administration UI can quickly check, who is currently logged in.

- **"Browse" -> "List Locks"**
  List locks displays a list of the locks that exist on objects which users are currently modifying. If a user attempts to modify an object which is locked by another user, a warning is displayed.

- **"Browse" -> "Notifications"**
  Lists all the notification messages sent to the user running the current browser session.

Admin - Analyse

Figure 66
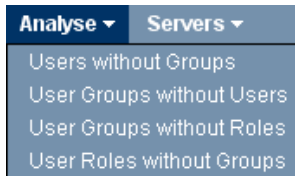
- **"Analyse" -> "Users without Groups"**
  Here you will receive a listing which user does not belong to any user group.

- **"Analyse" -> "User Groups without Users"**
  Lists empty user groups.

- **"Analyse" -> "User Groups without Roles"**
  This check lists user groups without any roles. It is vital that a user group has one or more user roles assigned. Otherwise no user in that group will be able to log in!

- **"Analyse" -> "User Roles without Groups"**
  Lists roles which aren't assigned to any user group.

Admin - Servers

Figure 67

- **"Servers"** shows which OMU server is currently selected and active. With Administration UI there is only one OMU server available.

Help Icon

Help - About

Figure 68
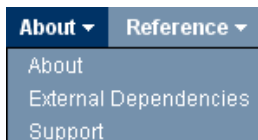
- **"About" -> "About"**
  lists the version and build number of the installed version of Administration UI.

- **"About" -> "External Dependencies"**
  Administration UI includes software developed by various open-source projects and organizations which are listed here.

- **"About" -> "Support"**
  Lists some troubleshooting tips.

Help - Reference

Editing is not possible here. All entries are for reference purpose only.

Figure 69

- **"Reference" -> "Logging"**
  Gives some details about the logging mechanism and how to change the logging level.

- **"Reference" -> "JMX"**
  Lists some information about configuration about the JMX self management.

- **"Reference" -> "Files"**
  Contrary to the information here, there is currently NO ftp file server installed together with Administration UI.

- **"Reference" -> "Auditing"**
  Audit fields inside the audit log and its location are explained here.

- **"Reference" -> "User Management"**
  Some information about LDAP, PAM integration can be found here.

- **"Reference" -> "Web Application"**
  Some overview on the application that controls the web interface is given here.

- **"Reference" -> "Command Line"**
  An overview on the command line parameters is listed here.

- **"Reference" -> "Password Tool"**
  Please consult the main Administration and Configuration Guide for Administration UI for usage of the password tool!

- **"Reference" -> "HPOM for UNIX"**
  Some information on the tools upload and Java GUI integration can be found here.

7 How To

This chapter will discuss the following topics in greater detail:

The first section shows you how to locate HPOM objects in Administration UI:

- Locate on page 72

The following section deals with policies and versioning:

- Compare Policies on page 74

- Versioning on page 76

The next section's subject is how to deploy your HPOM configuration:

- Deploy Configuration on page 81

Deassigning policies, policy groups, node groups:

- Deassigning Policies, Policy Groups, etc. on page 85

Since the responsibility matrix editor has some advanced features there is a dedicated section for it:

- Responsibility Matrix on page 91

Administration UI user management will be dealt with in the section:

- User Management in Administration UI on page 97

Since some steps need to be observed when removing a node via Administration UI there is a dedicated section for this subject:

- Node Removal on page 102

Agent installation will be discusses in a separate chapter. Please see Chapter 8, SSH Based Agent Installation

Locate

The Locate Configuration Objects page allows you to search for and locate all types of HPOM objects. While inside in an HPOM object class, for example policies or nodes this is called a filter, both filter and locate are the same function. The only difference is that within an HPOM object class the filter is limited to that object class.

Via the locate command you can define the locate "filter" yourself what type of HPOM object you are searching for.

You can access while being in the HPOM icon context via the Administrative Menu: "Find" -> Locate.

The locate window looks like the following screen shot (Figure 70 on page 72):

Figure 70 Locate Window

Please note, that the number of fields depends on the object selection inside the Locate drop down menu! Therefore, please use the Locate drop down menu to select first the object class in which you want to locate an object.

The previous example shows the default locate window for a policy.

Because of the object differences, a Policy Group locate window only offers a name field:

Figure 71 Policy Group Locate

Each available field can be used to narrow down the result. But it is not compulsory to use those different fields.

Locate usage boils down to this:

- **Locate** - Use the drop down menu to select the type of object you want to locate.

- **where name** - Use the drop down menu to decide the pattern matching technique to use as the search method, for example: "contains", "is", or "matches pattern" (see below). You will also have to enter a text string to use in the search.

Optional fields are for example:

- **and policy type is** - Policies only. If you are searching for a policy, use the drop-down menu to select the policy type, for example: event correlation (ec), logfile, monitor, and so on.

- **and network type is** - Nodes only. If you are searching for a managed node based on network type, use the drop-down menu to select the network type of the managed node you want to locate.

- **Machine type** - Nodes only. If you are searching for a managed node based on machine type, use the drop-down menu to select the machine type of managed node you want to locate.

You can define the way in which the string you enter is evaluated by choosing one of the available location methods, for example: "contains", "is", or "matches pattern". The way the string is evaluated determines what results are displayed.

- **"contains"** - The search option "CONTAINS" evaluates the object detail you specify (policy name, Tool label, etc.) and displays in a list any object it finds which contains the string you enter. If you enter the string "and", the CONTAINS filter evaluates the list of objects and displays only those which contain (in any position) the string "and", for example: "and", "blueand", "andblack", "blueandblack".

- **"is"** - The search option "IS" evaluates the object detail you specify (name, label, etc.) and displays in a list any object it finds which is identical to the string you enter. If you enter the search string "and", the IS search option evaluates the list of objects and displays only those which match the string "and". Note that the strings "blueand", "andblack", or "blueandblack" would not be displayed if you use the "IS" search option in combination with the string "and".

- **"matches pattern"** - The search option "MATCHES PATTERN" evaluates the object detail you specify (name, label, etc.) and displays in a list any object it finds which matches in any form the pattern defined in the string you enter. You can use all the special characters that are normally available in pattern matching, such as: asterisk (*), angled brackets (< >), and so on. For example, if you enter the string "an*", the MATCHES PATTERN filter evaluates the list of objects and displays all objects that contain the defined string pattern, which includes: "and", "blueand", "andblack", or "blueandblack". However, the following strings would also be displayed "ant", "blueanx", "anycolour", and "blueankle".

  Note that you can further restrict the context by using Perl pattern matching, for example: "[bes][bes][bes].net.*", for all node-group names with any combination of the characters "b", "e", "s", followed by ".net.", and any string (*) would display node names such as: "bes.net.com, ebs.net.com, sbe.net.biz, seb.net.eu, and so on.

Compare Policies

Administration UI gives you the ability to compare policies against each other. This can be especially useful if you want to find out what the difference between separate versions of the same policy is.

From Action Menu of a policy you can select: "Compare to" or "Compare to (Raw Mode)" if you want to do a raw format comparison (see Figure 72 on page 74).

Figure 72 Policy Compare Function
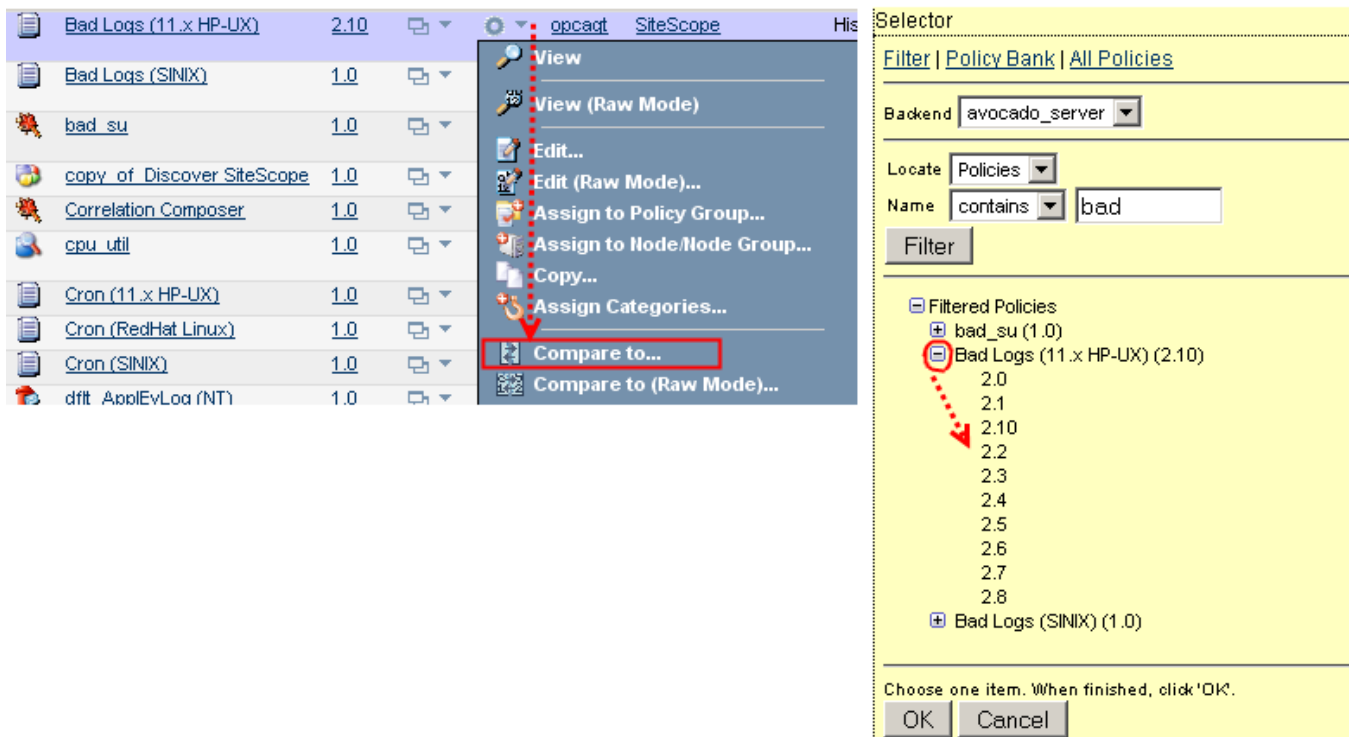
Inside the selector window you can use a free filter, the policy bank or even all policies listing in order to find the target policy against which you want to run the comparison against. Behind each policy its current version is listed.

Simply select the policy and press "OK".

In order to be able to run a comparison against a previous version of a policy, please use the [+] button in front of each policy. Once you clicked it, you will receive a list of all available policies inside the version control system, see Figure 72 on page 74.

The following screenshot (Figure 73 on page 75) shows the result of such a comparison. Here a previous policy version was compared against the currently "live" version inside HPOM.

A color coding system is used to show the differences:

- **Yellow** - Yellow highlights text which has been modified. This text has been modifed between the two policies.

- **Red** - Red highlights text (or a whole condition) which has been removed from the selected policy.

- **Green** - Green indicates newly added text (or a whole condition).

Figure 73 Policy Comparison Result

Versioning

As soon as a policy is modified and saved, a new version of it will be automatically checked into the version control system. Please note, there are no versions for policy groups. Versioning cannot be disabled, but it is possible to manually define the version number if necessary (see below).

Policies have a **major version** number (before the comma) and a **minor version** numer (after the comma). Both number parts can have up to four digits. Externally those four digits blocks are generally not visible. Version 1.1 is internally in reality 0001.0001.

How to Control Versioning?

By default for versioning "Auto-increment on save" will be used. This means that with each policy modification the version number will be incremented to the next minor version. For example: 2.9 will be incremented to 2.10; 1.19 to 1.20.

Whenever a policy is modified you can control the versioning mechanism which will be used. The field to do so can be found in the policy editor inside the tab "Properties", see Figure 74 on page 76.

Three options exist to control the versioning system:

• **Specify version manually** - Here the otherwise not editable version field can be accessed and a version number to your liking entered. For example when a new major version should be defined.

• **Specify version manually + force overwrite if already present** - This feature can be useful, if you do not want to create a new version but want to re-use an existing version number.

• **Auto-increment on save** - This is the default setting. Minor version increments take place each time a policy is modified.

Figure 74 Version Control
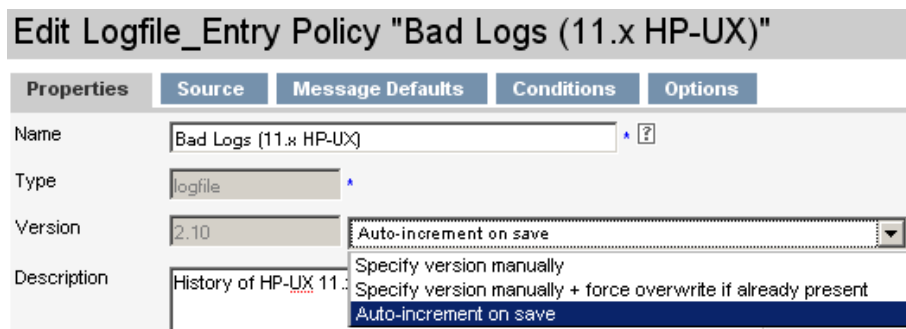
Version Listing

All existing versions of a policy can be accessed the policy's Browse Menu -> "Versions", see Figure 75 on page 77.

Figure 75 Version Access
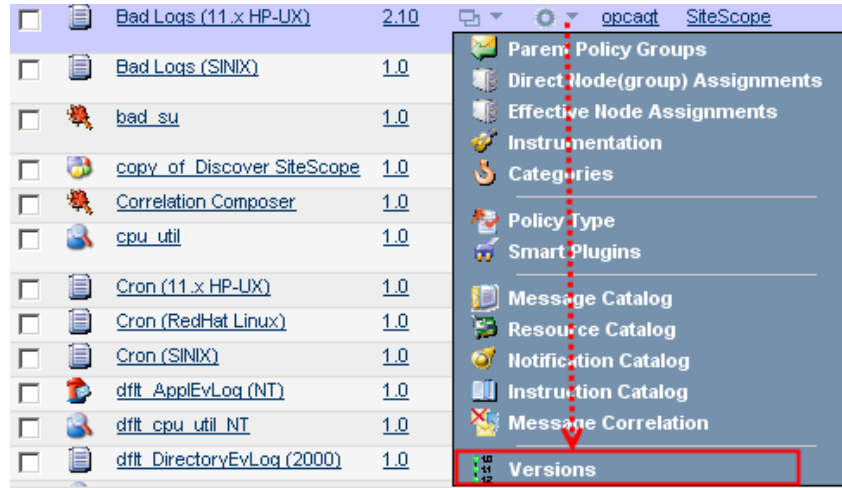
All versions existing for the policy will be listed, see Figure 76 on page 77.

Figure 76 Version Listing

Assigning Different Versions

Policies can be assigned to policy groups, nodes or node groups. It is possible here to define an assignment mode which defines what happens, when a new policy version is created:

- **Fixed** - The version which is used in the assignment is permanently associated with the object. Therefore, if a new policy version is created, this will have no effect on the assignment. The original policy version is still used for and on this managed node / node group.

- **Minor to Latest** - If only the minor version is changing, the latest minor version will be used for all assignments. If the major version changes (1.3 to 2.1) then this change will not impact those assignments where "minor to latest" has been defined.

- **Latest** - The assignment will be updated and adjusted to the latest version as soon as a version change takes place, whether this is a minor or major version change.

Conflicts are possible, if conflicting assignment rules exist. For example: if a *fixed* policy version is assigned via a policy group. But via the node group *latest* is defined. The conflict is solved that the highest, that mean latest, version will win.

Defining Policy Version Assignments

When a new policy version exists there are two possibilities to define:

- Once inside a policy group the function "Modify assigned Version" can be used from the Action Menu for this policy that was changed, see Figure 77 on page 78.

Figure 77 Modify Assigned Version
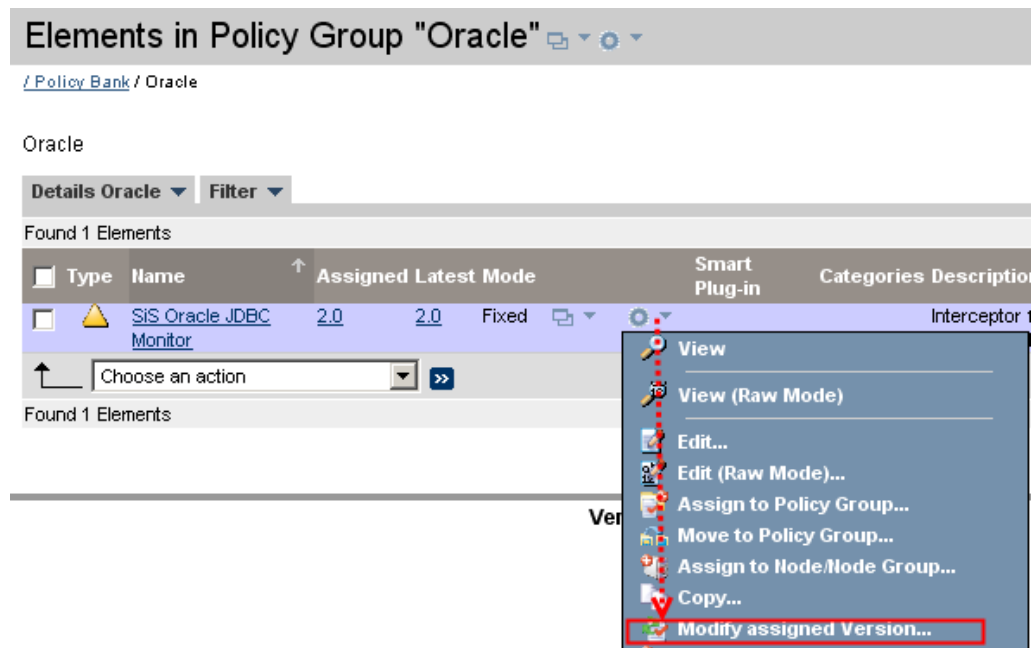
Via the yellow selector the assignment details can be defined, see Figure 78 on page 79. "OK" will start the policy-assignment update.

Figure 78 Version Assignments
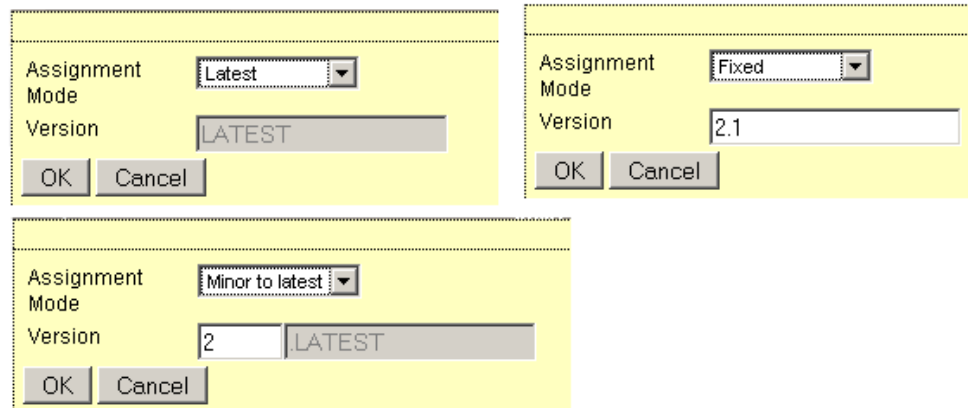
- However, usually it is easier to use the "Update Assignments" option in the Action Menu to update multiple policy assignments at the same time for a policy group, node or node group in a single operation, see Figure 79 on page 79.

Figure 79 Update Assignments
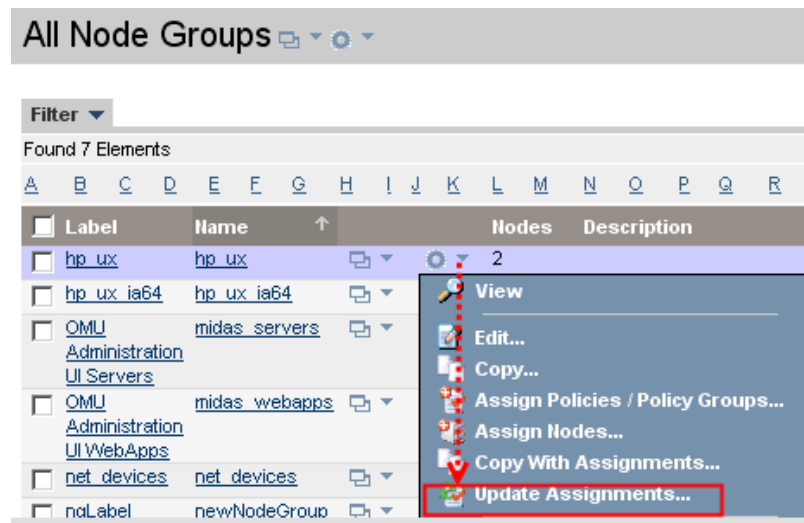
After Update Assignments has been selected a yellow selector window will appear, see Figure 80 on page 80.

Use the drop-down menus and dialog boxes displayed to specify the policy-assignment strategy you want to implement; the options available in the drop-down menus are described in detail in the tables below.

When you have completed the configuration steps, click OK to start the policy-assignment update.

Figure 80 Update Policy Assignment Details
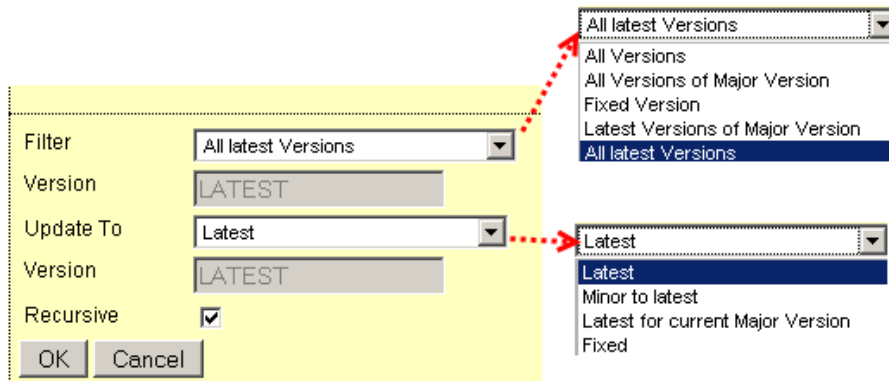
— **Filter Field:**

- **All Versions** - Consider for update all versions of any policies assigned to the selected object (node, node group, or policy group).

- **All Versions of Major Version** - Consider for update all minor (interim) versions of the specified major version, where the assigned major version is equal to the version number you specify in the Version field.

- **Fixed Version** - Consider for update all assigned policies where the assigned version is identical to the version you specify in the Version field.

- **Latest Versions of Major Version** - Consider for update all assigned policies where the assigned version is identical to the major version number specified in the Version field and the minor version is the latest version.

- **All Latest Versions** - Consider for update all assigned policies, where the assigned version is the latest version of the policy.

After you specify the assigned policies that must be updated, you have to define the version of the policy to use when performing the update operation.

— **Specify the Update Version:**

- **Latest** - Update the assigned policies to the latest (most recent) available policy version

- **Minor to Latest** - Update the assigned policies to the latest minor (interim) version of the currently assigned major version.

- **Latest for specific Major Version** - Update the assigned policies to the latest version available for the major version you specify in the Version field. For example, if the assigned policy version is 1.3, and you specify an update to the policy version 2, the update operation replaces the assigned policy 1.3 with the latest available interim version of the version 2 policy, even if there is a newer (version 3.*) policy available.

- **Fixed** - Update the assigned policies to the given fixed version.

Figure 81

Deploy Configuration

Introduction

The Deploy Configuration page allows you to specify the OMU instrumentation components that you want to distribute from the management server to the managed nodes and, in addition, to which managed nodes (or node groups) you want to distribute the instrumentation.

Three ways exist to run deployments which will be discussed in this chapter:

- The deploy function can be accessed within the HPOM context via the Administrative Menu: "Deployment" -> "Deploy Configuration". This will be discussed first. See Main Deploy Editor on page 81.

- But there is also an alternative. You can use the Action Menu of a node, node group or layout group, to issue the deploy command for that particular object.

- A third option is to use the List Menu when you want to select multiple distribution targets. See Context Based Deployments on page 82.

Main Deploy Editor

The main deploy editor can be reached from within the OMU icon context by selecting "Deployment" -> "Deploy Configuration".

You should get the following window (Figure 82 on page 82).

- Enable all check boxes for those items that should be included in the distribution package.
  If instrumentation is checked this will add the instrumentation files in the category directories to the distribution package. The option to include instrumentation and subagents is new in HPOM 9.

- Check the Force Update box if you want to overwrite existing data on the managed nodes during the distribution.

- Check the Purge box if you want to purge the distribution of the selected instrumentation components, even if this leads to conflicts with instrumentation that already exists on the selected managed nodes (new in HPOM 9).

- Use the [...] box to browse the available managed nodes and select the nodes or node groups to which you want to distribute the HPOM instrumentation (see Figure 83 on page 82).

- Trigger the actual distribution by selecting the button "Distribute"

.

**Figure 82 Deploy Main Window**   **Figure 83 Selector**
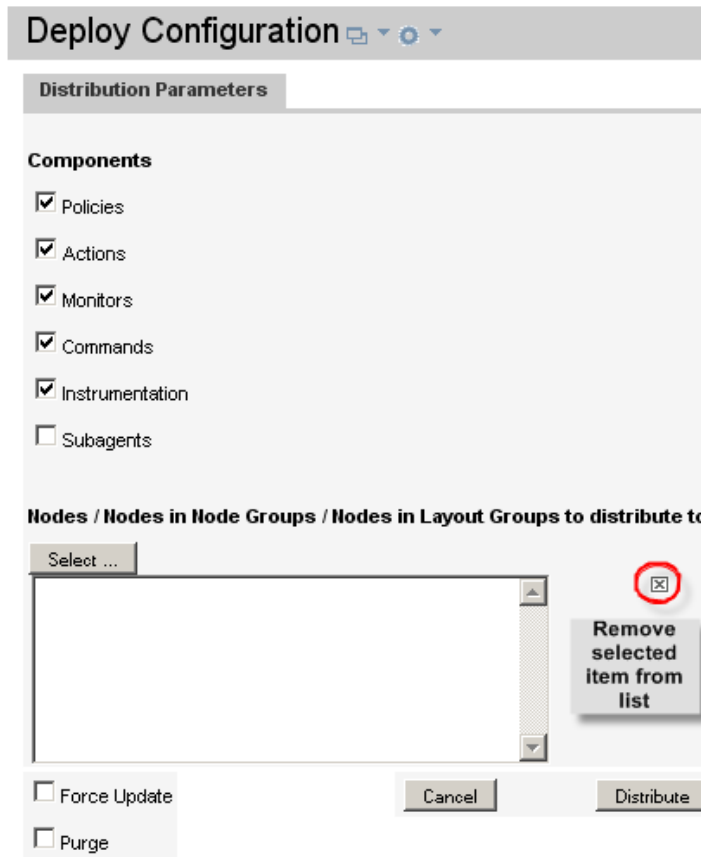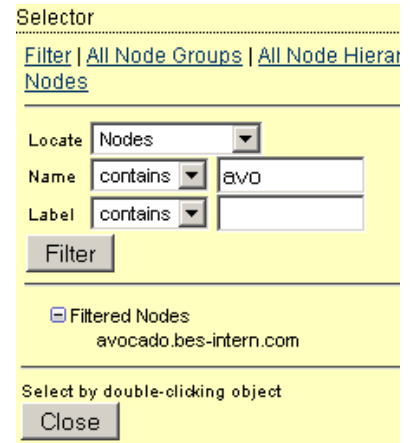
Context Based Deployments

The other two alternatives are to trigger the distribution from within the object class
you are in, for example: node, node group or layout group.

Action Menu

For a single object (node, node group, layout group or inside the node bank) the
distribution can be triggered via the context based Action Menu of that object, see
the following screenshots (Figure 84 on page 83):

Figure 84 Deploy via Action Menu
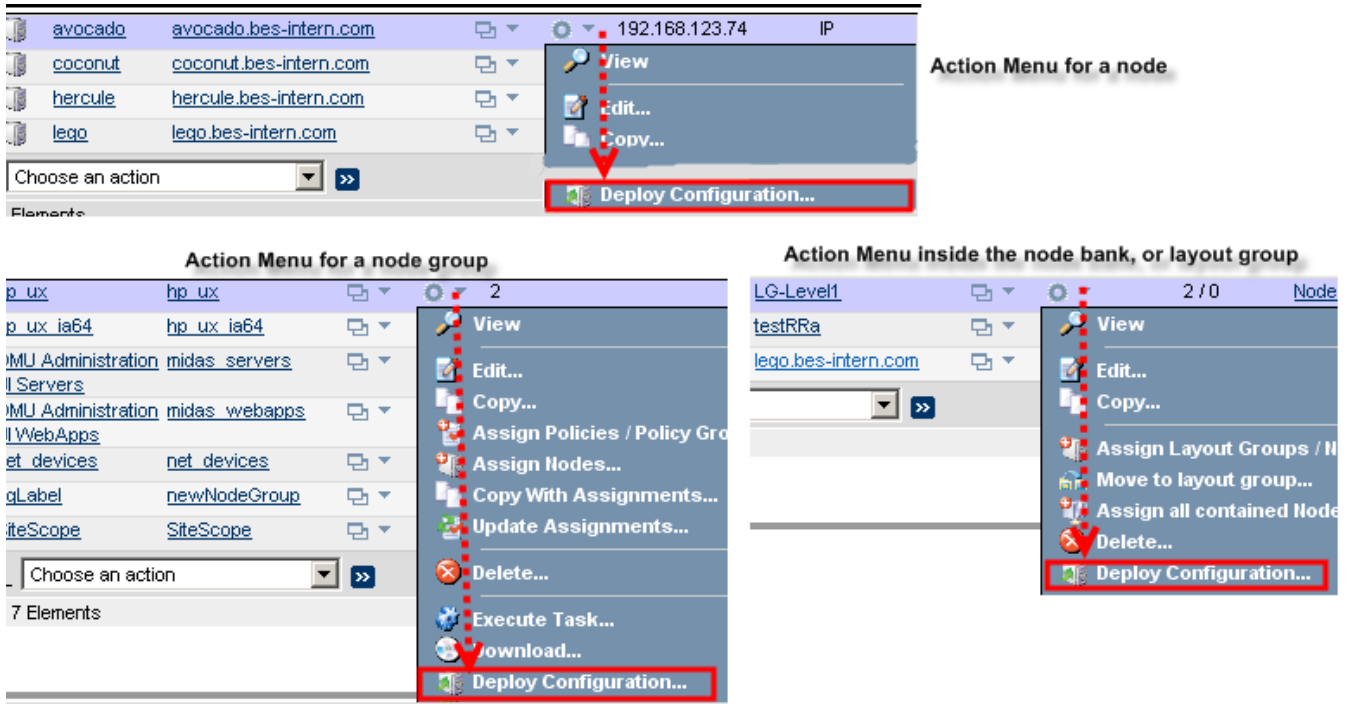
If the command "Deploy Configuration" is selected for an object a yellow pop up window will show up in which the distribution details can be defined.

The options are exactly the same option as they are available inside the main deploy window (see Main Deploy Editor on page 81).

Figure 85 Distribution Options
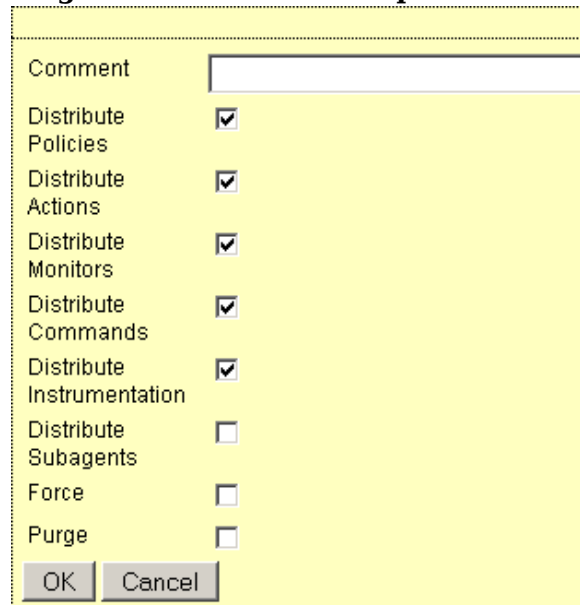
List Menu

Finally, the third alternative to trigger a distribution is also from within an object class like "All Nodes, "All Node Groups" or "All Layout Groups".

To select multiple nodes or node groups you can also use the List Menu to enable each check box of each object for which a distribution should be triggered.

Figure 86 Distribution via List Menu
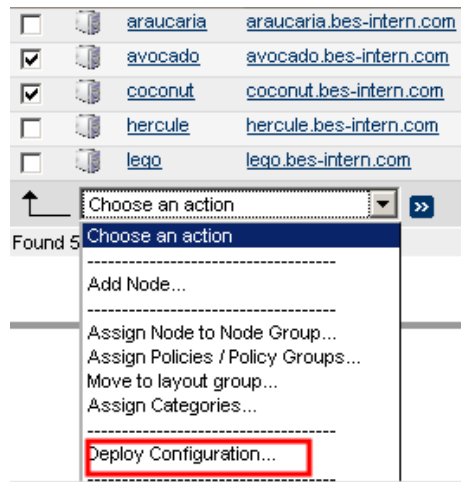
If the command "Deploy Configuration" is selected for one or more objects here a yellow pop up window will also show up in which the distribution details can be defined, see Figure 85 on page 83.

Deassigning Policies, Policy Groups, etc.

Customer feedback showed, that deassigning nodes, policies, policy/node groups sometimes proves to be difficult. It is planned to improve the menus in the next major version.

> **Note, that a delete is a delete and no deassign! Do NOT use any delete function if you want to perform a deassign operation!**

The following configuration example will be used to demonstrate how to display assignments and how to remove these.

Example:

- Our test node is called "woodford".
- The following *direct* assignments exist for this node:
    — Policy Group "DBSPI-Core",
    — Policies "cpu_util" and "cron (RedHat Linux)",
- "Woodford" is part of the node group "linux".
    — The node group "linux" has the policy group "Linux" assigned to it.
    — The policy group "Linux" itself contains the policy groups "Adv.Linux Policies" and "Quick Start Policies" which contain various policies.

The topics in this section are:

Direct Assignments

Direct assignments (polcies, policy groups) can easily be deassigned via the following workflow:

• From the Browse Menu select "Direct Policy(group) Assignments".

Figure 87 Direct Policy(group) Assignments

This would give the following result (Figure 88 on page 86):

Figure 88 Direct Policy(group) Assignments Result
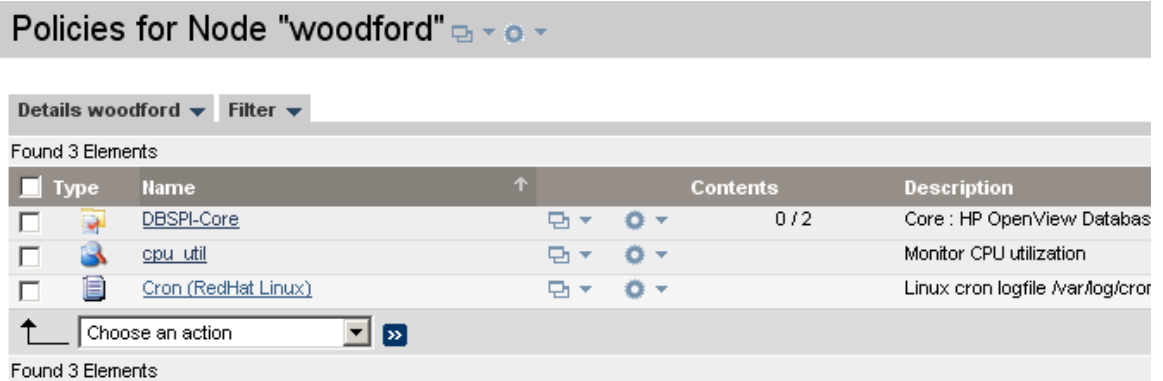
In order to deassign a policy and/or policy group here you have two options:

— For a single item use the Action Menu: "Deassign from Node"

Figure 89 Deassign from this Node - Action Menu
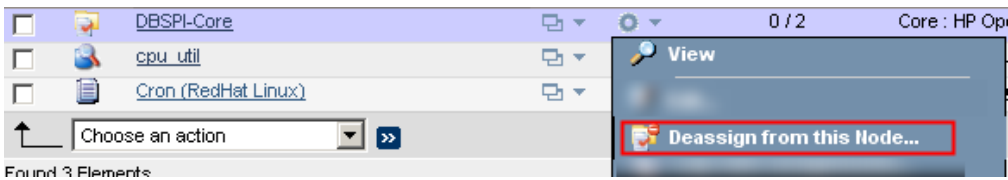
— The second option is useful if you want to deassign multiple objects from a node:

Enable all required checkboxes and select "Deassign from Node" from the List Menu at the bottom of the screen.

Figure 90 Multiple Deassignments
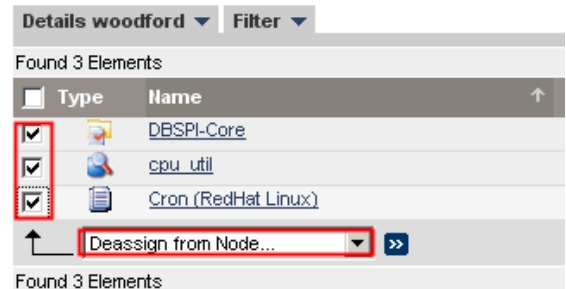
In our example we removed those three direct policy(group) assignments.

Deassigning Indirect Assignments

Basic procedure here is to find out what the node group assignments are. To do so various workflows exist.

- The function "Effective Policy Assignments" in the Browse Menu would show in our example for the node "woodford" something like the screenshot below (Figure 91 on page 87).

  A deassign operation is not possible in this screen. This is because of performance reasons. Resolving the origins (often multiple) of each policy and policy group would simply take too long.

  Moreover, if a policy belongs to multiple policy groups, a simple deassign operation might destroy other assignments, which is not wanted.

Figure 91 Effective Policy Assignments

The recommended procedure in our example would be this:

- Since there are no direct policy group assignments, the existing assignments are inherited from the node group the node "woodford" is in.

- From the Browse Menu of the node "woodford" select "Node Groups".

Figure 92 List Node Groups for a Node

This will list all node groups the node "woodford" is in. In our example "woodford" is only belonging to the node group "linux", see Figure 99 on page 90.

Figure 93 Node Groups for Node "woodford"

Node Groups for Node "woodford"

☐ Label	Name ↑			Nodes	Description
☐ linux	linux			3	linux nodes

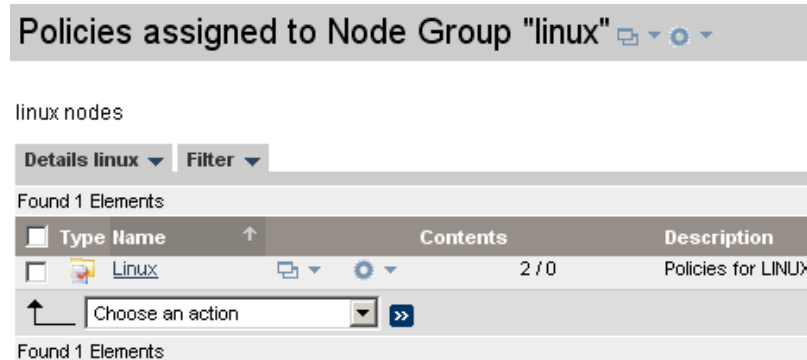Found 1 Elements

Choose an action ▾ »
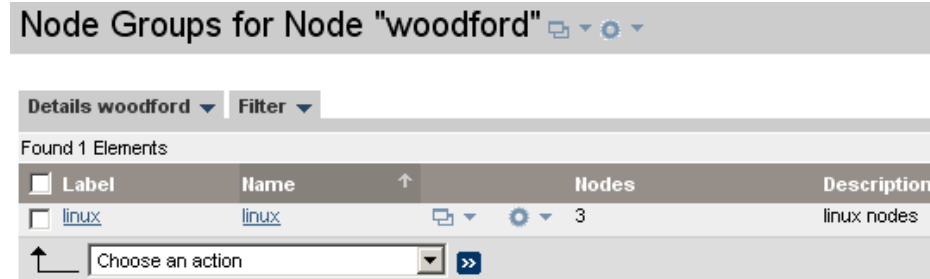
- Via the Browse Menu you again have the possibility to show various relationships ([Figure 94](#) on page 88). In our example select "Direct Policy(group) Assignments".

Figure 94 Browse Menu Node Group

Node Groups for Node "woodford"

Details woodford ▾ Filter ▾

Found 1 Elements

☐ Label	Name ↑			Nodes	De
☐ linux	linux			3	lin

Choose an action

Found 1 Elements

- Direct Policy(group) Assignments
- Effective Policy Assignments
- Effective Node Assignments
- Nodes
- Deployed Policies
- Users
- Profiles
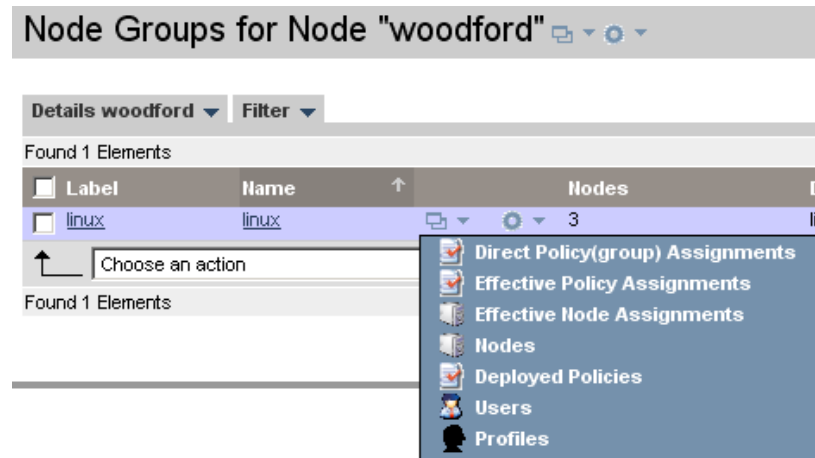
This would give us the following result ([Figure 95](#) on page 88):

Figure 95 Policy/Policy Group Assigment to Node Group

Policies assigned to Node Group "linux"

linux nodes

Details linux ▾ Filter ▾

Found 1 Elements

☐ Type Name	↑			Contents	Description
☐ 📋 Linux				2 / 0	Policies for LINUX

Choose an action ▾ »

Found 1 Elements

- In order to deassign the policy group "Linux" from the node group "linux" two options exist. Either by using the Action Menu or via the List Menu, see Figure 96 on page 89.

Figure 96 Deassign Policy Group from Node Group
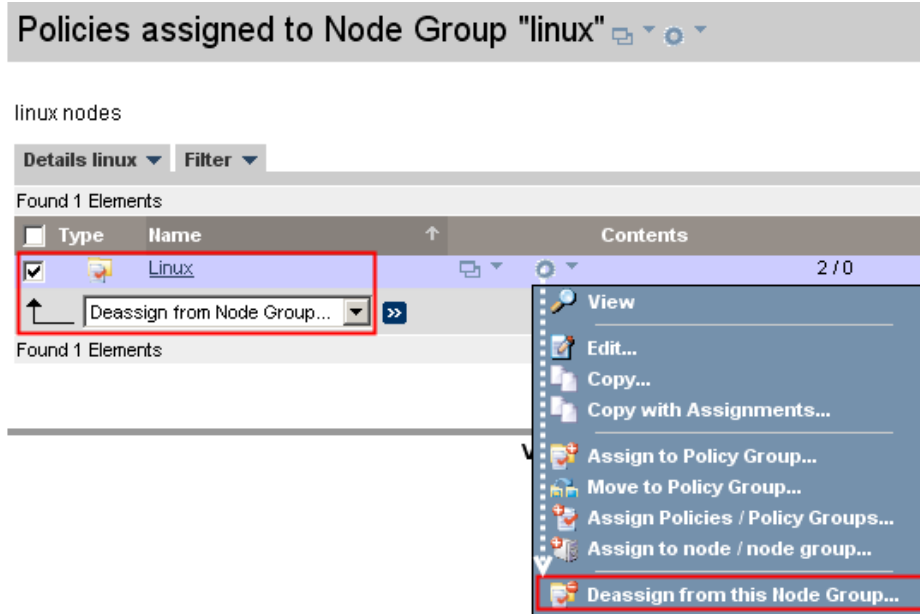
In case you want to deassign a policy group within the policy group (here "Linux") simply select the link for the policy group "Linux".

Here you can deassign any policy group from the policy group you are currently in, see Figure 97 on page 89.

Figure 97 Deassign Policy Group from Policy Group
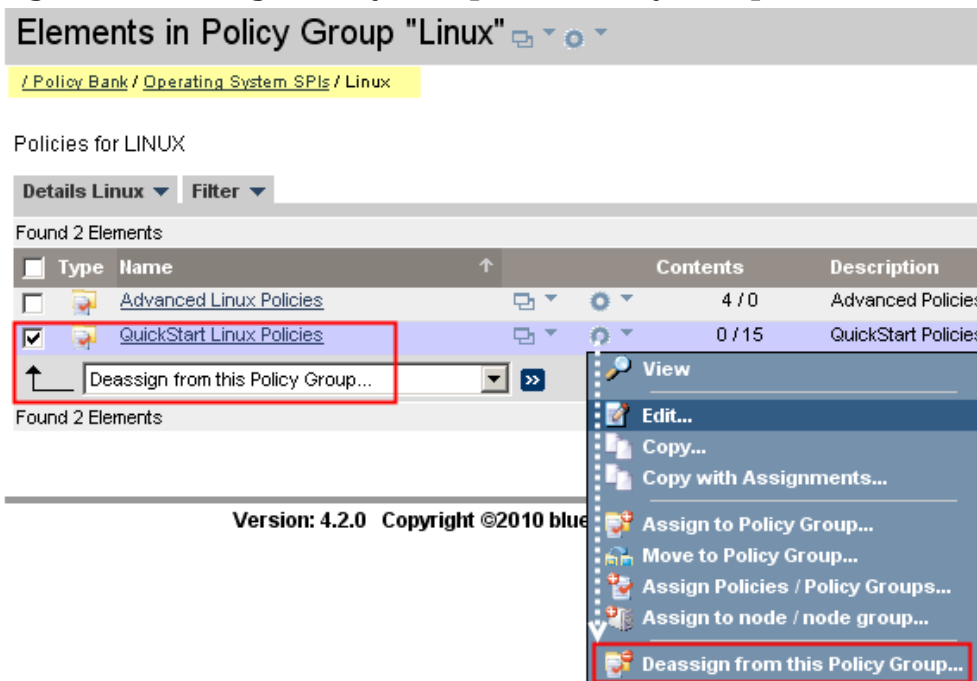
Deassigning Nodes from Node Groups

If you want to remove a node (in our example the node "woodford") from a node group select from the Browse Menu "Node Groups", see Figure 98 on page 90.

Figure 98 List Node Groups for a Node

This will list all node groups the node (here "woodford") is in. In our example "woodford" is only belonging to the node group "linux", see Figure 99 on page 90.

Figure 99 Node Groups for Node "woodford"
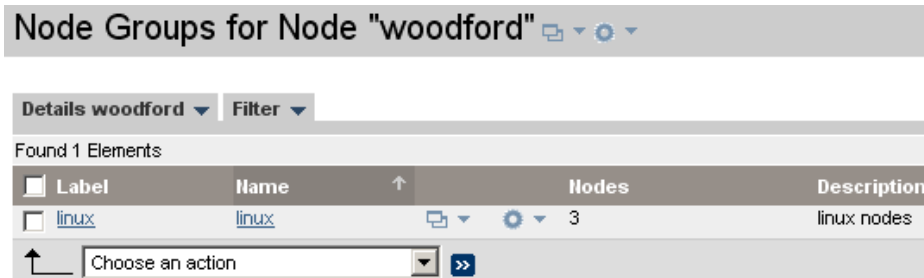
- Inside the results window, it is possible to deassign the node "woodford" from the node group "linux". Again you have two options:

  — You can use the Action Menu "Deassign node from this nodegroup", or

  — You can enable the checkbox and use the List Menu "Deassign node from this nodegroup", see Figure 100 on page 90.

Figure 100 Deassign Node from Node Group
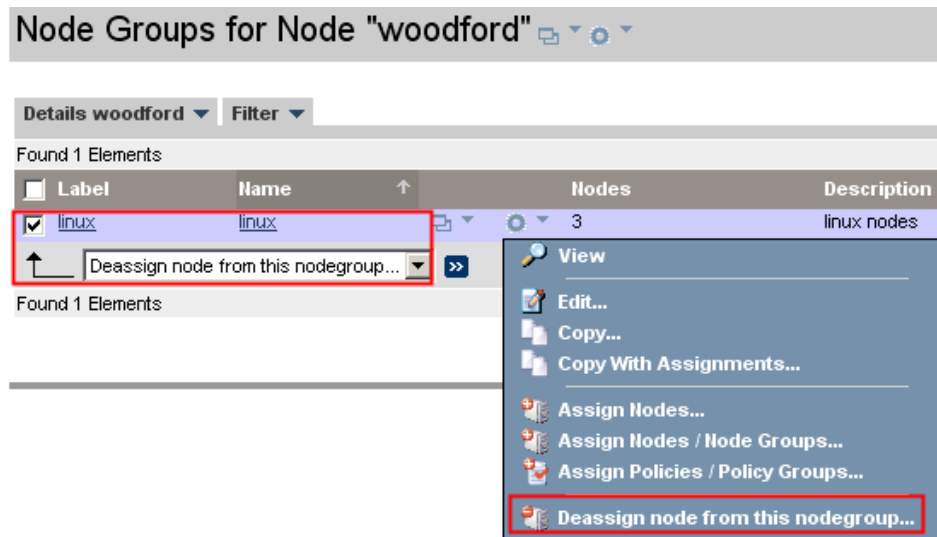
Addendum

- Please note, that the function "All Policy Assignments" (inside the Browse menu in the OMU context), only shows direct assignments.

Responsibility Matrix

Introduction

The Edit Responsibilities page enables you to modify the responsibility matrix for a specific user or user profile. The responsibility matrix specifies the areas of responsibility assigned to a user (or user profile). For example, you can specify the managed nodes a user is responsible for monitoring and, in addition, the message groups whose messages the user is entitled to see and work on.

After changing the responsibility matrix, you can re-assign the modified user profile to the HPOM users (or groups) who require it. A correctly configured responsibility matrix enables you to make sure that the right users receive the correct messages from the appropriate nodes. Please note, that disabled nodes are not considered in the responsibility matrix.

Overview

In order to look at the different features available inside the responsibility matrix editor, please perform the following steps:

Lab:

- Inside the OMU area, please select from the Administrative Menu: "Browse" -> "All Users".

- For the existing default user "itop" select from its Action Menu: "Edit Responsibilites".

The following figure shows how a screen could look like when the responsibility matrix editor is openened for this user ():

Figure 101 Edit Responsibilities

At first glance the responsibility matrix looks similar compared with the old Motif GUI. But several new features and enhancements exist now.

Those visible in the main screen are for example:

— It is possible to (de)select all rows or columns by clicking on the column or row header (see Figure 101 on page 91).

— The horizontal block Node Groups is always visible, also when scrolling down to the bottom of the list.

— If the mouse pointer is above a check box, a small transparent pop up box shows the corresponding coordinates (NG (node group), MG (message group)), see the previous screen shot Figure 101 on page 91.

At the bottom of the responsibility matrix you will find the following four buttons (details will be explained below):

- **EDIT VIEW** - Define what message and node groups are displayed in the responsibility matrix.

- **EDIT SELECTIONS** - Manually clicking on each check box is not ideal. This function is designed to help you in the selection process.

- **SAVE** - Save and exit the editor.

- **CANCEL** - Quit the responsibility matrix editor without saving.

Edit View

Introduction

EDIT VIEW opens the edit matrix view dialog. In this window you define which message groups and node groups you want to display in the responsibility matrix.

The items in the "Available ... Groups" list are those that are available for selection but not yet included in the responsibility matrix (Figure 102 on page 92). Items already within the current responsibility matrix are listed on the right hand side.

**Figure 102 Edit Matrix View**
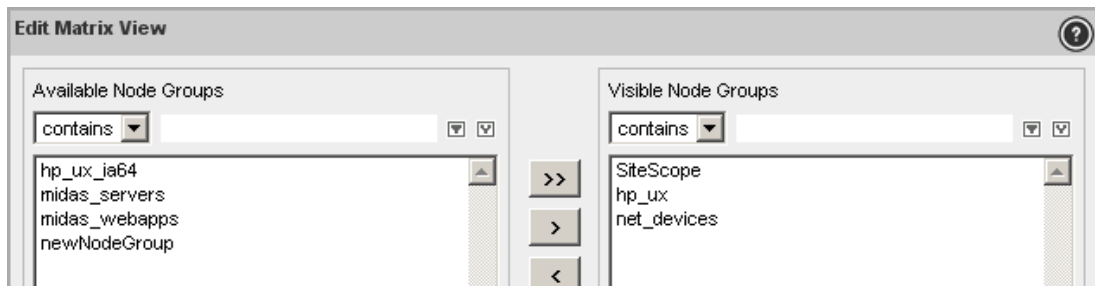
Filter

Since most HPOM management server environments tend to be big, the edit matrix view dialog also includes a powerful filtering option:

— "While you type" - The filter is applied on the fly while you type, giving you some immediate feedback on the listed results.

— While you type also matching results are displayed (below the filter field). Simply click on one of them to select the item, see Figure 103 on page 93.

Figure 103 Responsibility Matrix Filter
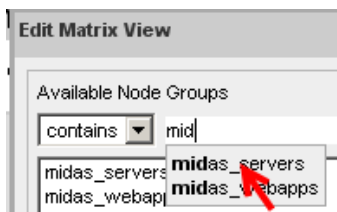
— "Multiple filters" - Sometimes it might be useful to be able to "filter the filtered result", thus applying a filter on top of another one.
For example, the first filter could be "hp" and the second filter "ia64". Such a process can be achieved by using the "lock filter" function, see Figure 104 on page 93. After entering "hp" press the "lock filter" icon. The filter field will be emptied and the filter "hp" kept in the background. Now you can enter "ia64".

To remove any filter use the unlock filter icon (Figure 104 on page 93).

— From the drop down menu, you can define what kind of filter should be used. Three options exist: contains, matches or exact filter.

Figure 104 Responsibility Matrix Filter
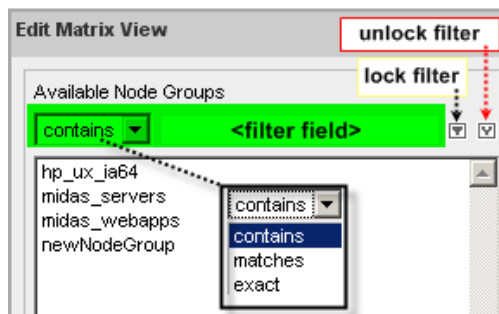
Selection Process

With or without using a filter, once you have identified group objects that should be moved in or out of the responsibility matrix, you have these options (see Figure 105 on page 94):

— use either the [<<] or the [>>] button to move ALL items displayed to the opposite window.

— If you only want to move those items you have selected (highlighted in blue), use [<] or [>] to do so.

You can select multiple items by holding the <Strg> key on your keyboard. By holding <Shift> you can select a whole range.

As soon an item is moved in such a way, it is removed from the other list.

Please note, that items which are enabled (check boxes enabled) in the responsibility matrix cannot be removed from the responsiblity matrix using the "Edit View" window.

Generally, it is possible to remove a node or message group from the responsibilty matrix in removing it from the visible column inside the edit view window. But this can only be done if none of check boxes of this node or message group is been enabled.

If one or more check boxes are enabled for a node or message group, and you remove this group from the visible section it appears inside the edit view window that this group is moved from the right to the left hand side. But as soon as you return to the responsibility matrix view, this group is still there.

Figure 105 Edit Matrix View
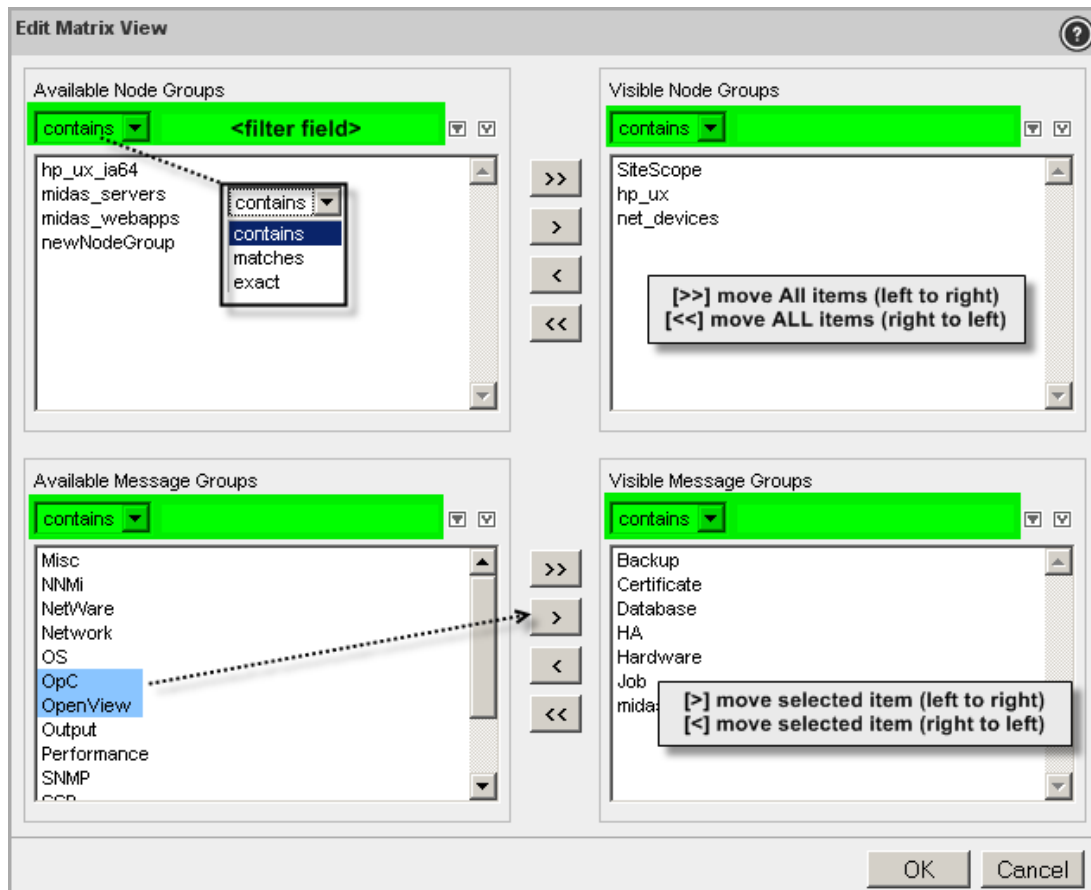
Edit Selection

EDIT SELECTIONS opens the selection editor (see), which you can use to select the combination of managed nodes and message groups to enable or disable for the currently selected user or user profile. This gives an advantage over individually clicking each required check box.

If the list of node groups or message groups is long, you can also reduce and refine the contents of the list using a filter (see above).

From the lists, select which of the node or message groups you want to enable or disable for the currently active user or user profile.

Figure 106 Selection Editor
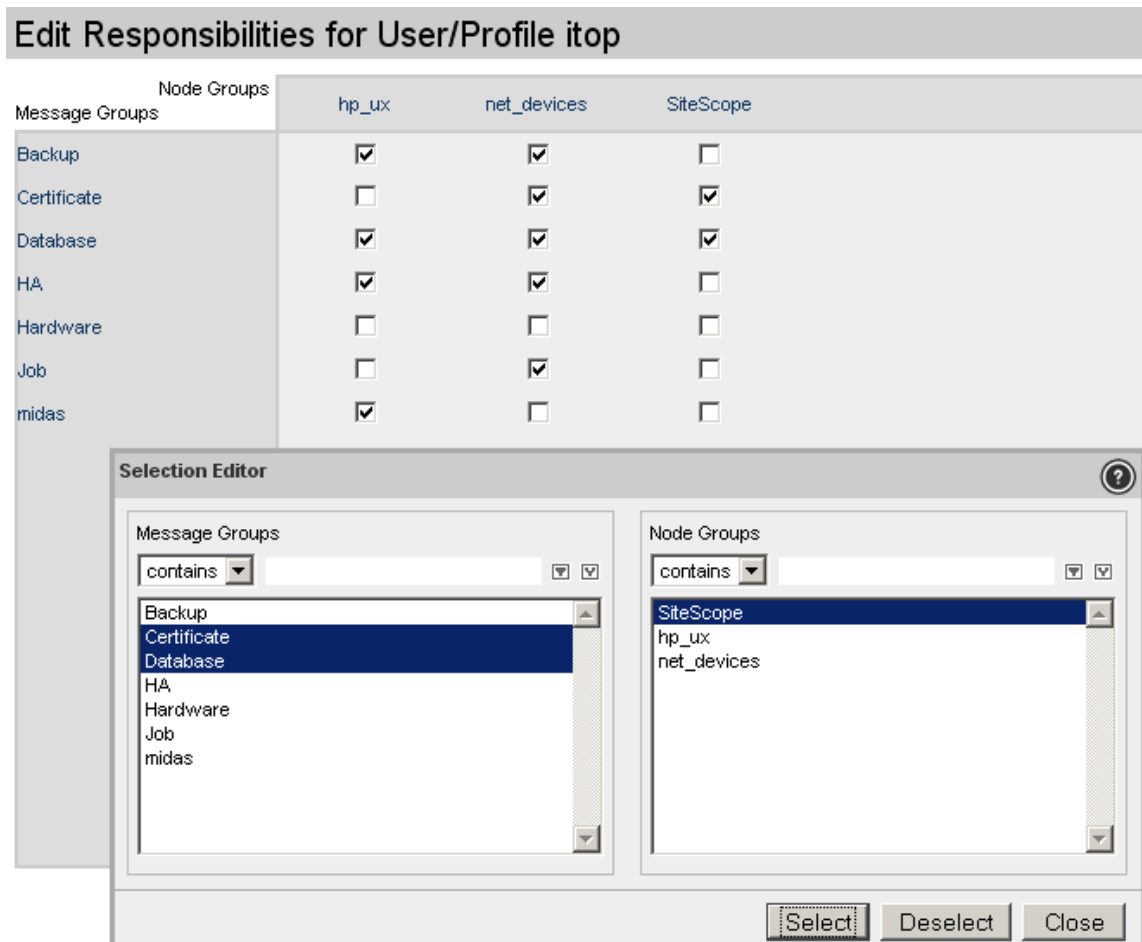
— On the left hand side you see all message groups that are available for selection in the responsibility matrix of the currently active user or user profile.

From the lists, choose the message groups that you want to enable (Select) or disable (Deselect) in the responsibility matrix.

— On the right hand side all node groups are listed that are available for selection in the responsibility matrix of the currently active user or user profile.

From the list, choose the message groups that you want to enable (Select) or disable (Deselect) in the responsibility matrix.

— SELECT - will enable (check) the selected items in the node-group or message-group column; the change is immediately applied to (and visible in) the responsibility matrix.

— DESELECT - will disable (uncheck) the selected items in the node-group or message-group column; the change is immediately applied to (and visible in) the responsibility matrix.

TIP: For quick access to the Selection Editor, for example to open the Selection Editor in the context of a specific node group or message group, right click the group you want to edit, see Figure 107 on page 96.

Figure 107 Edit Selections (Job)
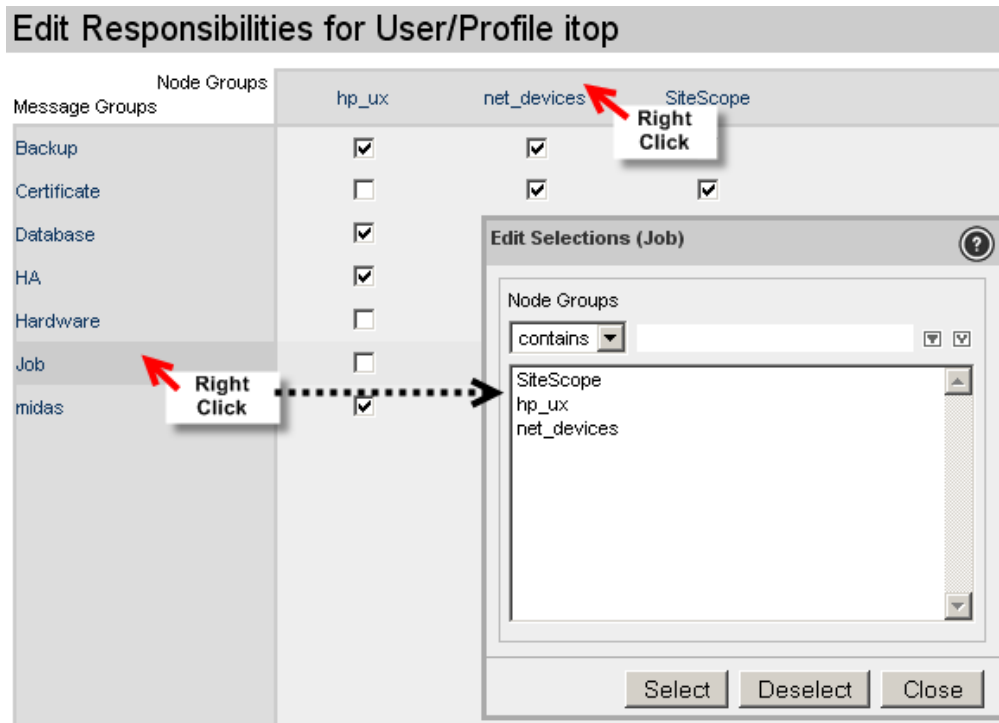
User Management in Administration UI

Overview

This section discusses the user management within Administration UI. Please notice that Administration UI users are separate from HPOM users:

- Administration UI users may work concurrently in HPOM.

- They are not HPOM operators, therefore, they have no message browser access.

- Generally Administration UI users are also HPOM administrators (unless a user is limited by read only roles). Typically access rights are based on those administrative and configuration tasks a user should perform.

- Administration UI user management can be accessed via the Toolbar Menu -> Admin icon.

User Model

The user model is based on the concept of user groups and user roles. Users must belong to user groups; the rights and responsibilities granted to members of a user group are defined in a user role, see Figure 108 on page 97. This definition in the user role defines what HPOM objects the user can see and what his user rights on these objects are.

Figure 108 Users, User Groups, User Roles
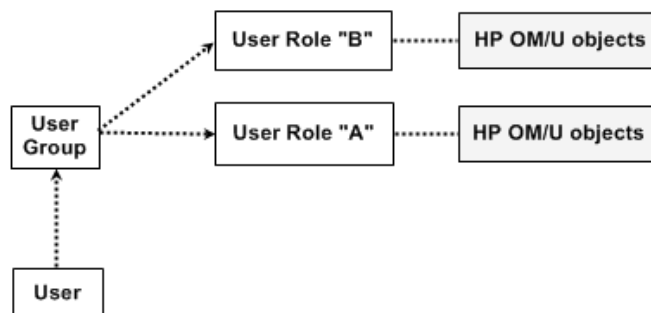
The user management is hosted on the Administration UI server itself. Its data (incl. usernames and passwords) is stored inside a local XML database. In order to get access to the Administration UI web interface each user must authenticate himself.

The authentication process can be linked to LDAP or UNIX passwd (via PAM) but currently all users also have to be setup with their username inside Administration UI. For this setup please consult the Administration UI "Administration and Configuration Guide".

Please notice, that a user who does not belong to any user group or if a user group does not have any user role assigned to it, **any login attempt of such a user will fail**.

Please notice, that you can define user roles at a global or at a more detailed level (down to the policy level). This will be discussed below.

The access rights which you can grant are either read only or all rights (add, modify, delete, assign, execute).

Those user access rights granted on a higher level will be passed on to the lower object levels, see Figure 109 on page 98. This means that if a right exists on a higher level, any user rights defined below that level will not be taken into account. For example if on a global basis a read right has been defined, then ALL HPOM objects will be readable.

Figure 109 Gobal Rights
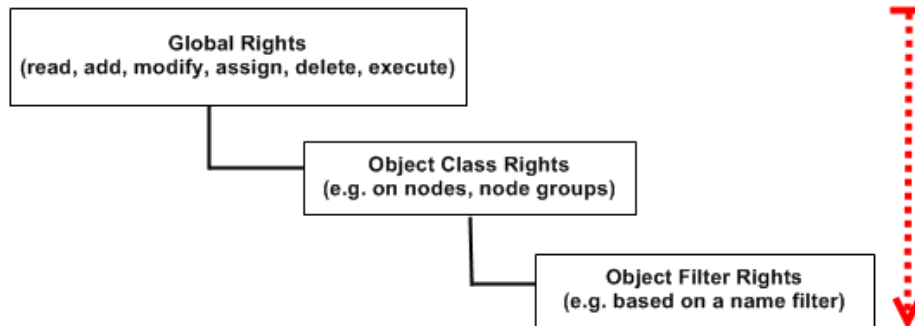
If you choose to define roles at a more detailed level, you need to be aware of the links and dependencies between the various objects in order to avoid creating problems where users have only read rights to objects which they need to modify or assign.

For example, in HPOM, there is a dependency between node groups, messages groups, and policy groups. Users who can modify node groups also need to be able to see lists of policies and message groups and, in addition, be able to assign the policies and message groups to the nodes.

Note that user rights are exclusive and cumulative, that is: users have no rights until these are explicitly granted them. Also a granted user right cannot be taken away by another user role or individual object filter. There are no "negative filters", that means it is not possible to define: This user should have full access rights, but not to policy or node group "C". This is not possible.

Configuration of Administration UI Users

To define a new user, add the user to a user group, assign user rights and responsibilities, and grant the user a login, perform the following steps:

Steps to perform:

- Design a user model which meets the requirements of your user environment, for example: database administration, node management, policy assignment, simple operators, and so on.

- Create a user role for each type of user you want to add: A user role describes a set of objects accessible (scope) and the operations (permissions) on those objects. For example: which objects are accessible on which servers, and what type of access is granted.
In order to create the user role select from the Administrative Menu: "Edit" -> "Add User Role".

  For more information about the user role editor, see the list of related topics below, see Figure 112 on page 101.

- Create a user group for each logical type of user you want to create, for example: global administrators, database administrators, policy administrators. Simply define, the user group name, label (optional) and description (optional), see Figure 110 on page 99.

Figure 110 User Group Editor

- Assign the appropriate user role to the corresponding user group; the role defines rights and responsibilities granted to users who belong to the user group.

  To do so select from the Administrative Menu: "Browse" -> "All User Groups". For the newly created user group select from its context Action Menu: "Assign roles" and select the newly created user role in order to assign it to this user group.

- Create and define a new user, including: name, label, and password, see :Figure 111 on page 100:

Figure 111 User Editor

Assign a user to a user group. Place the new user in the user group whose rights and responsibilities meet the users role best.
To do so select from the Administrative Menu: "Browse" -> "All User Groups".
Now assign your new user to the previously created user group. For this user group select from its context Action Menu: "Assign user" and select the newly created user in order to assign him/her to this user group.

User Role Editor

To define a user role should be pretty much straight forward in regard of the interface options regarding the access scope and the corresponding access rights, see Figure 112 on page 101.

- **Access scope** (HPOM objects) can be defined:

  — On a global level, for example for a universal admin user.

  — On an object class level, for example: everything that belongs to policies, policy groups, categories etc.

  — On individually filtered HPOM objects defined by their key attributes (for example name or path) or by their parent container (for example a node in a node group).

    These filters are used in conjunction with the already known dropdown menus "contains", "is" and "matches".

- **Access Rights.** Two access rights exist for each of the above mentioned objects:

  — **"Read only"** (not available where it does not make sense, for example for the deployment function or for the function "agent installation").

  — **"All rights"**. This includes depending on the HPOM object: add, modify, delete, assign or execute rights.

Please notice, that access rights on a higher level are passed on to downwards. This means if a global read right is granted, then all OMU objects will be readable, see

Therefore, if "All Rights" is granted on a global nodes, node groups, etc. level, then individual filters for these objects will be of no effect.

When creating or editing a user role, any existing inherited setting is indicated by a ticked but greyed out checkbox. This indicates that the corresponding user right is already set via a higher group based or global rights definition.

• When defining individual rules for filtered objects, it is possible to add (also multiple) single rules using the "Add new rule" button. This will add a new line where the object can be defined accordingly. Using the (X) button removes this object filter.

Figure 112 User Role Details

Node Removal

Please note, that the process to remove a node is pretty much similar to the process existing in the previous HPOM 8 version. Before the node can actually be removed several manual tasks have to be performed first. For example, acknowledge all message in the message browser, stop node heartbeat polling, etc. Please refer therefore to the main HPOM 9 guide discussing this topic.

The following items should be remembered:

*   Acknowledge all messages for the to-be-deleted node in the message browser.

*   If a node is used in some policy suppress condition it has to be deleted there as well.

*   Stop heartbeat polling (node Action Menu: "Execute Task").

*   Deinstall the agent on the target node.

*   Perform a history download of all messages for that node (node Action Menu: "Execute Task").

*   Remove all policy/policy group/node group assignments for that node.

Except the message acknowledgement, all functions are accessible via the Browse or Action Menu for each node.

Only then a node can be successfully removed via the "Delete" function. Otherwise, some node references will remain in some Oracle tables. In this instance you will receive a warning message that the node removal was not 100% successful.

8 SSH Based Agent Installation

Overview

This chapter will cover the SSH based installation of HPOM agents via the Administration UI GUI:

Introduction

The goal is to install the HPOM agent binaries onto managed nodes:

- Initiated from HPOM server
    - Actual work done by HPOM `inst.sh` script
    - „Off-line installation" is not considered
- Fresh install or update (patch install)
- Asynchronous request/response behavior
    - Purely non-interactive

HPOM always offered a method to install the agent software on a managed node. This agent installation could be triggered from the Motif GUI (HPOM 8) or from the command line – in both cases however, the „`inst.sh`" script was used..

> Administration UI also uses the „`inst.sh`" script. There are no special or independent scripts in Administration UI for that purpose. Therefore, existing limitations or well known specifics still apply.

Installing an agent can mean either a complete fresh install or an update installation (for example to install an agent patch). Both ways are supported by `inst.sh` and therefore by Administration UI as well.

Unlike the Motif GUI, Administration UI is a web-based GUI. As a result it is not easily possible to start `inst.sh` as a child process and display input/output in a terminal.

Thus, the Administration UI agent installation is purely non-interactive and works in a request/response fashion. All parameters will be collected, checked and then passed on to the `inst.sh` script. When the `inst.sh` has finished the results will be sent back to the Administration UI and saved in an agent installation log file.

SSH Based Agent Installation

It is possible to use SSH during the the agent installation. If you plan to do this, make sure that "Use SSH during installation" is enabled for these nodes.

To do so, select for a node: "Edit" (Action Menu). Inside the tab "Installation" enable the checkbox [X] Use SSH during installation.

Please remember that the following pre-requisits also have to be met:

- if necessary, generate SSH keys on the HPOM server
- for each node, connect manually once to the node and accept the host key
- copy the public key of the HPOM server to the target node
- for each node, check the connection if ok (without being asked for a password!)
- edit `/opt/OV/OMU/adminUI/conf/ovoinstall.properties` uncommenting the line:

    `ovoinstall.sshCmd = ssh -o StrictHostKeyChecking=no`

- Restart Administration UI: `# ovc –restart adminui`
- Do a test installation by using standard mode (remsh)

Agent Installation Start

The agent installation can be triggered from two locations:

- For multiple in- or de-installations. From the Administrative menu select "Deployment" -> "Agent (De)Installation" (Figure 113 on page 105)

Figure 113 Agent Installation Start
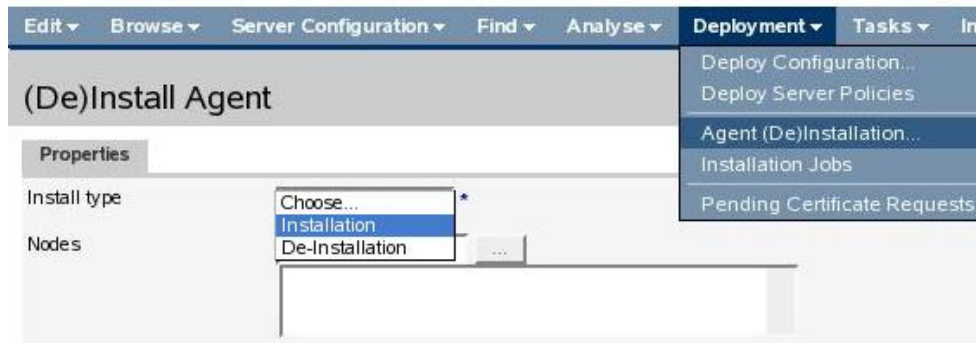
- Single context based installation. Here use the context Action Menu of a node and select: "Install Agent" (Figure 114 on page 105)

Figure 114 Context Menu Installation Start
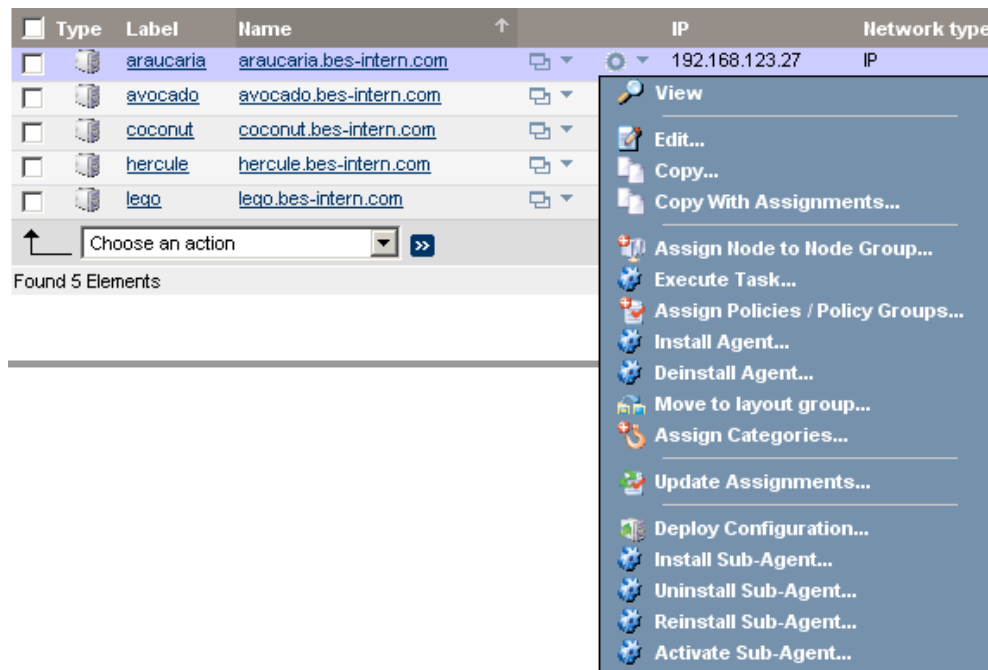
- When selecting the global menu "Deployment" -> "Agent (De)Installation" the first step is to choose the installation mode – installation or de-installation.

- Secondly, press the browse button and select the set of target nodes from the selector as shown below (Figure 115 on page 106). Node names may also be typed into the text field left of the "..." browse button, however the name must be literally identical to the primary host name as configured in HPOM (there is no name resolution!).

Figure 115 Selection of Target Node(s)
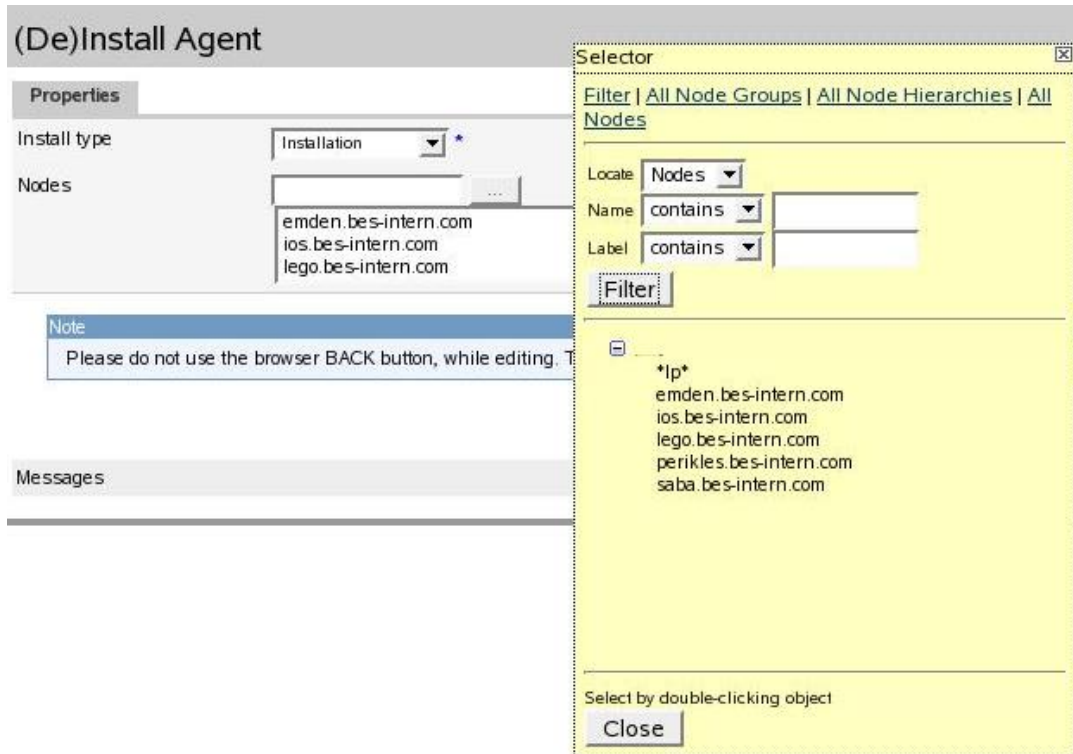
Select as many nodes as needed and press "Close" to close the selector window. After that please click the "Preinstall check" button to start the prerequisites analysis. This analysis may run a while and will validate all selected nodes.

Pre-Install Check Result

When the prerequisites analysis is complete, the list of target nodes is displayed as shown in the example below (Figure 116 on page 107). Please check for each node the analysis result. The important columns are:

- **Status**. This can indicate:
  - *ready* (all prerequisites are fulfilled, installation may proceed)
  - *invalid* (some error occurred; an installation is not possible)
  - *passwdrequired* (prerequisites OK, but installation method requires a password, which has to be entered manually in the text field at the very right)
- **Method**. Lists the installation method, which either
  - SSH (expressesly configured), see SSH Based Agent Installation on page 104.
  - Has been discovered as applicable (*local*, *HTTPS*, *standard*) or if an error has occurred (*invalid*).
- **Comment**. Lists the reason of each status result. A click on the "?" will display more information.

More details can be found below.

Nodes, which have been considered as installable, are automatically selected on the very left. If desired, individual nodes may be manually deselected to exclude them from the actual installation. Nodes, where an error occurred during the prerequisites check, are automatically deselected and cannot be selected.

If required, enter a password. In order to re-install an existing agent, enable the checkbox "Force". This value will be passed on to the `inst.sh` script..

Only nodes passing the analysis phase can be installed!

If no nodes at all have been found as installable, the "Install ..." button will be greyed out and disabled.

Figure 116 Pre-Install Check Results

Main Installation Phase

After clicking the "Install ..." button, Administration UI will generate a parameter file for *each* selected node and execute the `inst.sh` script with these parameter files. The actual installation may take a long time. Therefore, Administration UI performs this operation asynchronously in the background in order to avoid communication timeouts.

The output of the `inst.sh` script will be captured and stored in the Administration UI BackEnd module (on the HPOM server) and can be reviewed later by following the link as shown in Figure 117 on page 108 below.
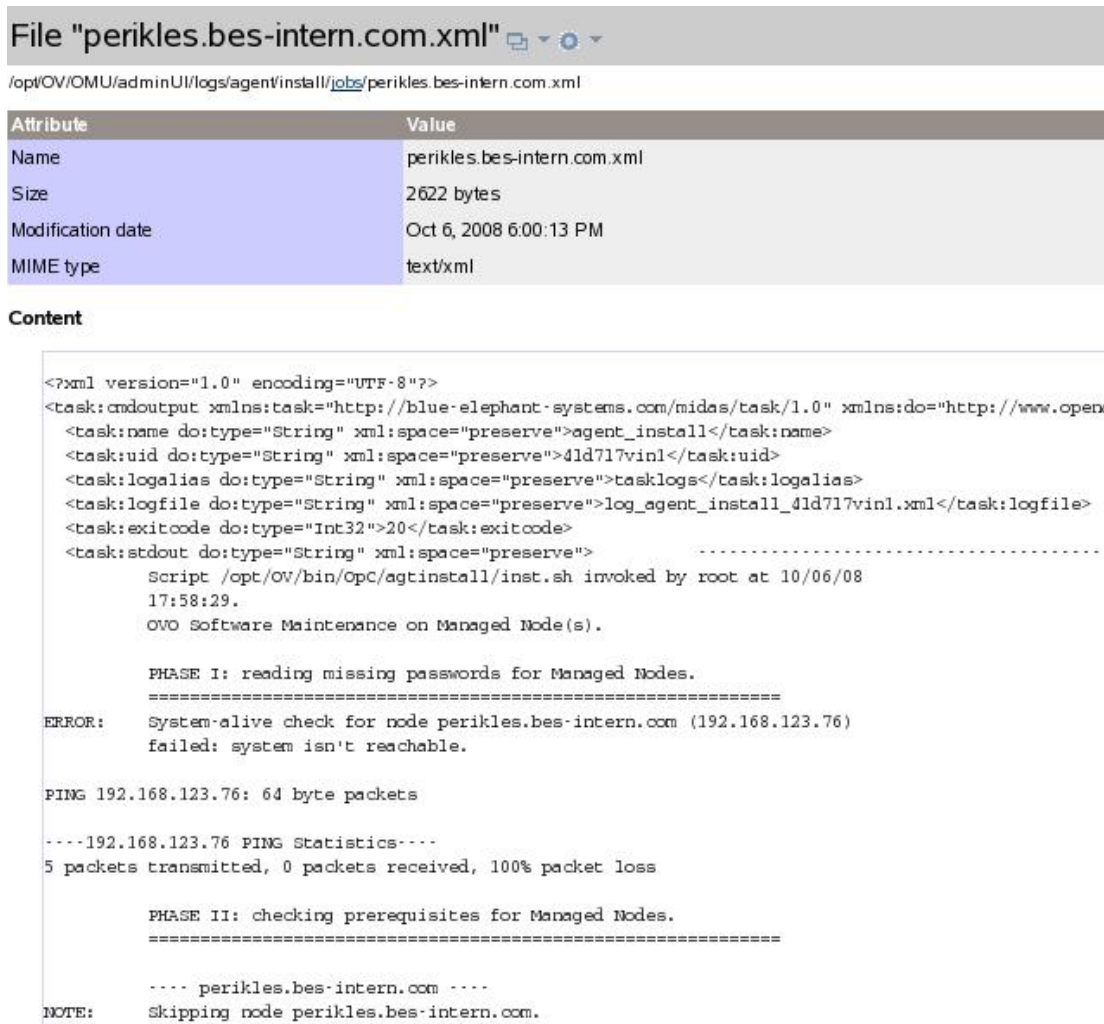
Figure 117 Installation Phase
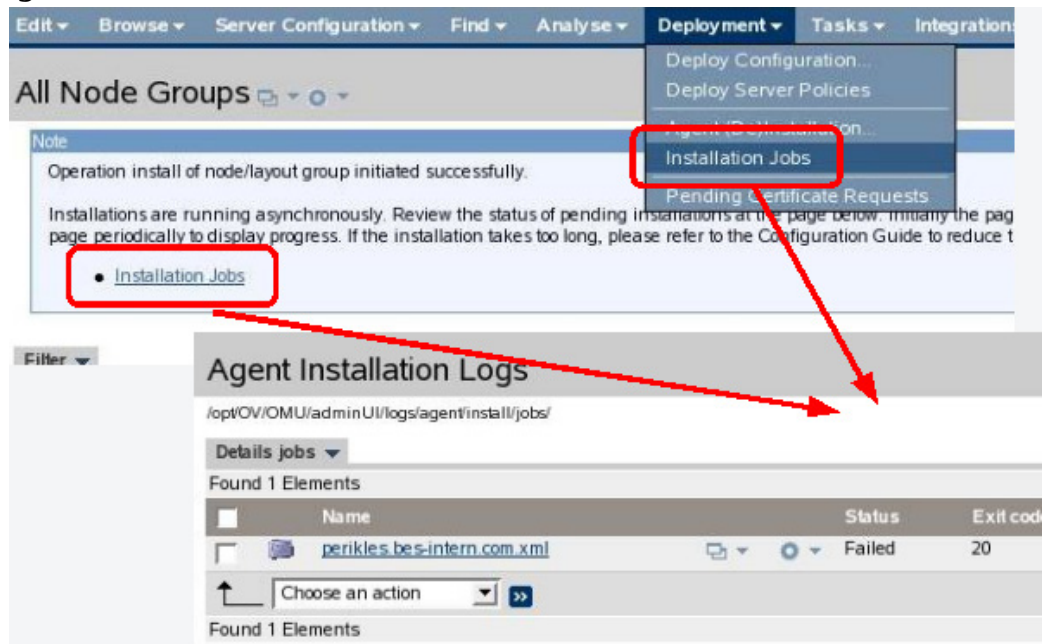
	The installation takes place in a sequence (one node after the other as `inst.sh` cannot run concurrently multiple times) and may take a long time. Hence, the installation logs will appear one after another over time. Please refresh the log file view every now and then.

Installation Log

The content of the installation log is written by HPOM `inst.sh`. Review this output whether the actual agent installation was successful or not (Example Figure 118 on page 109). In the example the node "perikles" isn't reachable.

In the Administration UI overview page, an exit code of zero is considered as successful.

Figure 118 Installation Log

Details About Pre-Installation Analysis

The flowchart below describes the steps performed during the prerequisites analysis for each node. The resulting states and methods are explained further down below.

The commands stated are executed as sub-processes of the Administration UI BackEnd server on the HPOM server. The output of the command can be viewed in the prerequisite analysis results list.

The SSH and ICMP ping commands are partially configurable through the Administration UI property file (its contents will be explained later):

```
# /opt/OV/OMU/adminUI/conf/ovoinstall.properties
```

Essentially these are the same tests which are also performed by the `inst.sh` script before actually starting the agent installation.

Method - Installation Method

When the prerequisites analysis is finished, the resulting installation method is shown. Please consult the flowchart (Figure 119 on page 111) indicating under which circumstances the corresponding method has been determined.

The "standard" method represents the "classic" FTP/rexec based communication, which actually has not been verified – it only remains as the only possibly method after all other options have turned out as inappropriate. This standard method actually may also involve a rhosts-based RCP.

> The status and method values do not guarantee, that the installation will succeed but rather represent a best-effort prerequisites check to identify typical problems at the very beginning.

Possible values:

- "***local***" – Applies to local HPOM server only.
- "***HTTPS***" - A remote HTTPS HPOM agent could be contacted and the HPOM built-in HTTPS communication will be used.
- "***SSH***" - SSH installation is configured for this node.
- "***standard***" - Traditional FTP/rexec communication will be attempted.
- "***invalid***" - An error occurred, check "comment" column.

Figure 119 Pre-Installation Analysis Flowchart
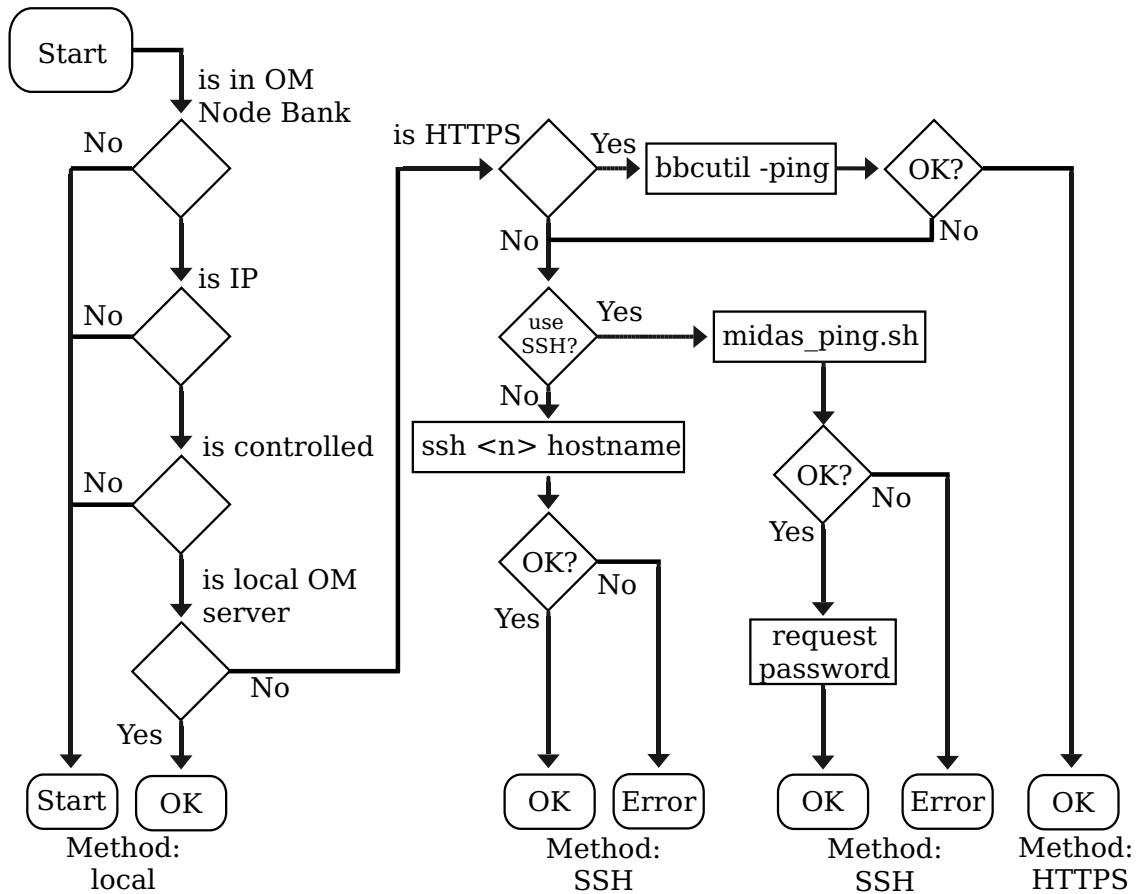
Comment - States / Error Codes

- Possible error codes:
    - "***nosuchnode***" - Node is not found at all or not the IP.
    - "***notcontrolled***" - Node is a member of HPOM NodeBank but it is not set as "controlled".
    - "***sshnopubkey***" - SSH installation requested, but key-based SSH failed (exit non-zero).
    - "***pingfailed***" - Node is not reachable via ICMP.
- Click on the "**?**" question mark to obtain more details.
- Not an error is:
    - "***passwdrequired***" - FTP/rexec method detected, needs password.

Details will be discussed in the next sections.

Details SSH

- SSH is purely non-interactive.
  - Public-key based access to target node must be possible!
    - There is no way to pass the password to the SSH command.
    - Key may have a passphrase. If this is the case it must be registered with SSH-add to environment of Administration UI server.
    - An automatic initial host key acceptance is possible.
- Local user is root, remote user configurable as HPOM node attribute.
- Administration UI DEBUG mode also runs SSH in verbose mode, see Administration UI logs for output.

Unlike FTP or RCP/REXEC, SSH is still considered as an acceptable communication method and is therefore particularly important as an agent installation method. Therefore, here some specific details.

There is no way to pass a password to the SSH command via command line or parameters. Because of that, the only possible authentication method is public-key based. This requires that

- The host key of the target node must be present in the SSH "known_hosts" file locally (on the HPOM server). To accomplish this, either
  - Manually execute the SSH command and confirm the host key.
  - Configure the SSH command to automatically accept new host keys. This configuration can be done globally, per user (root) or for Administration UI only. The last is recommended and explained later.
- The public key of the local (HPOM server) user "root" must be added to the SSH "authorized_keys" file of the installation user configured for that node (usually root) on the target node.

The local key of the user root on the HPOM server may be protected by a passphrase. To make this passphrase available to the Administration UI BackEnd server process (which will effectively start the SSH command as sub-process), use the SSH-add command to register the passphrase with the SSH-agent. The Administration UI BackEnd server process must inherit some environment variables pointing it to the SSH-agent. This can be accomplished by starting an SSH-agent process during OS boot (or any time before starting the Administration UI BackEnd server) and write the printed environment variables into the file `.../ssh.env`, for example:

```
# ssh-agent -s > /opt/OV/OMU/adminUI/ssh.env
# cat /opt/OV/OMU/adminUI/ssh.env
SSH_AUTH_SOCK=/tmp/ssh-DJBhmN5478/agent.5478; export SSH_AUTH_SOCK;
SSH_AGENT_PID=5479; export SSH_AGENT_PID;
```

Then, at any time later on the command line, pass on the passphrase to the ssh-agent:

```
# ssh-add
Enter passphrase for /.root/.ssh/id_dsa:
Identity added: /.root/.ssh/id_dsa (/.root/.ssh/id_dsa)
```

In case of problems, review the following section which gives some troubleshooting instructions.

Troubleshooting SSH

Please remember the following SSH points:

- SSH key must be locally stored in ~root/.ssh/known_hosts.

  — Associated with hostname as typed in with SSH command.

  — Short and long host names NOT identical (neither IP address).

- Check configurable with SSH option.

SSH expects that the host key of the remote host has to be confirmed once – normally on the command line this looks as shown in the example below (Figure 120 on page 113).

Figure 120

Since Administration UI does not run interactively, nobody can confirm the host key. Thus, the host key confirmation has to be accomplished some other way. There are two possibilities:

- Somebody has to manually do a # `ssh root@targetnode` on the command line and confirm the remote host key. This has to be done once before attempting the Administration UI-based agent installation. Watch out for the problem with the host names illustrated in the example above: different host names representing the same node are not considered as identical by the SSH command!

- Administration UI can be configured to automatically accept remote host keys by always specifying the `StrictHostKeyChecking=no` option. Instructions how to configure this are presented later.

Locking

- Concurrent usage is not possible (see)

    — Administration UI lock protects deployment view

    — HPOM `inst.sh` locks execution of script

The regular Administration UI locking mechanism is implemented to prevent multiple users from opening the agent installation view at the same time. In addition, the HPOM `inst.sh` script maintains a lock file which guarantees, that only *one* instance of `inst.sh` executes at a time.

The HPOM lock is normally removed by `inst.sh` unless the `inst.sh` script has been killed with SIGKILL (signal 9) or has crashed – then the lock file remains and subsequent executions of `inst.sh` will fail because of the (wrong) assumption that `inst.sh` is still running. To remedy such a situation, Administration UI presents the view shown in the example below () and offers the user three choices:

- **Cancel** entirely

- **Refresh** to retry testing the HPOM lock file. For example, if the `inst.sh` script has been started 5 min. ago, this option might be appropriate.

- **Ignore**/Break lock and continue. This may be appropriate if the lock is older than a certain time (lets say 1h) and/or no `inst.sh` process is running anymore – then, most likely the lock just has not been cleaned up properly.

Figure 121 Locking
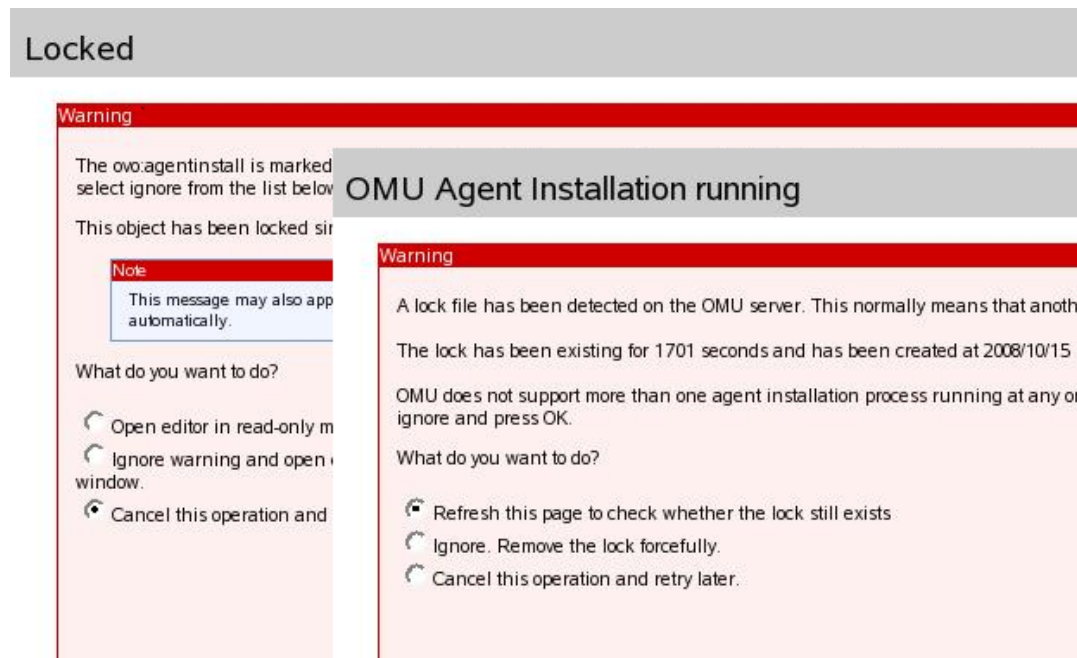
Configuration & Tuning

To adapt the behavior of SSH and ICMP ping executed during the prerequisites analysis phase, configure the properties as shown below.

- SSH and ICMP ping are configurable. In order to do so, please edit:

```
# /opt/OV/OMU/adminUI/conf/ovoinstall.properties

[...]
# Local SSH command to check SSH access in pre-install phase:
# ovoinstall.sshCmd=ssh

# Command executed remotely by SSH:
# ovoinstall.sshCmdRem=hostname

# Local command to ping node in pre-install phase:
# ovoinstall.pingCmd=midas_ping.sh
```

The "sshCmd" property can be used to configure the exact command executed to test SSH connectivity. For example, a full path may be specified or additional options. The latter may be necessary to enable automatic host key acceptance – this can be accomplished by configuring:

```
ovoinstall.sshCmd = ssh -o StrictHostKeyChecking=no
```

The property "sshCmdRem" can be used to change the command executed remotely. By default this is hostname, but any other remote command can be configured like echo 123 or date, etc. The only requirement is that upon success, the exit code of the command must be zero.

During runtime, the actual SSH command is:

```
<sshCmd> <debug options> -l root -o BatchMode=yes <target node> <sshCmdRem>
```

where `<sshCmd>` and `<sshCmdRem>` are substituted by the properties specified above, `<debug options>` is empty normally or "-v -v -v" in DEBUG mode, and `<target node>` is the primary host name (as configured in HPOM) of the target node.

To enable ICMP please remove the # in front of this line, so it becomes:

```
ovoinstall.pingCmd=midas_ping.sh
```

- The ICMP ping behavior itself can be customized in the following file:

```
/opt/OV/OMU/adminUI/bin/midas_ping.sh
```

For example, directly exit 0 for no ping at all. The ICMP test will be done normally by executing the command `midas_ping.sh` with the target host name. The `midas_ping.sh` command is a small wrapper script to deal with platform-specific flavors of the ping command. If needed, the script can be customized to change the ping behavior. For example, if no ICMP ping is desired at all, just make the script exit zero directly.

Troubleshooting

- In the prerequisites analysis phase please:
  - — Review output of pre-check command (click "?" question mark).
  - — Set Administration UI to DEBUG mode (especially for SSH).
- During the agent installation phase please:
  - — Review generated parameter file.
  - — Review installation log file (output of `inst.sh`).
  - — Run inst.sh manually.

In case of problems, perform the steps described above. Depending on the installation phase, the appropriate steps differ.

Note that the actually installation always invokes the `inst.sh` script. If the prerequisites analysis has succeeded, a parameter file will be generated and passed on to the `inst.sh` script. If the actual installation still fails, the HPOM `inst.sh` script should print diagnostic output which will be captured and can be reviewed in the installation log files.

Setting the prerequisites analysis phase to DEBUG mode can be done by editing:

```
/opt/OV/OMU/adminUI/conf/log4j.xml
```

Change the log level to DEBUG in the following section:

```
<logger name="com.bes.ovo.comp.install" additivity="false">
 <level value="DEBUG"/>
 <appender-ref ref="ovo"/>
</logger>
```

No restart of the Administration UI software is necessary. 30-40 sec. after the modification, DEBUG logging will be enabled. Then, after testing, review the log file

```
/opt/OV/OMU/adminUI/log/ovo.log
```
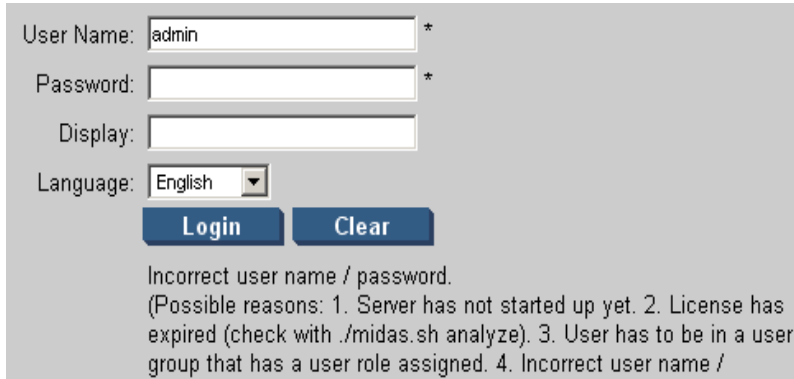
Particularly for SSH-based nodes, the SSH command executed during the pre-install phase, will run in verbose mode and generate detailed diagnostic output.

9 Login Problems

Help, I cannot login!

If the correct web interface shows up, but your login and password is rejected, that as a result you receive the following error message (Figure 122 on page 117), please try the troubleshooting tips (listed below) first:

Figure 122 Login Error

In case you are *not* presented with the main web interface in Figure 123 on page 117, but see some other error screen or some sort of directory listing, please consult the Administration UI Installation Guide chapter "Installation Troubleshooting"-> "Web Interface Problems" for further advice.
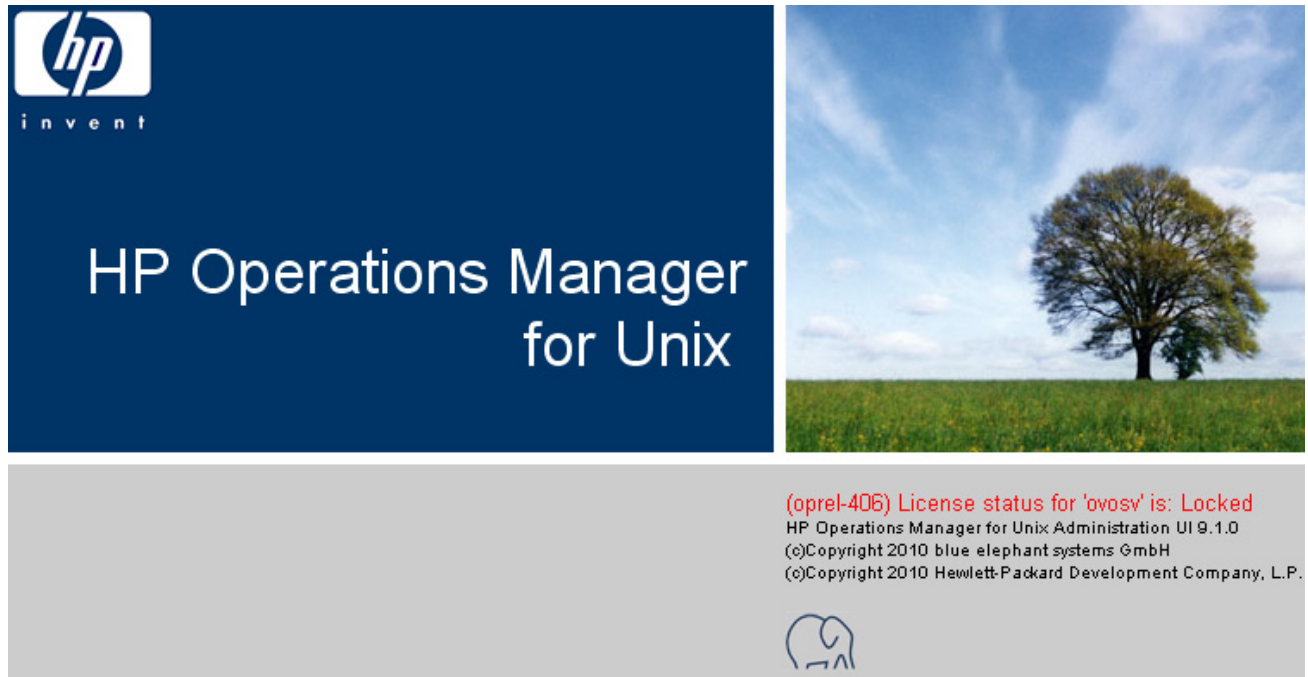
Figure 123 Login Screen

Another possibility is an expired HPOM 9 license password. If a problem exists here, a warning will be displayed. The login fields will be not shown (Figure 124 on page 118).

Figure 124 License Status Warning

Please check the OM 9 license password, for example via:

```
# ovolicense -s -p HPOM
```

or

```
# ovolicense -s -p HPOM | grep ovosv | grep -i critical; \
/opt/OV/bin/ovolicense -s -p HPOM | grep ovosv | grep -i locked
```

Here it is required to install a valid HPOM license password. In order to install a new license you can for example use the GUI by executing:

```
# JAVA_HOME=/opt/OV/nonOV/jre/b
# export JAVA_HOME
# /opt/OV/bin/ovolicense -gui -a HPOM
```

Currently it is required, to perform a restart of Administration UI after the license update:

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

Note: If you still receive the warning message "(oprel-406) License status for 'ovosv' is: Locked" you should delete your browser cache, or try to do a force reload of the webpage:

- Firefox: <SHIFT> # <F5>

- Internet Explorer: <F5>

It is also possible if a proxy is used, that this still displays the old webpage.

Login Troubleshooting Tips

Generally there are five possible explanations for a login problem:

- If the Administration UI has been restarted a few moments ago, all components might no be fully running yet. Although you can see the login web interface, the Administration UI XML user database will generally take longer to start.
  Solution: Please wait for another 30-120sec before you try to login again.

  There should be no more logging activity inside `/opt/OV/OMU/adminUI/logs/servicemix.log`.

  If a user tries to log into the WebApp too soon, the following typical error codes can be found inside `servicemix.log`:

  ```
  [...]
  ERROR - 2009-08-06 08:17:38,825 | BaseLifeCycle.onMessageExchange(48)
  | Error processing exchange InOnly[
    id: ID:192.168.123.110-122ee5aef40-4:2
    status: Active
    role: provider
    service: {http://blue-elephant-systems.com/midas/servicemix/
  1.0}audit-listeners
    endpoint: backend
  [...]
  javax.jbi.messaging.MessagingException: Could not find route for
  exchange: InOnly[
    id: ID:192.168.123.110-122ee5aef40-4:6
    status: Active
    role: provider
  [...]
  service: {http://blue-elephant-systems.com/midas/servicemix/
  1.0}custom-audit-list
  [...]
  ERROR - 2009-08-06 08:17:38,932 | BaseLifeCycle.onMessageExchange(48)
  | Error processing exchange InOnly[
    id: ID:192.168.123.110-122ee5aef40-4:10
    status: Active
    role: provider
    service: {http://blue-elephant-systems.com/midas/servicemix/
  1.0}global-list
  [...]
  ```

  These messages indicate that the users, user groups and user roles which define the access rights could not be read yet.

- Another possibility is that the user is in no user group or that this user group does not have a user role inside Administration UI assigned.
  Solution: try another user login, e.g. the main Administration UI user "admin" in order to validate if the login process is generally broken or not.

- In case the previous tips do not help a file corruption might exist, preventing some modules to start up successfully.
  Solution: Perform a "clean" restart of the application itself, using the following command:

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

This will restart the application performing a cleanup of all log and run-time files, forcing the application to unpack all necessary run-time files again.

> Please make sure no other users are logged in and working inside the Administration UI before you restart the application like this! Otherwise their current work might be lost.

- If a "clean" restart also does not help it might be possible that a rare case of corruption of the XML database exists.
  Solution: Please create a backup of the Administration UI configuration including the XMLDB, using

  ```
  # /opt/OV/OMU/adminUI/adminui save
  ```

  Additionally also create a "support zip" containing all Administration UI configuration and log files. Use the following command:

  ```
  # /opt/OV/OMU/adminUI/adminui support
  ```

  Please forward both zip file packages to Support explaining your problems so they can analyze the XMLDB files for any problems.

- Note: Details on the `save` and `support` command can be found here:
  - Save & Reload on page 40
  - Support.zip on page 40

- If the XMLDB with the user database wasn't successfully initialized during the installation, the user and its role might be missing, therefore, any login will fail.

> **Please note, that the following command is ONLY recommended after a fresh installation of the Administration UI software if a login isn't working at all.**

The recommended command to fix this behavior will perform a complete reset of the XML database. **Therefore, all users and user roles will be lost!**

```
# /opt/OV/OMU/adminUI/adminui init force
```

No restart of Administration UI is necessary. After the command has completed successfully it is possible to login with the default user (login) and password (secret).