HP Operations Manager for UNIX 9.10

for the UNIX operating system

Administration UI

Software Version: 9.1.0

Installation Guide

Document Release Date: August 2010
Software Release Date: August 2010

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2009-2010 Hewlett-Packard Development Company, L.P.

© Copyright 2009-2010 blue elephant systems, GmbH

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

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)

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 blank page)

1 Introduction

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 document provides information about the installation, basic configuration and lists some basic troubleshooting information of Administration UI. See also the Administration UI “Administration and Configuration Guide”, “User Guide”, as well as the online help, particularly for all aspects of actually using the product.

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

The Operations Manager Patch Overview can be found here:

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

2 Installing Administration UI

Overview

This chapter describes the necessary installation prerequisites.

It will guide you through all installation steps and finally show you how to access and verify the installation of Administration UI.

Especially if you are in a hurry, please make sure to check that all the installation requirements are met. Furthermore, you could use (though it is not recommended) the Installation Protocol (see below) also as an installation checklist in a nutshell.

In case you are faced with installation problems, for example when launching the Administration UI or after the installation has finished, you can find troubleshooting information in the following chapter:

- Installation Troubleshooting on page 41

In order to get Administration UI successfully installed, the topics below should help you:

- Installation Prerequisites on page 4
- Technical Requirements on page 8
- Installation Protocol Administration UI on page 13
- Overview on Installation Steps on page 12
- Starting the Administration UI Installer on page 14
- Installing the Software on page 16
- Testing and Verifying the Installation on page 31

Installation Prerequisites

This section explains the checks you have to perform to ensure that the Administration UI can be installed successfully. For example it is vital to obtain the correct passwords and Oracle configuration settings.

HA CLUSTER: The information in this section applies to all types of installation of Administration UI. If you are installing Administration UI on a system that is configured in a high-availability (HA) environment, make sure you review chapter Installing in a Cluster on page 37 **before** starting the installation.

Please note, that installers **cannot** be used for version updates!

To update an existing version of Administration UI (for example 9.1.0 to 9.1.1) please apply the latest available patch using the `patch` sub-command. Please refer to the main Configuration and Administration Guide for details.

HPOM needs to be up and running on the HPOM Management server.

Make sure that on the target server, where you want to install Administration UI, it is possible to export the display. The required X libraries need to be installed.

The information in this section covers the following topics:

Previous Configuration Value Pack (CVP) Version

An upgrade from CVP 3.x to Administration UI is **not** supported. Instead you need to remove the existing CVP 3.x software and install Administration UI after that.

Passwords

Before starting to install Administration UI, please make sure that you have access to the following password:

- HPOM Oracle database user

  The Administration UI installer suggests by default to use the user “opc_op”. But it is also possible, for example to use the user “opc_report”.

  Any Oracle user with read-only access to the HPOM database objects can be used. Both opc_op and opc_report users who are created during the HPOM server installation fulfill this requirement. The user opc_op even has write capabilities. But these are not needed for Administration UI.

Please note, that Oracle 11g uses by default password aging. Passwords (for example for the opc_op user) will expire after 6 months!

If the password of the Oracle user opc_op expires, the HPOM processes & Administration UI are no longer able to connect to the database!

For details please see the Administration UI Administration & Configuration Guide section “Oracle 11 Password Aging”.

OMU 8 with Oracle 10.2.0 doesn't have an expiry date.

TIP: If you do not know a password, see chapter “Wrong or Unknown HPOM Passwords on page 42“ for information about how to determine, verify or if necessary how to change it.

Java Runtime

The Administration UI installer includes for convenience reasons a bundled JDK version 1.6.

Please note, that for future JDK DST changes or JDK hotfixes you need to update the JDK in Administration UI yourself. These JDK updates or hotfixes will not be included in any Administration UI patch.

For details please refer to chapter External Software: DST – Daylight Saving Time Patches on page 67.

Solaris Zones

The installation of Administration UI is generally supported on Solaris whole-root non-global zone.

Please note, that in some rare cases the startup of Administration UI might fail. The error recorded in the

```
#/opt/OV/OMU/adminUI/logs/wrapper.log
```

shows the following error message

```
[...]
INFO | jvm 1 | 2009/09/11 11:43:01 | java.net.SocketException: Address already in use
[...]
```

As a result the whole startup process fails and the user will not be able to see the web-interface of Administration UI after the installation has completed.

In order to fix the installation it is possible to update three binary files manually after the installation has finished.

Please refer to section Solaris Zone Wrapper Problem on page 57 for the download location of these binary files which need to be updated and on details on the update process.

Generally there should be no problems. The above error was recorded once during the beta testing phase of Administration UI.

Oracle HPOM Database Settings

It is essential that the correct Oracle access parameters are provided during the installation of Administration UI, for example the (cluster) hostname, port, database name, etc.; also check whether secure Oracle communication is used or not.

Otherwise, the connection to the HPOM Oracle database will **not** be successful.

To verify the Oracle parameters of your HP management server, you can use, for example the following two commands. Also check that the `$ORACLE_HOME` environment variable is set correctly:

```
$ORACLE_HOME/bin/tnsping <oracle_server>
```

The output could look like this:

```
[...](DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=kotao.bes-intern.com))(
ADDRESS=(PROTOCOL=TCP)(HOST=192.168.123.123)(PORT=1521)))
```

or

```
$ORACLE_HOME/bin/lsnrctl status
```

On the Oracle database server itself, the command `lsnrctl status` should produce an output like this:

```
bash-3.1# $ORACLE_HOME/bin/lsnrctl status
Alias                     LISTENER
Version                   TNSLSNR for HPUX: Version 11.1.0.7.0 -
Production
Start Date                17-APR-2009 20:36:26
Uptime                    9 days 2 hr. 17 min. 32 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File   /opt/oracle/product/11.1.0.6/network/admin/
listener.ora
Listener Log File         /opt/oracle/diag/tnslsnr/avocado/listener/
alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=openview)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=avocado.bes-intern.com)
(PORT=1521)))
```

(PROTOCOL=TCP) stands for unencrypted communication.
(PROTOCOL=IPC) indicates that an encrypted (secure) Oracle connection is used.

If IPC and TCP are both used we recommend to configure Administration UI in such a way that it uses an unsecure Oracle connection, as it would be possible with the output in the last example.

Further details to the Oracle configuration will be given further down below.

Technical Requirements

This section describes the technical requirements for the HPOM target server on which the Administration UI will be installed.

Hardware

Administration UI for OMU supports Itanium IA64 and Sun SPARC architecture. whereas Administration UI for OML supports Intel and AMD processors on x64 architecture.

Table 1 on page 8 lists the minimum requirements that the target systems should satisfy for running the Administration UI.
The amount of RAM listed below is not the total amount of memory of the HPOM server, but the amount that should be exclusively available to Administration UI.

Table 1 Disk- and Memory Requirements

Memory	Administration UI
Disk	1100MB in target installation directory `/opt/OV/OMU/adminUI/`
Disk	2000MB temporary disk space in `/tmp` or some other location (needed temporarily during the installation of Administration UI only). The temporary diskspace needed is 4 x size of the installer binary. For example: 3x 515mb=2060mb.
RAM	1024MB

Demand on system resources depends on the size and scale of the managed environment. For details please see the Administration UI “Performance and Scalability Guide”.

Operating-System

Table 2 on page 9 shows which hardware platforms, operating systems, and high-availability software is supported with the current Administration UI release. The columns OMx <#> show which versions of HPOM (and on what operating-system version or with what high-availability software) the Administration UI BackEnd supports.

Table 2 Operating-System Support

Operating System	OMU, OMS, OML 9
Management Server on HP-UX Itanium on HP Integrity	11.31 (11iv3) and later **base_pagesize=4 must be set and cannot be changed (default setting)! Other settings will not be supported by Administration UI.**
Management Server on Solaris SPARC	10
Management Server on Red Hat	RHEL 5.2, 5.3
MC ServiceGuard for HP-UX	11.18 (incl. support for campus clusters)
Veritas Cluster for Solaris	5.0
Sun Cluster	3.2
Red Hat Cluster Support	version included in RHEL 5.2, 5.3

All HPOM 9.0 releases are supported in conjunction with Oracle software version 11.1.0.7 as supported by HP for each HPOM release. Oracle's Real Application Cluster (RAC) is currently not supported. In order to support Oracle RAC some post installation configuration adjustments have to be performed. Please refer to section Oracle RAC Cluster Support on page 58 for all details.

It is recommended also to check the current HPOM 8/9 SUMA (support matrix): http://support.openview.hp.com/selfsolve/document/KM323488

Operating-System Patches

- As a general rule of thumb, make sure that the system you want to use for the installation meets all the hardware and software requirements of HPOM and Oracle as described in the HPOM documentation.
- Furthermore, all latest operating-system patches especially for the Java Virtual Machine (JVM) should be present.
- **Important**: Make sure that the following UTF-8 locale is installed on your system:

  en_US.UTF-8

  Please note, that the en_US.UTF-8 locale must be installed also if other UTF-8 locales are already installed!
- There are currently no OS Patches/Hotfixes required by the Administration UI in addition to those already needed by the HPOM server software itself.

Software on User Workstation

The following software details should be observed in regard of the end users workstation.

Web Browser Support

Administration UI uses a GUI which can be accessed by any standard web browser from the user's workstation.

The following web browsers have been tested and are supported:

- Microsoft Internet Explorer 7 and later.
- Internet Explorer on CITRIX is **not** supported!
- Mozilla Firefox 1.5, 2.x, 3.x.

Older browser versions such as Mozilla before 1.0 are not supported; these older browsers are known to have problems with incomplete or incorrect implementations of CSS and other technologies used.

X-Server

The Administration UI installer is a GUI based installer. For the installation it is necessary that the DISPLAY of the HPOM server is exported to your workstation.

As of April 2009 the following Windows based X-Servers versions are confirmed to work correctly with the Administration UI installer:

- X-Ming v.6.9.0.31
- Exceed v.13.0.0.22
- Reflection X v.14.0.5

Other versions have not been tested and are not supported. If there are problems it is recommended to start XDMCP and get a CDE desktop onto your PC and start the installation from there.

For UNIX-based workstations the same rules apply.

Verify the correct X-Window setting using a regular X-based program, for example xclock. The application must show up on your workstation display correctly.

JRE

JRE 5 or 6 needs to be present on the user’s workstation.

Overview on Installation Steps

To install Administration UI, you have to perform the following high-level steps, which are explained in detail in the subsequent sections:

NOTE: If Administration UI is installed in a cluster environment, please read first Chapter 5, Installing in a Cluster.

1. Login as root user and mount the product media or copy the installer image to the HPOM target system. Have 1250MB of temporary disk space available for unpacking the installation software.

   IMPORTANT: If you are installing Administration UI on a remote system, you will need to set and export the DISPLAY variable to your own workstation.

2. Define a temporary directory to which the installer can be extracted.

3. Start the installer program that matches the operating system installed on the HPOM target system.

4. Configure the Administration UI server:
   - Define whether HPOM or Oracle will run as HA cluster applications.
   - Define the HPOM and Oracle (cluster) hostname(s).
   - Oracle database configuration for HPOM.
   - Administration UI port configuration.

5. Review the pre-installation summary of port numbers, server names, disk space.

6. Execute the automatic installation of the Administration UI software

The installer will attempt to determine most parameters by itself and, in most cases, it should be sufficient to confirm the provided default values. However, please review the parameters to make sure that they are correct!

Please note, that the installer is not able to determine all values automatically; you will have to provide values for passwords manually during the course of the installation.

If you enter an incorrect value for an important parameter and need to change the parameter value later. All values can also be modified after the installation has completed.

Installation Protocol Administration UI

In order to prepare and track the installation of the Administration UI software you can use the protocol (or checklist) below. This protocol also summarizes all important configuration tasks:

- On the HPOM server: login as 'root' & export DISPLAY if needed
- make sure /tmp has at least 1250mb of free disk space. Calculate 3 x size of the installer binary:
  Define a temp directory to which the installer can be temporarily extracted:

  ```
  # export IATEMPDIR=/directory/with/enough/space
  ```
- Start the Administration UI installer: `#./install.bin`
- Introduction and Context Help informational screens will be shown
- **HA Cluster**: Is HPOM and/or Oracle running in a HA cluster ( ) YES ( ) NO
- **Server Settings**:
  Server Hostname: _____
  (full DNS recommended, **HA cluster**: use virtual **HPOM** cluster hostname!)

  Local Server Identifier: _____
  Example: <hostname>_server, or generic name “production_server”

  Server Description (optional): _____
- **Oracle for HPOM Settings**
  Suggested values are read from HPOM. Carefully review all settings!
  Caution: especially if a remote Oracle (HA clustered) database is used.
  Oracle home path: _____
  Oracle hostname: _____
  HA cluster: use virtual hostname of **Oracle** (remote) database.
  Oracle listener port (default 1521): _____
  [ ] Secure Oracle connection
- **Oracle for HPOM Access Settings**
  Oracle DB name (default ov_net): _____

  OpenView DB instance name (default openview): _____

  Provide an Oracle user and his/her password. Tip: use opc_op or opc_report.
  Read-only access is only required.
  Oracle DB username (default opc_op): _____

  Oracle DB password: _____
- **Web Application Server Settings**
  Web application ports to which the user will connect with his web browser.
  HTTP (default 9662): _____
  HTTPS (default 9663): _____
- **Pre-Installation summary**
  After that the actual Administration UI installation will start. At the end an installation and port summary will be shown.

Starting the Administration UI Installer

The installation of the Administration UI software has to be performed as the UNIX/LINUX user “root” on the HPOM Management Server, because the installer performs various tasks which need root permissions. The installer checks whether root privileges are available.

Remember to export the DISPLAY of the HPOM server to your workstation. If necessary allow access to it by using the `xhost +` command.

The DISPLAY variable should be set **before** starting the Installer. If it is not set correctly, the installer will fail and you will receive a Java-Error in the shell window. See also the chapter on troubleshooting Display problems on page 41.

- If a previous version of Administration UI already exists please observe the following points:
  - An upgrade from CVP 3.x to Administration UI is not supported! CVP should be uninstalled first.
  - Please note, that the installer cannot be used for version updates, for example to update version 4.1.0 to 4.1.1 or 9.0.0 to 9.0.1. For this purpose patches are available.
- Make sure that the product media is mounted (e.g. on UNIX systems to `/mnt`) or the installer image has been copied to some temporary location.
- Also make sure there is enough disk space (~1250MB) in the `/tmp` directory (on UNIX systems) or in some other directory.
- In order to define the directory for temporary unpacking the installer, please run:

  ```
  # export IATEMPDIR=/directory/with/enough/space
  Example: # export IATEMPDIR=/tmp
  ```

- After that please start the installer itself:

  ```
  # ./install.bin
  ```

If there is not enough free disk space inside `/tmp` or the other directory you defined, you will receive the following message:

```
bash-2.05b# ./install.bin Preparing to install...
WARNING: /tmp does not have enough disk space!
  Attempting to use / for install base and tmp dir.
WARNING! The amount of / disk space required to perform this
installation is greater than what is available. Please free up at
least 512262 kilobytes in / and attempt this installation again. You
may also set the IATEMPDIR environment variable to a directory on a
disk partition with enough free disk space. To set the variable enter
one of the following commands at the UNIX command line prompt before
running this installer again:
- for Bourne shell (sh), ksh, bash and zsh:
   $ IATEMPDIR=/your/free/space/directory
   $ export IATEMPDIR
- for C shell (csh) and tcsh:
   $ setenv IATEMPDIR /your/free/space/directory
```

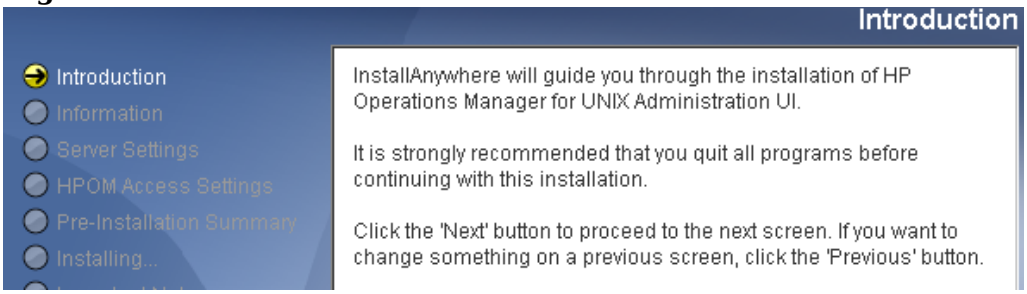
In case you receive this message, set the IATEMPDIR variable to a location with enough disk space for the time of the installation and restart the installer. Example:

```
# export IATEMPDIR=/directory/with/enough/space
# ./install.bin
```

The installer will unpack itself into the defined IATEMPDIR. After a few moments the actual installer GUI should appear (Figure 1 on page 15). Please note, that this startup process can take some time, please be patient and do not interrupt the execution.

After the installer has started successfully you will get the following welcome screen:

Figure 1 Introduction



The installer will guide you through the various installation steps, which are described on the following pages below.

Installing the Software

The installation wizard will take you through all the steps, required to install Administration UI. The installer will try to gather all the information that is required to complete the initial phase of the installation successfully. During this phase, you are presented with a number of screens which require you either to confirm the suggested configuration or supply new information if you want to change the default settings.

You will perform the following steps:

Installation Warning

If Administration UI is already installed on the HPOM server you will receive a warning message (Figure 2 on page 17). The installer will exit after clicking OK.

If Administration UI was installed, but manually removed, for example by using the command

```
# rm -rf /opt/OV/OMU/adminUI/
```

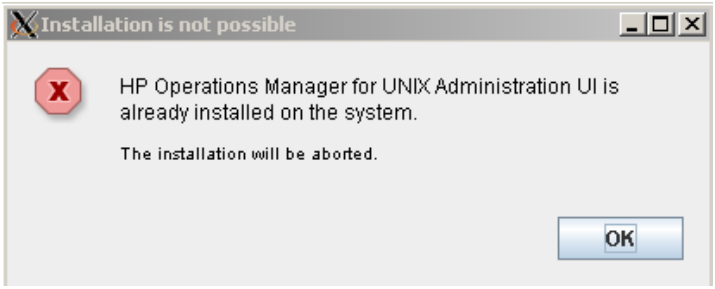
it is also necessary to remove the following directory (it contains the installation properties from the previous installation).

```
# rm -rf /var/opt/midas
```

Unless this information is removed, the reinstallation will not be possible..

Please note that the Administration UI installer cannot be used for version updates.

Figure 2 Installation Warning

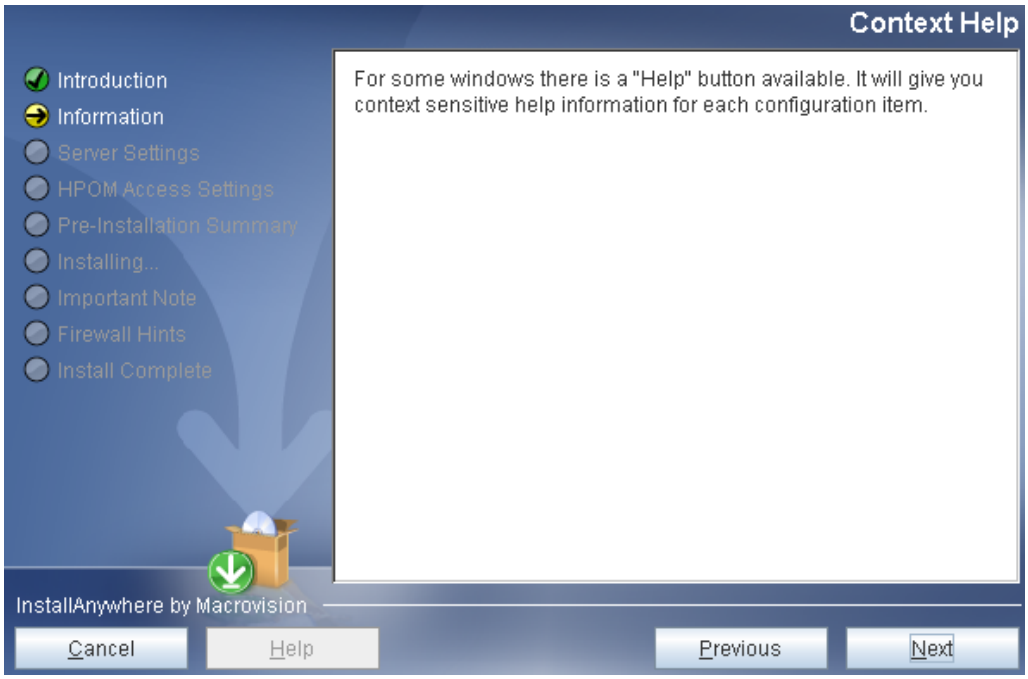


Context Help

In some windows a context sensitive "***Help***" button is available.

The Context Help window (Figure 3 on page 18) simply informs you about this installer feature. If no help information is available, the Help button will be grayed out.

Figure 3 Context Help



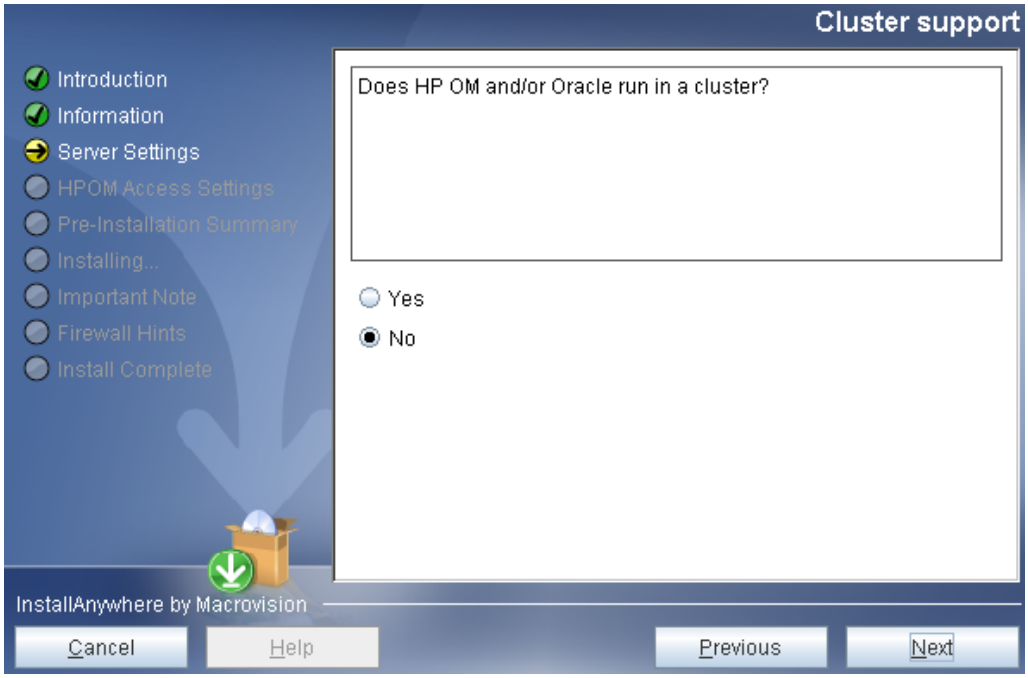
Cluster Support

The installer will ask you if HPOM itself and/or Oracle is running in a HA cluster package (Figure 4 on page 19).

If either of this applies, please select [X] Yes.

Subsequent installation steps depend on this choice.

Figure 4 Cluster Support



Server Settings

In this step of the installation procedure you have to confirm the name of the system hosting the Administration UI server (Figure 5 on page 20).

- ***Server Hostname:*** This is the local server hostname. Specify a name or IP address which can be resolved and reached from all involved systems. Default entry is the output of the command "`hostname`", for example

  ```
  # hostname
  ```

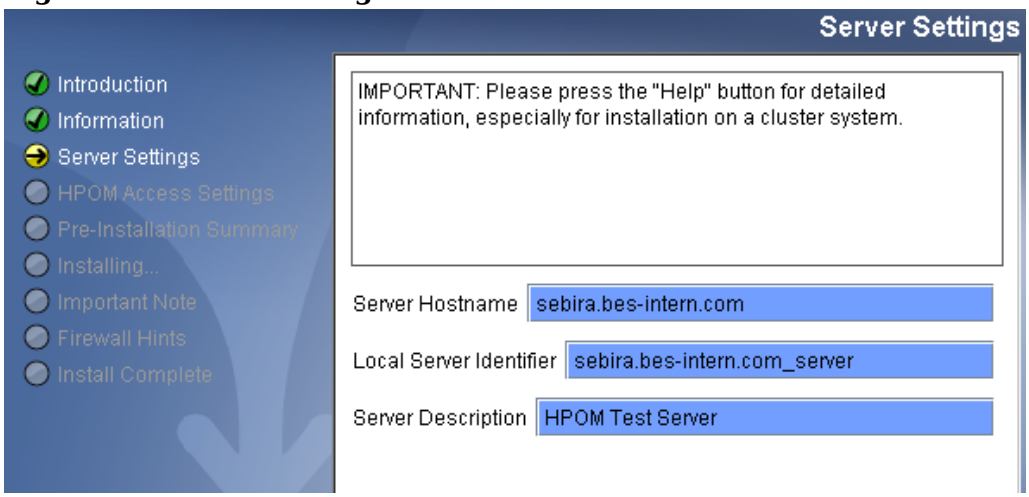
  HA CLUSTER: In HA clusters, use the virtual host name that represents the HA package running the HPOM Server (which includes Administration UI)!

- ***Local Server Identifier:*** This is used within Administration UI to identify individual instances of Administration UI. The value you assign as a local identifier must **not** contain any spaces.

The recommended naming scheme for the Local Server Identifier is to use some generic name extended by "_server". This has the advantage that if the system's hostname changes the Server Identifier does not need renaming.

- ***Server Description:*** Optional field in which you can enter some short description. For example: "OMU Test Server EMEA" server.
- Click the ***Help*** button for further context sensitive help information.

Figure 5 Server Settings



HPOM Configuration

Next you have to confirm or newly define the Oracle database connection settings.

The information in this section covers two configuration items:

- Oracle Settings for the BackEnd Server on page 21

- Oracle Access for the BackEnd Server on page 23

Oracle Settings for the BackEnd Server

HPOM uses an Oracle instance to store its configuration data. Administration UI retrieves the HPOM configuration data (for example nodes, policies) directly from that Oracle database instance in read-only mode.

Important: It is vital to review and verify all connection parameters! The majority of configuration problems are down to incorrect settings here, especially when non-standard ports or incorrect Oracle hostnames are used.

The installer attempts to detect most Oracle settings by examining the file `/etc/opt/OV/share/conf/ovdbconf`. `ovdbconf` which is the main HPOM configuration file containing some database access parameters. Unfortunately, the Oracle listener port is not stored in this file (see below for more details).

Oracle RAC environments: The correct configuration setup has to be done AFTER the installation of Administration UI is finished. Please see: Oracle RAC Cluster Support on page 58.

Generally, there should be no need to change the suggested settings, unless the HPOM Oracle database is located on a remote server.

- ***Oracle home path***: This must match the ORACLE_HOME environment variable on the HPOM server. Make sure the path is correct, especially on a HA cluster or when Oracle is running on a remote server.
- ***Oracle hostname:*** By default the suggested hostname is the HPOM server hostname which was entered in the previous screen (“Server Settings”). FQDN, short name, or IP can be used. They must be resolvable on the HPOM server.

  HA CLUSTER: If Oracle is running as a HA cluster package, please provide the virtual cluster hostname of that HA cluster package.
- ***Oracle port:*** Since the installer cannot automatically determine the Oracle listener port, the standard port 1521 is used by default. Please double-check if this is the correct port!

You can verify the Oracle listener port by checking the file `tnsnames.ora`. On the HPOM server you can for example use the following commands:

```
# su – oracle
$ cd $ORACLE_HOME
$ORACLE_HOME/bin/tnsping <oracle_server>
```

The output could look like this:

```
[...](DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=kotao.bes-intern.com))(
ADDRESS=(PROTOCOL=TCP)(HOST=192.168.123.123)(PORT=1521)))
```

or

```
# su – oracle
$ cd $ORACLE_HOME
$ more network/admin/tnsnames.ora
```

The output should looks like this (shortened):

```
ov_net =
  [...](ADDRESS =  (PROTOCOL = IPC)(KEY =openview))
          (PROTOCOL=TCP)
          (HOST=avocado)
          (PORT=1521)
    (CONNECT_DATA=
      (SID=openview)
```

- ***Secure Oracle connection:*** Enable the checkbox if a secure Oracle communication is being used. Use the following commands to determine if this is the case:

```
# su – oracle
$ cd $ORACLE_HOME
$ more network/admin/tnsnames.ora
```

For the output see above. Or run:

```
$ORACLE_HOME/bin/lsnrctl status
```

The result could look like the following output:

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=openview)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=avocado.bes-intern.com)
(PORT=1521)))
```

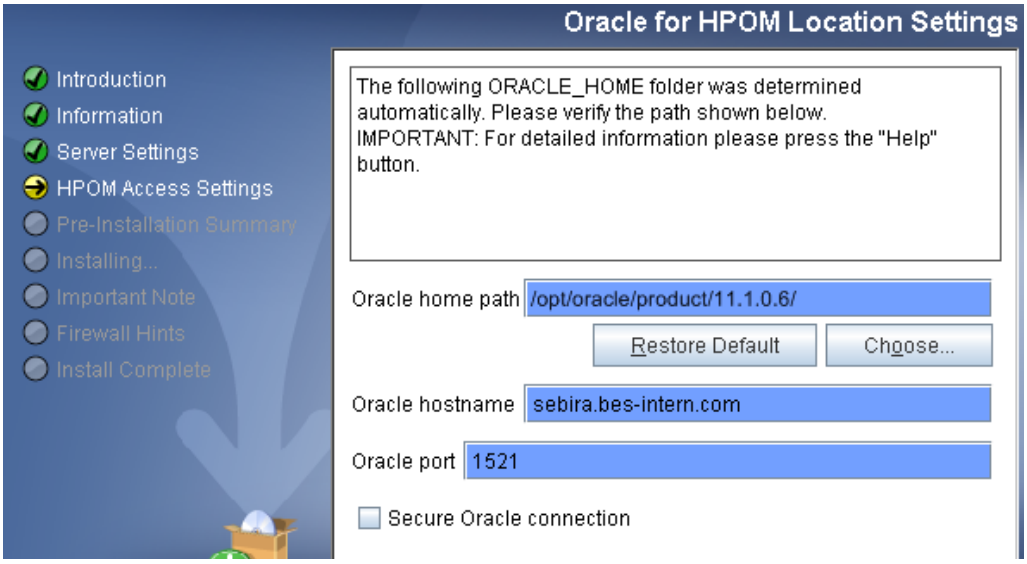
(PROTOCOL=TCP) stands for unencrypted communication. (PROTOCOL=IPC) indicates that you need to enable the checkbox in the installer for secure Oracle communication.

If both `ipc` and `tcp` is available, it is suggested to use an unsecure Oracle connection.

- Click on the ***Help*** button to receive more context sensitive help information.

The following figure shows the dialog used to specify the database location:

Figure 6 Oracle Settings 1



Oracle Access for the BackEnd Server

The subsequent screen (Figure 8 on page 24) asks for additional database parameters like instance name, username and password required to access the correct Oracle database instance.

Check that the Oracle DB name and HPOM DB instance name are correct. These values are also read from `/etc/opt/OV/share/conf/ovdbconf` and generally should be correct.

You also need to specify the user name and password for the Oracle user which will be used to connect to the database. By default, it is assumed that the Oracle user **opc_op** will be used; alternatively, the Oracle user **opc_report** (who has read-only rights) can be used as well.

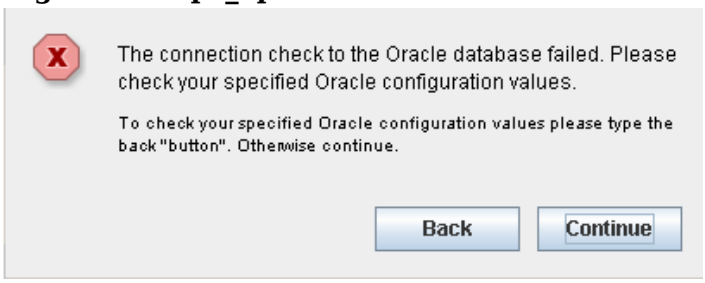
Generally, any Oracle user can be specified as long as the Oracle user has sufficient privileges to read all relevant HPOM database objects.

The passwords for the both Oracle users (opc_op or opc_report) are set during the installation of the HP HPOM server. In the Administration UI installer screen you must supply exactly this password. See chapter Wrong or Unknown HPOM Passwords on page 42 if you do not know any of them.

CAUTION: Do not confuse the Oracle opc_op account with the accounts of the same name in HPOM for UNIX and the UNIX operating system itself. All three exist and are completely different accounts!

The installer will verify the entered password. If the test fails, the following warning (Figure 7 on page 23) will be displayed:

Figure 7 Opc_op Connection Error



If you ignore this warning and proceed anyway, the Administration UI BackEnd server will fail to connect to the Oracle database and most Administration UI functionality will be unavailable.

Therefore, it is strongly recommended to use the correct password. However, it is possible to finish the installation first and then re-configure the DB access with the correct information later.

To change the password at a later stage, please use the command:

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

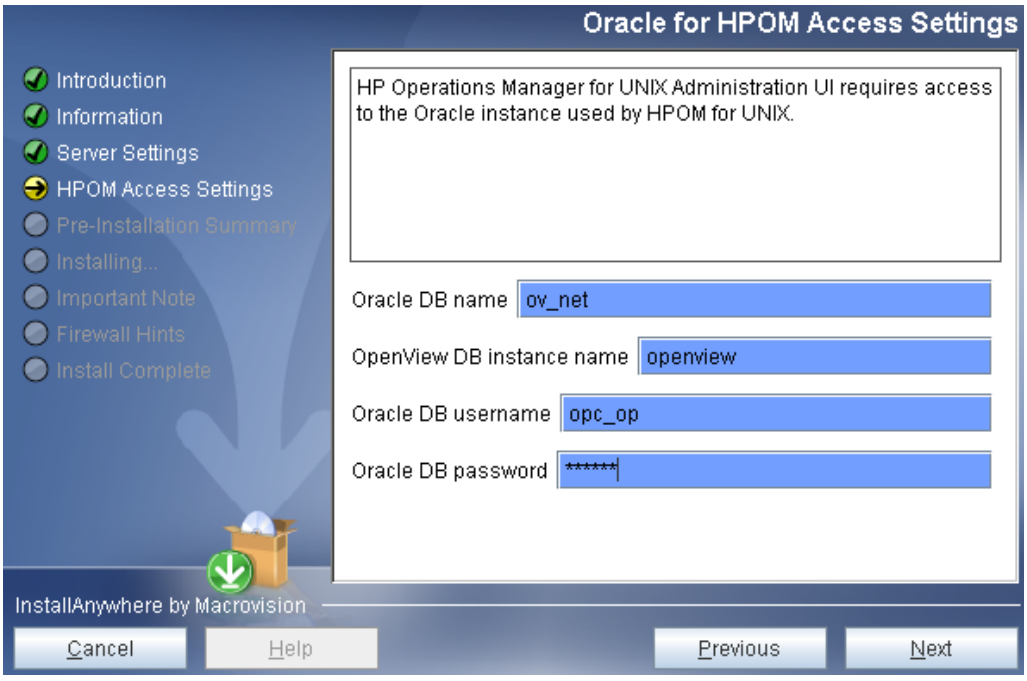
After such a password change, restart Administration UI via:

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

The password will not be shown in the installer GUI as you type it; the password is stored in encrypted form inside the Administration UI configuration files.

For more information about configuring passwords later, see the Administration UI Administration and Configuration Guide.

Figure 8 Oracle Settings 2



Configuration of Web Application Ports

The installer will ask you for the port on which the Administration UI Web Application can be reached by a browser, as illustrated in Figure 9 on page 25.

The installer will perform a check if the specified ports are available. If this is not the case, a warning message will be displayed and you will be asked to change the port before proceeding. The default ports are:

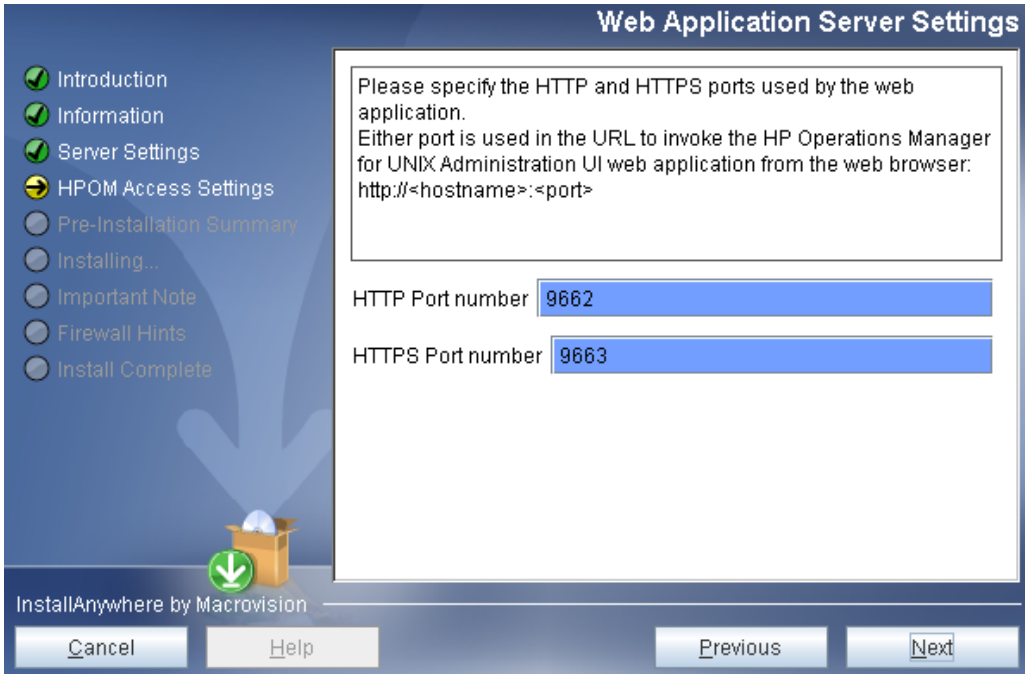
- ***HTTP*** 9662
- ***HTTPS*** 9663

It is currently not possible to disable either port. If you enter a non-default port number, you also have to specify the alternate port number in the URL, which is used to invoke the Administration UI Web Application from the web browser. With the default ports, this is:

```
http://<HP-OM-Server>:9662/
https://<HP-OM-Server>:9663/
```

For example: `http://sebira.company.com:9662`

Figure 9 Web Application Server Settings



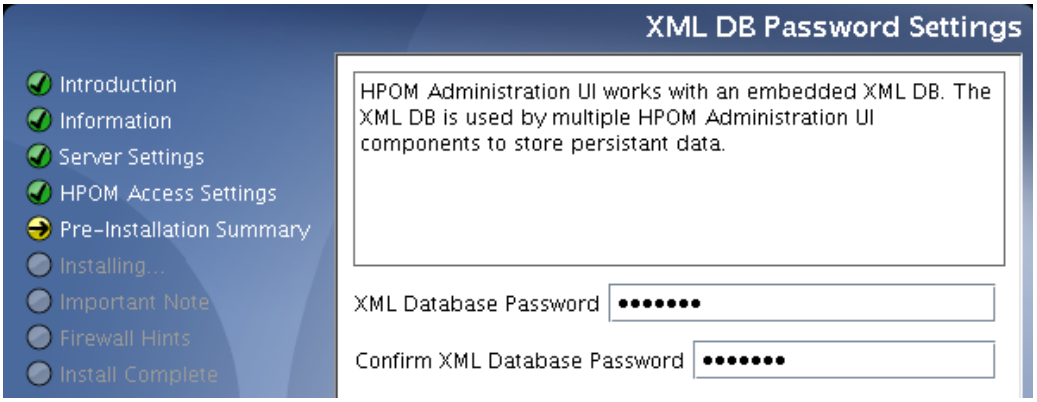
Please note, that the port numbers supplied here, are also inserted into a set of HPOM tools (formerly „OMU Applications“). These will be uploaded into the HPOM database during the installation of Administration UI.

For details on the Java GUI integration, please refer to the Administration and Configuration Guide.

XMLDB Password Settings

In this installation window you are asked to enter a password for the XMLDB. It stores the Administration UI users, user groups, user roles, etc.

Figure 10 XMLDB Password Settings



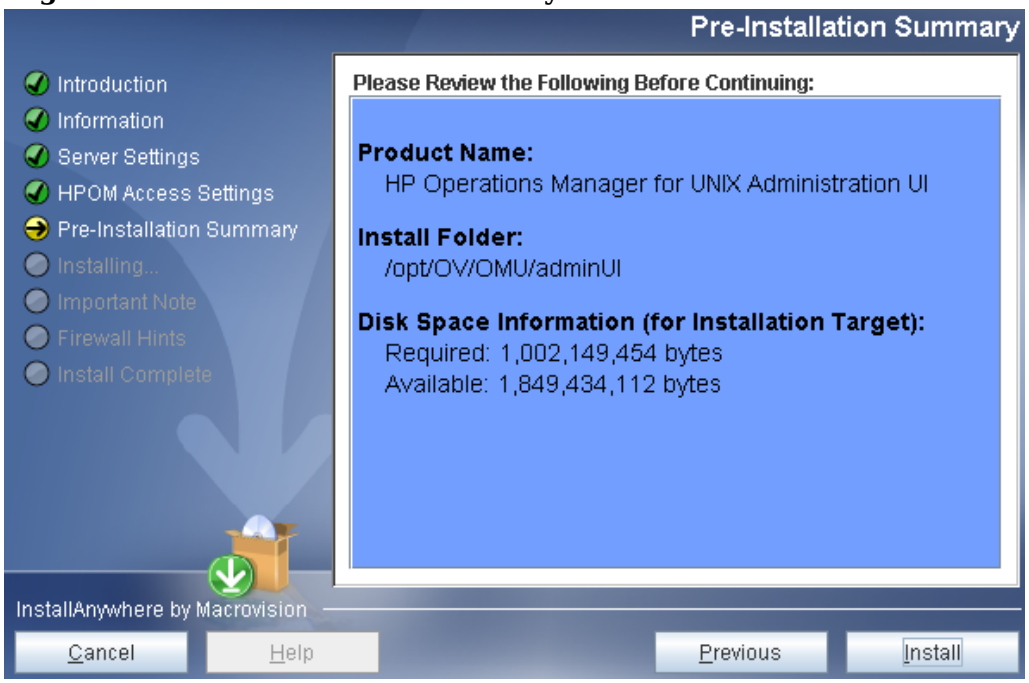
Pre-Installation Summary

Until now, no actual installation of the Administration UI software has taken place. Before the actual software installation process starts, the installation wizard displays a summary screen. See the example below.

Take this opportunity to check the details you supplied, in particular the installation folder and disk space requirements, as illustrated in Figure 11 on page 26.

Click Install to start the actual installation; click Previous to return to any dialog where you may check or change your installation parameters.

Figure 11 Pre-Installation Summary



Starting the Software Installation

After pressing the “Install” button, the installer starts the actual installation and displays the progress. During the installation some pop-up windows will appear when the different internal modules are configured and started.

The installation procedure consists of two phases:

1) Installation of the software itself (binaries, configuration files, documentation,etc.)

2) Configuration of the Administration UI components based on the parameters provided during the installation

The configuration phase of the installation includes the execution of various scripts and commands.

Please note, that there is currently one known problem, which you might encounter during the configuration phase of the installation:

- “XML Database Startup Error” on page 27

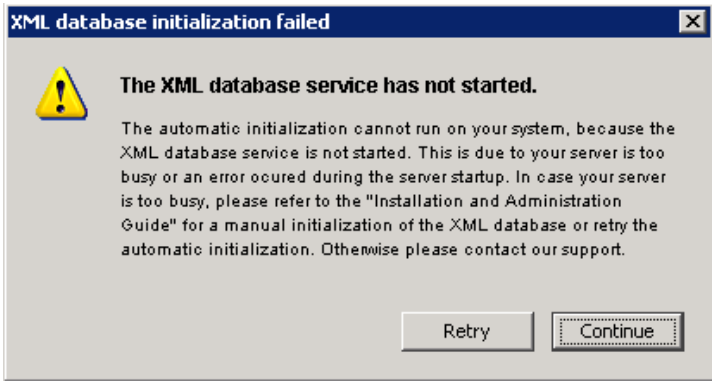
XML Database Startup Error

If you are installing Administration UI on slower systems or machines with a high workload during the installation, the XML database startup might fail which will result in the error illustrated in Figure 12 on page 27.

- In case you receive this error message, please press the RETRY button.

This should generally fix the problem. After that continue with the installation.

Figure 12 XMLDB Initialization Error



If the Retry command was not successful, or if you cannot login at all into the Administration UI web interface, please run the following command **AFTER** the installation has completed:

```
# /opt/OV/OMU/adminUI/adminui init force
```

The `adminui init force` command will load the default BackEnd and user definitions into the XML database.

The command line output should show something like this:

```
[...]
intern.install_xmldb:
     [echo] Initializing usermgmt database...
[xdb:create] Database driver already registered.
[xdb:create] Created collection /db/usermgmt
```

```
[xdb:store] Database driver already registered.
[xdb:store] Found 3 files.
[xdb:store] Storing roles.xml ...
[xdb:store] Storing usergroups.xml ...
[xdb:store] Storing users.xml ...

intern.update_datalocal:
     [echo]       - update data_local.xml
     [copy] Copying 1 file to /opt/OV/OMU/adminUI/conf
   [delete] Deleting directory /opt/OV/OMU/adminUI/work/tmp/
datassemblies
     [echo] please re-login in the GUI after a initialization!

BUILD SUCCESSFUL
Total time: 19 seconds
```

Please check that you receive a `BUILD SUCCESSFUL` message at the end.

CAUTION:

Do **not** perform this initialization before the Administration UI has started up completely.

Otherwise the operation will fail because the `adminui` script cannot connect to the internal XML database.

Also, **DO NOT** perform this command later during normal operation (unless absolutely needed – please consult Product Support first) as it will destroy and re-initialize all custom user configuration made until this point in time.

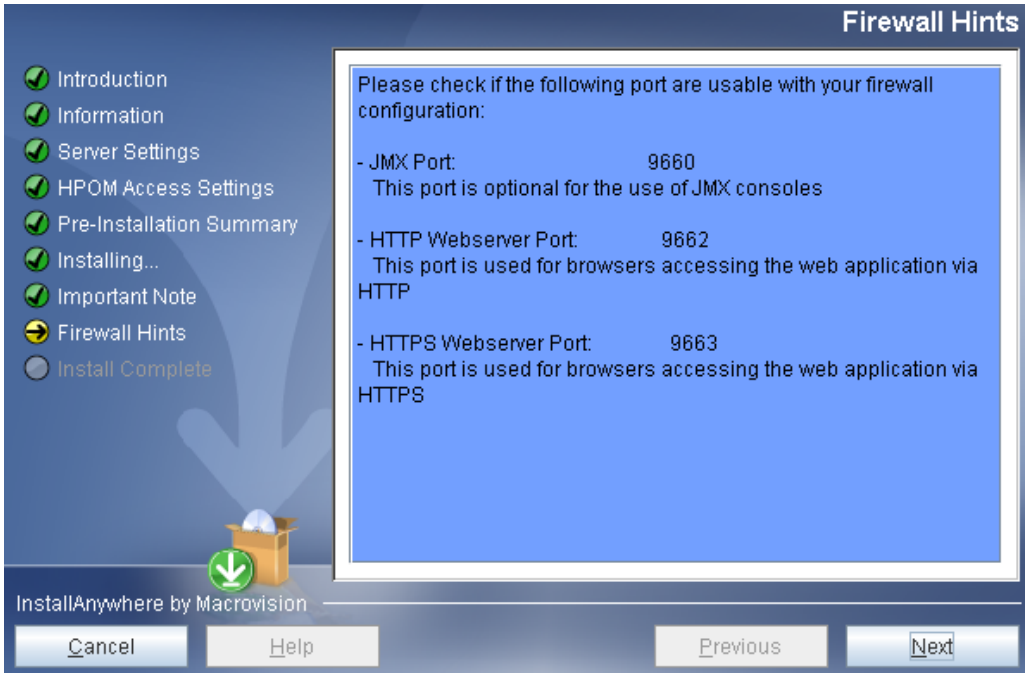
Post-Installation Summary

When the installation has completed, two screens appear displaying a summary of the port configuration of your Administration UI installation. It is a good idea to print or save this information. But you can also view this information at any time after the installation, too, by running the command

```
#/opt/OV/OMU/adminUI/adminui backend
[...]
    [echo] Server elisa3.bes-intern.com_server: OM Development System
EMEA
     [echo]   Server Identifier: elisa3.bes-intern.com_server
     [echo]   Hostname: elisa3.bes-intern.com
     [echo]   Protocol: http
     [echo]   Port: 9661
     [echo]   Secure Communication: false
     [echo]   Platform: unix
     [echo]   Install Directory: /opt/OV/OMU/adminUI/
     [echo]   Services:
     [echo]     file
[...]
BUILD SUCCESSFUL
```

Figure 13 on page 29 shows the summary of the port configuration.

Figure 13 Firewall Hints



Please also see the chapter Post Installation Tasks on page 55!

Here it is especially strongly recommended to set the admin user password for the XML database.

(intentionally left blank)

Testing and Verifying the Installation

To access the web interface for the first time

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 14 on page 31).

2) Enter your login name and password

- 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 2-3minutes.

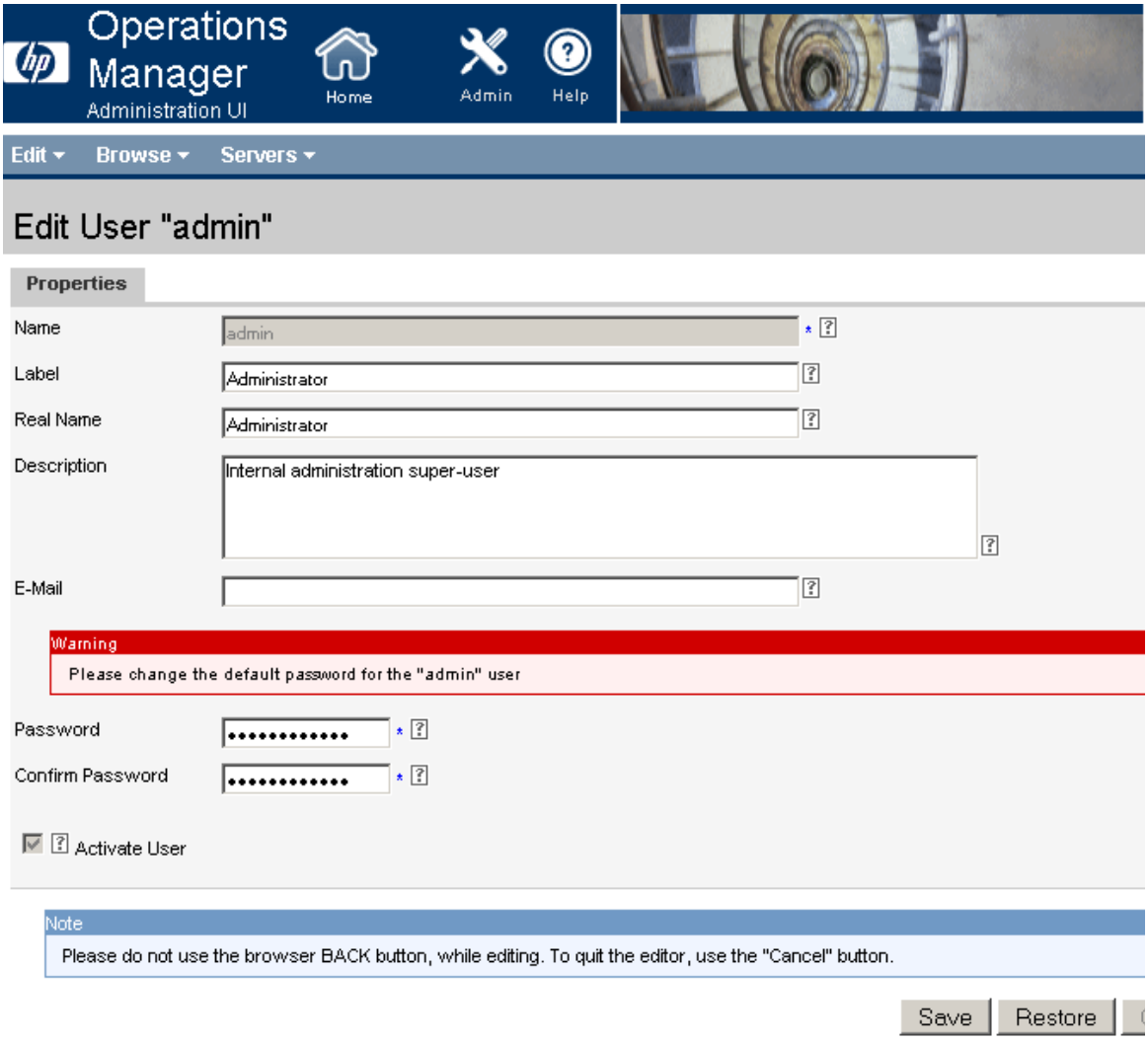
TIP 2: Please be patient. The login screen will be displayed **before** the actual XML user database is ready to process the login request!
If you try to login too soon, you will receive a message that the user name/password is incorrect. Simply wait a little longer and the login will be successful.

If you cannot login at all or get a password error: see Web Interface Problems **on page 45.**

Figure 14 Web Interface Login Screen

When you log in for the first time into the Administration UI web interface with the user “admin” you will be asked (for security reasons) to change the default password as shown in the example below´(Figure 15 on page 32). When done press “SAVE”:

Figure 15 Edit User “admin”

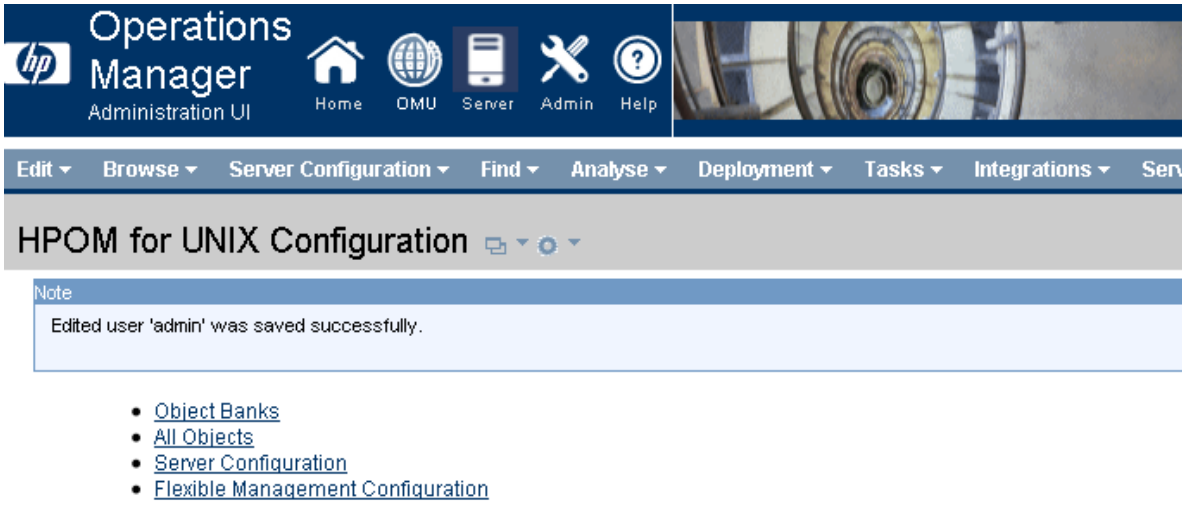


After the password has been changed you will be presented with the main Administration UI front page (Figure 16 on page 33).

In a final step a quick verification will show if the Oracle database connectivity is working correctly.

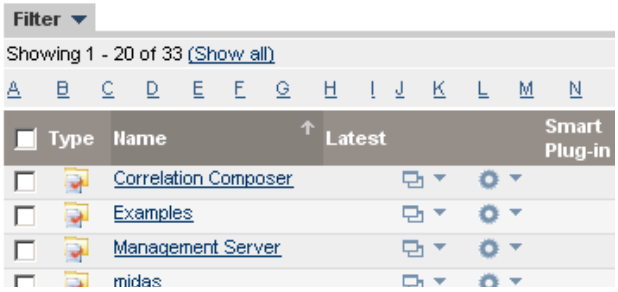
Please refer to the separate Administration UI **User Guide** on how to use the Administration UI interface and its functionality.

Figure 16 Administration UI Front Page



In order to verify that the application is generally working, click on the link “Policy Bank”. At this point in time the data will be requested from the HPOM Oracle database. If successful, you should see a result like Figure 17 on page 33 below:

Figure 17 HPOM Policy Bank



(intentionally left blank)

4 Silent Installation

Overview

It is possible to install the Administration UI silently without any user interaction.

Please contact HPOM Support to obtain the default file.

To be able to perform a silent installation this configuration property file must exist on your server containing the necessary configuration settings like hostname, Oracle connectivity, etc.

Installation Call

Two commands can be used to start the silent installation. The difference between them is basically only in regard of the location of the configuration property file.

If the configuration property file is located in the same directory as the Administration UI installer binary the silent installation command is:

```
# ./install.bin -i silent
```

Alternatively, if the configuration property file is located in some other directory, the silent installation command has to be:

```
# ./install.bin -f /path/to/property_file
```

If the configuration property file is in a different directory location than the Administration UI installer, it is important, that the first line inside the configuration property file is:

```
INSTALLER_UI=silent
```

Remove this line if the property file is located in the same directory as the installer binary, when the command `# ./install.bin -i silent` is used.

Configuration

The silent installation property file must contain all settings which are also queried during a normal interactive installation. This section explains the structure of such a configuration file.

- The variable HOSTNAME represents the hostname of your HPOM management server. If the HPOM management server is running as a HA cluster package, please use the virtual hostname of that package.

  ```
  HOSTNAME=samplehostname
  ```

- Next the Oracle database connectivity information has to be provided:

  ```
  MIDAS_DB_INSTANCE=openview
  MIDAS_DB_NAME=ov_net
  MIDAS_DB_PASSWD=opc_op
  MIDAS_DB_PORT=1521
  MIDAS_DB_USER=opc_op
  #possibilities: thin, oci
  MIDAS_JDBC_CONNMETH=thin
  MIDAS_ORACLE_SEC_FLAG=0
  MIDAS_ORACLE_SID=openview
  MIDAS_ORACLE_VERSION=11
  MIDAS_ORACLE_HOME=/opt/oracle/product/11.1.0.6
  ```

  Please contact your Oracle database Administrator if the correct settings are unkown.

- In the next variable some free text server description can be entered:

  ```
  MIDAS_BACKEND_DESCRIPTION=OMU Test Server
  ```

- All other details about the Administration UI (e.g. ports) also have to be defined:

  ```
  MIDAS_BACKEND_PROTOCOL=http   (value has always to be http!)
  MIDAS_CHECK_PORT=9662         (HTTP webserver port - default 9662)
  MIDAS_JMX_PORT=9660
  MIDAS_SEC_WEBSERVER_PORT=9663 (HTTPS webserver port - default 9663)
  MIDAS_SERVER_PORT=9661
  MIDAS_UNINSTALLER_FOLDER=$USER_INSTALL_DIR$$/$jre$/$bin$/$java
  MIDAS_USE_HTTPS=0             (value has always to be 0;equivalent of
                                MIDAS_BACKEND_PROTOCOL=http)
  MIDAS_WEBSERVER_PORT=9662     (HTTP webserver port - default 9662)
  ```

- The next block depends on whether Administration UI is installed as a HA cluster package.

  If you are installing Administration UI NOT as a cluster package, use:

  ```
  #Cluster disabled:
  MIDAS_CLUSTER_DISABLED=1
  MIDAS_CLUSTER_ENABLED=0
  #Cluster enabled:
  #MIDAS_CLUSTER_DISABLED=0
  #MIDAS_CLUSTER_ENABLED=1
  ```

  Otherwise, to configure Administration UI as a HA cluster application, please use:

  ```
  #Cluster disabled:
  #MIDAS_CLUSTER_DISABLED=1
  #MIDAS_CLUSTER_ENABLED=0
  #Cluster enabled:
  MIDAS_CLUSTER_DISABLED=0
  MIDAS_CLUSTER_ENABLED=1
  ```

- All other configuration items in the silent installation configuration file should generally not be modified unless advised by HP Support.

If unsure please contact Product Support.

5 Installing in a Cluster

Service Guard Cluster

Overview

The Administration UI can be installed in a high-availability (HA) cluster.The term “HA resource group” used within this section equals the term “HA package” defined with HP MC ServiceGuard.

Whatever the actual structure of the HA set-up is, the following rules must be obeyed (details will follow below):

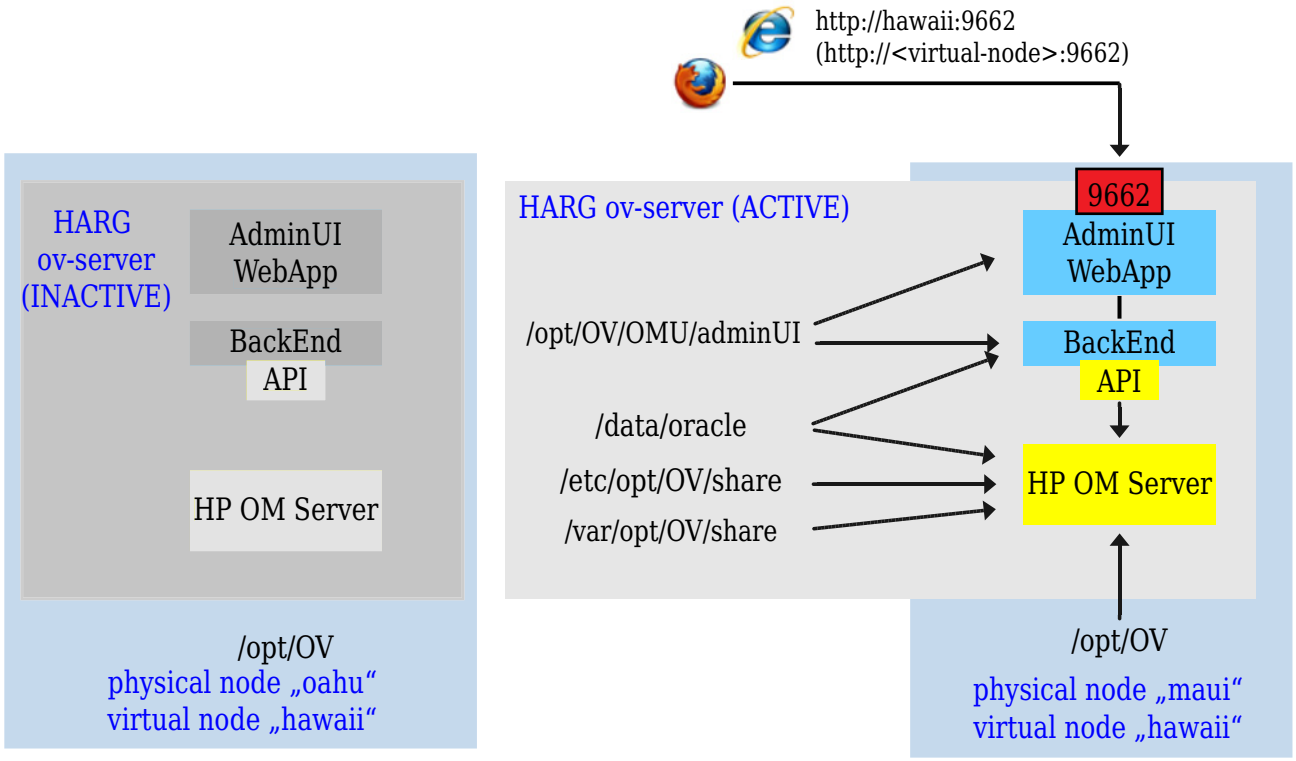
- The Administration UI has to be installed on the HPOM server itself. Remote setup and communication is **not** possible.
- The installation of the Administration UI software must be performed on the cluster’s **active** physical node.
- The virtual name and IP address of the HA resource group containing a Administration UI server must be resolvable with the name service (DNS, `/etc/hosts`, ...) at all locations where needed, e.g. by end-users accessing the Administration UI web interface.
- The virtual host name of the HA resource group must be specified during installation of Administration UI and, when logging in to Administration UI with a web browser.
- By default the installation path of Administration UI is `/opt/OV/OMU/adminUI/` which cannot be changed. Therefore, it is necessary to create a symbolic link in a clustered environment. The symbolic link `/opt/OV/OMU/adminUI/` needs to point to a directory on the shared disk into which the Administration UI software will be installed. **This has to be done BEFORE the Administration UI software is installed.**
- On all ***inactive*** physical nodes the symbolic link also has to be created also, so `/opt/OV/OMU/adminUI/` points to a directory on the shared disk where the Administration UI software will be installed to.

The information in this section helps you to install the software in a HA cluster and covers the following topics in more detail:

Installation in a HA Cluster

If Administration UI is installed as a HA cluster application the resulting situation can be illustrated with the following picture (Figure 18 on page 38):

Figure 18 Cluster Overview



This example shows the following characteristics:

Administration UI needs to be installed to the shared disk. In order to achieve this a symbolic link `/opt/OV/OMU/adminUI/` has to to point to a folder on the shared disk into which Administration UI should be installed. This file system is defined as resource belonging to the HA resource group (HARG, also referred to as HA package) “ov-server”.

The Administration UI server is configured as application resource into the same HARG “ov-server” as the HPOM Management Server itself.

The names of the physical nodes are: “**oahu**” and “**maui**”. Currently the HARG is active on “**maui**”. In case of a fail-over the entire HARG including the HPOM Server and the Administration UI application moves to “**oahu**”.

The virtual host name of the HARG is “**hawaii**”. The virtual IP address of hawaii must be resolvable by the DNS. In case of a fail-over this name and address moves along with the HARG from “**maui**” to “**oahu**”.

The WebApp front-end port (default 9662) is allocated by the running WebApp module. The GUI session always connects to the Administration UI WebApp module using the URL `http://hawaii:9662/`.

The physical node, on which the WebApp is actually running, is completely transparent to the user.

Installation Locations in a HA Cluster

The Administration UI is installed only once per HA cluster. The software has to be installed on the currently active physical node.

Since the default installation location of `/opt/OV/OMU/adminUI/` cannot be changed, it is necessary to create `/opt/OV/OMU/adminUI/` as a symbolic link **BEFORE** the Administration UI installer is started. Make sure that the symbolic link `/opt/OV/OMU/adminUI/` points to a directory on the shared disk.

By creating such a symbolic link, the Administration UI software will be installed onto the shared disk. Therefore, if the HA cluster package running the Administration UI switches to another physical node, the Administration UI software itself will also be available on this other physical node. See also the next section for the setup steps required on the inactive node.

Setup of Administration UI on Inactive Node

Although Administration UI does not need any installation on the inactive physical node, it is necessary to perform two jobs on it (if you use HPOM 9):

- Create a symbolic link of `/opt/OV/OMU/adminUI/` pointing to the directory on the shared disk where Administration UI is installed.
- Register Administration UI via `ovcreg` so it is started after a cluster switch together with HPOM.

  For this purpose, copy the following file **from the active node**

  ```
  # /opt/OV/OMU/adminUI/conf/ovo/midas.xml
  ```

  to your **inactive node** into `/tmp`.

  Now run on the inactive node the `ovcreg` command by executing:

  ```
  # /opt/OV/bin/ovcreg -add /tmp/midas.xml
  ```

Server Startup and Shutdown in a HA Cluster

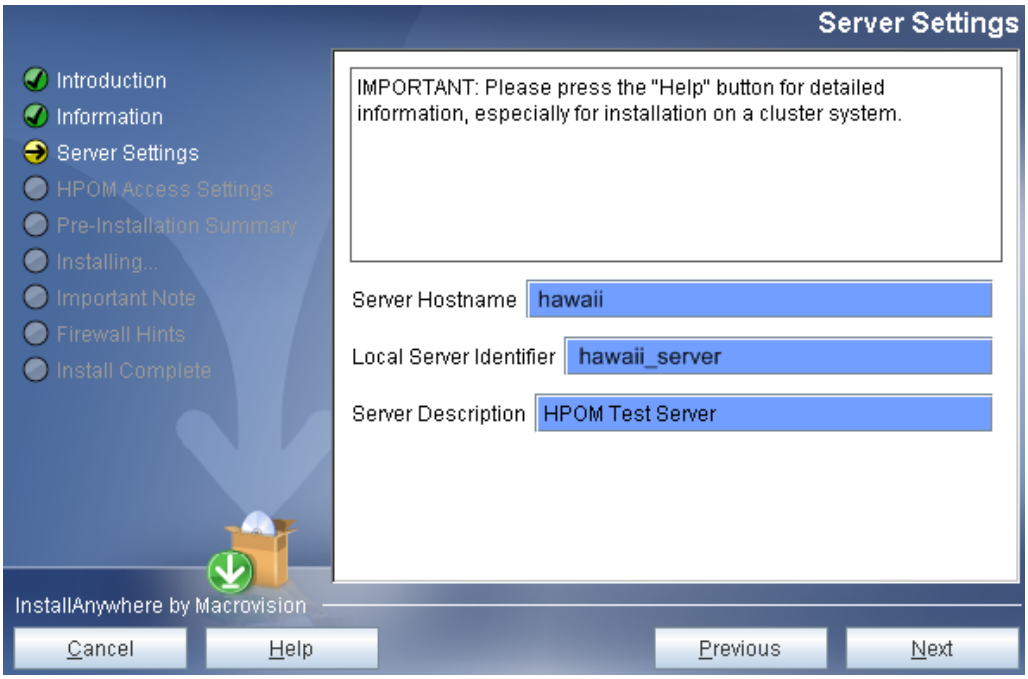
- HPOM 9 Administration UI: Since the `ovc -start` and `ovc -stop` integration is used, no manual configuration for startup and shutdown is necessary.

  Please make sure to register Administration UI on the **inactive node** via `ovcreg` (see previous section).

Server Settings in a HA Cluster

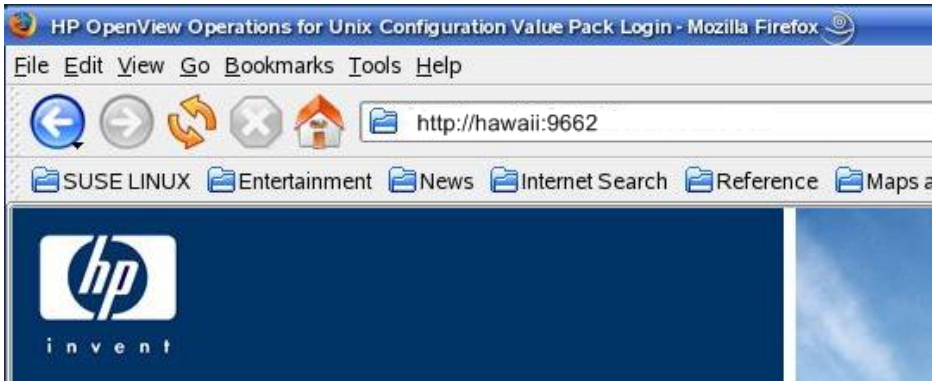
During the installation of Administration UI as a high-availability cluster package, it is crucial to specify the virtual host name of the HA package representing the virtual host where the where the Administration UI runs. If the name of the virtual host is “hawaii” (as in our example in Figure 18 on page 38), enter “hawaii” in the Server Hostname field, as illustrated in Figure 19 on page 40.

Figure 19 Specifying the Server Hostname



To log in to Administration UI running within a HARG, you also enter the name of the virtual host in the URL you use to log in, as illustrated in Figure 20 on page 40:

Figure 20 Displaying the Administration UI Login Screen



IMPORTANT: Whenever you have to refer to a Administration UI server running as part of an HA package, specify the host name, IP address, and Administration UI server ID of the virtual host running the HA package.

6 Installation Troubleshooting

Overview

This section gives basic troubleshooting information for the most common problems, which may occur during or after the installation. The information in this section covers the following topics:

Display problems

X Server Problems

The Administration UI installer attempts to open a GUI after unpacking itself. On UNIX system, this requires the correct setting of the DISPLAY environment variable and permission to access the X server on the workstation where the installation is initiated.

If not set correctly, the installer will print an error similar to the one shown in the following example (particularly watch out for the text talking about the LocalGraphicsEnvironment):

```
# /tmp/install.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer
archive...
Configuring the installer for this system's environment...
Launching installer...
Invocation of this Java Application has caused an
InvocationTargetException. This application will now exit. (LAX)
Stack Trace:
java.lang.NoClassDefFoundError
        at java.lang.Class.forName0(Native Method)
        at java.lang.Class.forName(Class.java:141)
        at
java.awt.GraphicsEnvironment.getLocalGraphicsEnvironment(GraphicsE
nvironment.java:62)
        at java.awt.Window.init(Window.java:231)
        at java.awt.Window.<init>(Window.java:275)
```

[...]

To point the installer to the correct target, prefix the installer command by the correct DISPLAY variable as shown in the following example (the example assumes that Administration UI is to be installed on the HPOM Management Server whereas the user is logged on at the system “tgt”, i.e. the display must be redirected from “src” to “tgt”):

```
# [root@src]> DISPLAY=tgt:0 /tmp/install.bin
```

If needed, allow access on the target “tgt” workstation by executing this command:

```
# [user@tgt]> xhost +
```

To test general X connectivity, execute any other X application. For example, open a clock using the command xclock:

```
# [root@src]> DISPLAY=tgt:0 xclock
```

If this works correctly, also the Administration UI installer must be able to open the display properly.

NOTE: If during installation the installer dialogs and fields do not show and you are using Reflection X, try to start XDMCP and get a CDE desktop onto your PC and start the installation from there.

Wrong or Unknown HPOM Passwords

Quite often the biggest problem is to remember the password for the Oracle user “opc_op”. Since it is only entered during the installation of HPOM server, most users forget it soon afterwards.

Tip: During the HPOM server installation the suggested default is “opc_op”. Otherwise, also try “po_cpo” or “OpC_op”. If none of these works the following tests may help you in determining it.

Testing an Oracle password

First determine the related Oracle parameters on the HPOM Management Server: In order to do so please enter the following command:

```
# cat /etc/opt/OV/share/conf/ovdbconf
DB_VENDOR Oracle
DB_NAME openview
DB_RELEASE 10.1.0
DB_TIME_STAMP "Tue Aug 1 14:50:20 METDST 2006"
DB_USER ovdb
ORACLE_SID openview
ORACLE_HOME /opt/oracle/product/11.0.6
ORACLE_BASE /opt/oracle
DBA_USER oracle
DATA_DIR /opt/u01/oradata/openview
CREATE_DIR /opt/oracle/admin/openview/create
INDEX_DIR /opt/u01/oradata/openview
ADMIN_DIR /opt/oracle
OS_AUTHENT_PREFIX
```

```
CHARACTER_SET WE8ISO8859P15
BASE_DATA_TS_SIZE 25
BASE_INDEX_TS_SIZE 5
DATA_TS_SIZE 25
INDEX_TS_SIZE
TEMP_TS_SIZE 2
DATA_TS_EXTENT_SIZE 2
DATA_TS_MAX_SIZE 500
INDEX_TS_EXTENT_SIZE
ECHO_CMD echo
PROMPT TRUE
DBA_PROGRAM sqlplus
OV_USER ovdb
DBA_LOGFILE /var/opt/OV/share/log/sqlplus_log
ORACLE_BASE_REV 10
ORACLE_SECOND_REV 1
NLS_LANG american_america.WE8ISO8859P15
ITO_DATADIR /opt/u01/oradata/openview
ITO_INDEXDIR /opt/u01/oradata/openview
SQLNET_ALIAS ov_net
```

Log on to the HPOM Management Server (or use the su(1) command) as user oracle and try to connect to the database using the user-password combination you want to test. If the HPOM database instance does not contain the default user accounts opc_op or opc_report, check the `ovdbconf` file for the appropriate values for the user name. The example above shows an excerpt from an ovdbconf file.

After logging on as user „oracle“, make sure that the environment variables ORACLE_SID and ORACLE_HOME match the entries in `ovdbconf`. Then use the sqlplus command as shown in the example below:

```
# su – oracle
$oracle> env | grep ORA
ORACLE _SID=openview
ORACLE _HOME=/opt/oracle/product/11.0.6

$oracle> sqlplus
SQL*Plus: Release 11.0.6.0 - Production on Tue Mar 29 16:42:16 2005
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.
Enter user-name: opc_op
Enter password:
[...]
Connected.
SQL> exit
```

If the `sqlplus` command displays the response Connected, the user name and password you tested are correct; if not, you will have to try again.

CAUTION: DO NOT USE the sqlplus command to login like this (or similar):

Enter user-name: opc_op as sysdba

Here you can enter any password even a wrong one and you can still login, so this is no real check.

This should work with all Oracle version through 11.x.

Updating the Oracle password

If it is not possible to find out the password of the specified Oracle user, you will have to change the password.

CAUTION: You should change the Oracle password only if it is absolutely necessary. For more information about changing the password, see the opcdbpwd man page.

To change the password of the Oracle user opc_op for the HP Operations Manager database, use the HPOM command `opcdbpwd` as illustrated in the following example:

First, create a backup of this file:

```
/etc/opt/OV/share/conf/OpC/mgmt_sv/.opcdbpwd.sec
```

Now change the password using the command:

```
# /opt/OV/bin/OpC/opcdbpwd -set
```

You must use the `opcdbpwd` command to change the Oracle password for the HPOM Oracle database (rather than the Oracle SQL command alter). The `opcdbpwd` command also updates HPOM's internal security file `opcdbpwd.sec` with the new authentication, which is essential for HPOM to continue to work properly after the password change.

After you have used `opcdbpwd` command to change the Oracle password, make sure you also update the Administration UI configuration by running:

```
# /opt/OV/OMU/adminUI/adminui password -u ovodb -a -p {new_password}
```

Note, that you have to use the SAME password as in the `opcdbpwd` command!

After this password change it is necessary to restart Administration UI via the following command:

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

Please note, that the Oracle opc_report password cannot be changed using `opcdbpwd`, instead use the appropriate sqlplus commands as shown in the following example:

```
SQL> alter user opc_report identified by {new password};
SQL> commit;
```

Since the Oracle user opc_report is not used by the HPOM server, there is no need to update the password in HPOM. If the Oracle user opc_report has been configured in Administration UI, the password must be updated there as well using the same „`adminui password`“ command as explained above.

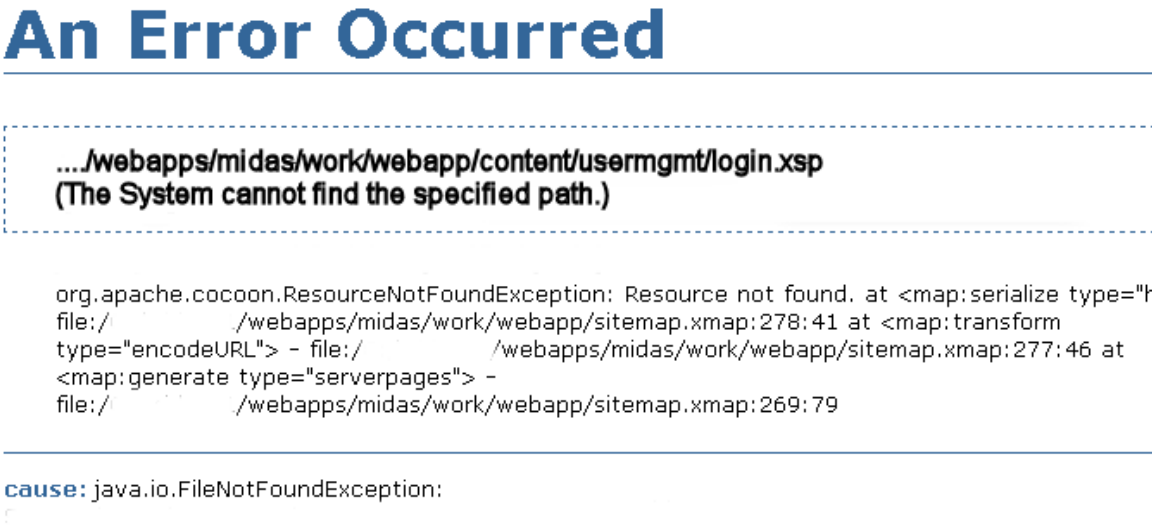
Web Interface Problems

This section gives troubleshooting tips for the most common web interface problems which are currently known.

Login.xsp Error

It is possible that after a fresh installation of the Administration UI and attempting to log on by entering the URL `http://<HP-OM-server>:9662/` an error message as shown in Figure 21 on page 45 appears:

Figure 21 Login.xsp Error



To solve this problem please run the following command:

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

This will stop Administration UI and recompile all webassemblies which are needed for a correct display of the Administration UI web interface. This compilation can run for a few minutes, please be patient. The following BUILD SUCCESSFUL message should be shown at the end:

```
[war] Building war: /opt/OV/OMU/adminUI/work/tmp/webdeploy/midas.war
[echo] copying war file to webapps
[copy] Copying 1 file to /opt/OV/OMU/adminUI/webapps
[delete] Deleting directory /opt/OV/OMU/adminUI/work/tmp/webdeploy
[delete] Deleting directory /opt/OV/OMU/adminUI/webapps/midas
[echo] done. please restart server.
BUILD SUCCESSFUL
Total time: 1 minute 53 seconds
```

Please restart Administration UI via the following command:

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

Login Error 2 - Directory Listing

Another error screen which might show up instead of the Administration UI web interface can be found below, see Figure 22 on page 46. Instead of the web interface some kind of file and directory listing can be seen.

Figure 22 Directory Listing Error

To solve this problem please run the following command:

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

This will stop Administration UI and recompile all webassemblies which are needed for a correct display of the Administration UI web interface. This compilation can run for a few minutes, please be patient. The following BUILD SUCCESSFUL message should be shown at the end:

```
[war] Building war: /opt/OV/OMU/adminUI/work/tmp/webdeploy/midas.war
[echo] copying war file to webapps
[copy] Copying 1 file to /opt/OV/OMU/adminUI/webapps
[delete] Deleting directory /opt/OV/OMU/adminUI/work/tmp/webdeploy
[delete] Deleting directory /opt/OV/OMU/adminUI/webapps/midas
[echo] done. please restart server.
BUILD SUCCESSFUL
Total time: 1 minute 53 seconds
```

Please restart Administration UI via the following command:

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

Menu Display Problem

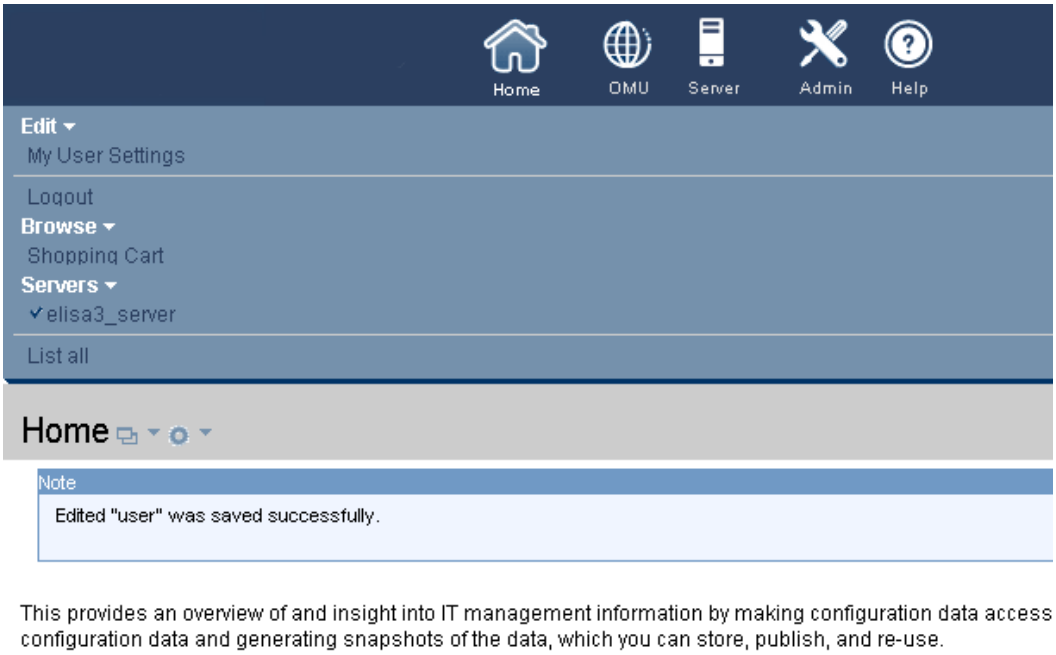
On a couple of occasions it happened that for some reasons the cache of the web browser is causing the following problem (see Figure 23 on page 47) after the user has logged in.

To solve this problem please press the Reload button or use the following computer keyboard shortcuts (otherwise delete the browser cache manually):

- Firefox: <Strg> + <F5>
- Internet Explorer: <F5>

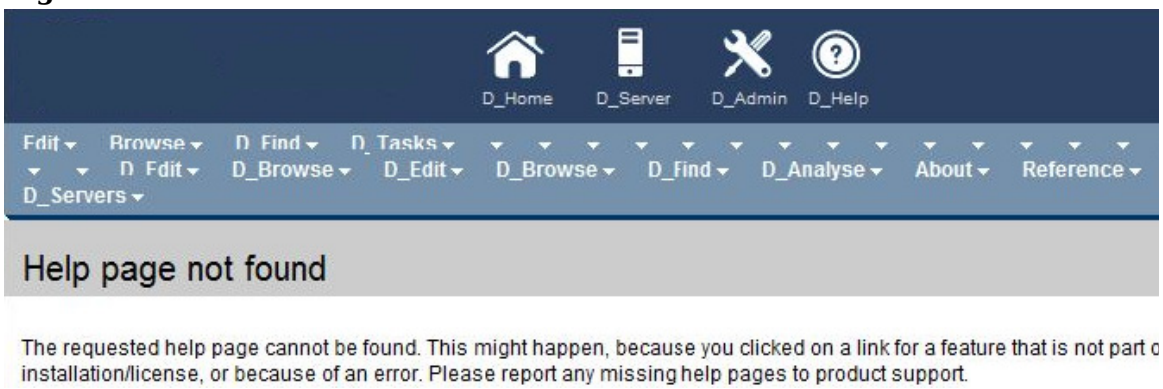
This will reload the page without using the existing cached data and display the menus horizontically instead of vertically.

Figure 23Menu Display Problem



The following incorrect screen might show up after a successful login. The reason is a browser bookmark containing an URL from a previous Administration UI version.
Example: http://192.168.10.88:9662/midas/en/index.html
Solution: Shorten the URL to http://address:port like this: http://192.168.10.88:9662.
Don't forget to update the bookmark in your browser.

Figure 24 Old Browser Bookmark



Web-Interface - No Login

Another possible problem might be, that although the correct web interface shows up, that you cannot login using the default username (admin) and password (secret).

The interface will inform you that the provided username & password is incorrect as it is shown in the example below (Figure 25 on page 49).

There are three possible explanations for this message:

- Administration UI hasn't fully started yet. Please wait for another 30-60sec. 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
  endpoint: client
javax.jbi.messaging.MessagingException: Could not find route for
exchange: InOnly[
  id: ID:192.168.123.110-122ee5aef40-4:14
  status: Active
  role: provider
  service: {http://blue-elephant-systems.com/midas/servicemix/
1.0}custom-list
[...]
```

  These messages indicate that the users, user groups and user roles which define the access rights could not be read yet.

- If the previous tip does not help, try to run:

  ```
  # /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 again all necessary run-time files. When issuing this command you should receive a “BUILD SUCCESSFUL” message at the end. Again there should be no more logging activity to `/opt/OV/OMU/adminUI/logs/servicemix.log`.

- If the XMLDB which stores the user database wasn’t successfully initialized during the installation (as described in XML Database Startup Error on page 27), all initial user data may be missing, therefore, any login attempt will fail.

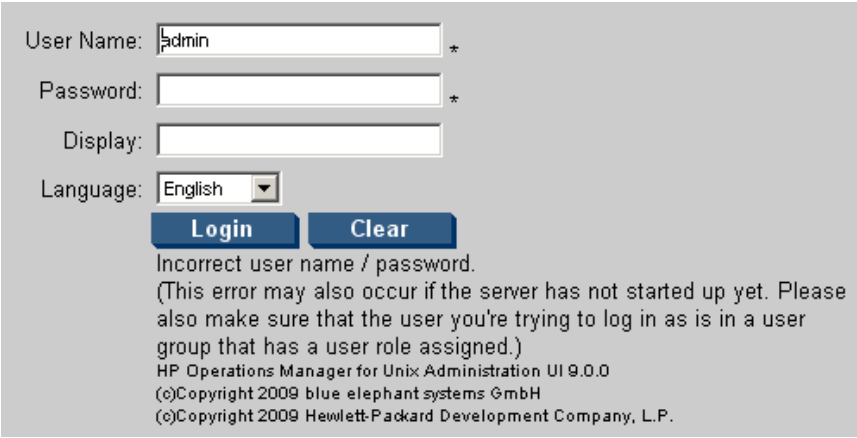
  In this situation it is recommended to perform a complete reset of the XML database. A reset will completely re-initialize the XML database.

  CAUTION: The following command is **ONLY** recommended after a fresh installation of the Administration UI software if a login isn’t working at all. In order to run this command Administration UI must be running, therefore, you need to be able at least to see the web interface. The command is:

  ```
  # /opt/OV/OMU/adminUI/adminui init force
  ```

  NO restart of Administration UI is necessary. After the command has completed successfully (“BUILD SUCCESSFUL” message) it is possible to login with the default user (login) and password (secret).

Figure 25 Incorrect Username / Password Error Message



If none of this helps, please contact Product Support.

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 26 on page 50).

Figure 26 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.

Installation Log Files

The Administration UI installation procedure creates one log file in the installation root directory `/opt/OV/OMU/adminUI/`:

```
HPOM_Administration_UI_InstallLog.log
....
```

This file contains information about the values of variables used during installation, the JRE etc. In addition, any output created by the various scripts called during the installation process, for example, to determine the Oracle installation directory or to create configuration elements, will be logged to this file.

It is also possible to redirect the Administration UI Installer debug output to the console. To do this on a UNIX operating systems, set the environment variable LAX_DEBUG to true, before starting the installer, for example:

```
# LAX_DEBUG=true /tmp/install.bin
```

Please note, that if you redirect the output to your screen by setting the LAX_DEBUG variable, the installer will not create the midas_install.log log file.

If there is a persistent problem with the Administration UI installation which you cannot resolve yourself, send the installation log files to your product support together with the support archive you may be able to create with the following command:

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

NOTE: This command will only exist, if at least the software installation phase was successful.

(intentionally left blank)

7 Uninstallation

Uninstallation

Before starting the Uninstaller, please stop the Administration UI using:

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

Make sure that no Administration UI-related wrapper or Java processes are running before you start the removal process. If any Administration UI-related wrapper or java processes are running, stop or kill them as necessary. You can check this using the following command:

```
# ps -ef | grep _server
```

If Administration UI is still running the result (showing two processes) should look like this:

```
root 22741 17364  1 02:54:26 pts/0  0:00 grep midas
root 22706 22698  0 02:52:45 ?  0:25 /opt/OV/OMU/adminUI/jre/bin/
IA64N/java -server -DbesId=midas_server -Dclassworlds.conf=/opt/OV/
OMU/adminUI/conf/servicemix//ser
root 22698  1997  0 02:52:44 ?         0:00 /opt/OV/OMU/adminUI/
wrapper /opt/OV/OMU/adminUI/conf/servicemix/wrapper.conf
wrapper.syslog.ident=midas_server wrapper.pidfile=
```

The uninstallation program to remove Administration UI is located in the Administration UI home directory. This uninstallation utility is also GUI-based and all explanations regarding X connectivity made in section Display problems on page 41 apply here as well.

Start the Uninstaller with the following command:

```
# /opt/OV/OMU/adminUI/Uninstall/uninstall.bin
```

If the Administration UI was installed in “silent” mode, the uninstallation will also automatically be performed silently. Therefore, there will be no uninstallation screens visible.

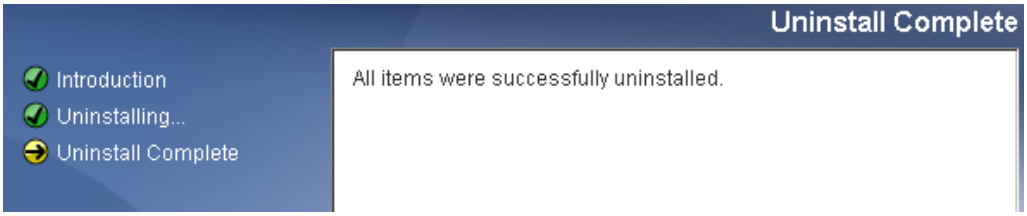
After a few moments the GUI of the Uninstaller should appear (Figure 27 on page 54).

Figure 27 Uninstallation Welcome Screen

Click the ***Uninstall*** button to start the un-installation procedure. After completion (Figure 28 on page 54)of the un-installation may display a list of the directories which could not be removed, for example, because they are still in use by other components or contain customer-specific files (documents or configuration files).

To completely remove the entire Administration UI installation simply remove **`/opt/OV/OMU/adminUI/`** manually.

Figure 28 Uninstallation Completion



If Administration UI is removed without using the Un-Installer, it is recommended also to remove the following directory with its contents:

```
# rm -r /var/opt/midas
```

The directory contains the configuration file, which is created when Administration UI is installed. If it is not removed any subsequent new installation of Administration UI will fail. You will receive the message, that Administration UI is already installed.

8 Post Installation Tasks

This chapter discusses recommended post installation tasks.

Currently, the following topics exist:

In order to improve performance please refer to section:

- Java Memory Parameters on page 56If you are using Solaris Zone's you should consult the following section:

- Solaris Zone Wrapper Problem on page 57

Some additional configuration changes are necessary in order to support an Oracle RAC cluster environment. For the configuration details please refer to section:

- Oracle RAC Cluster Support on page 58

Disabling WebApp port 9662. It is possible to disable port 9662 in order to force users using secure access to the web application port 9663:

- Disabling the WebApp's HTTP Port (9662) on page 59

Java Memory Parameters

It is highly recommended to fine tune the JAVA memory parameters used by Administration UI. If the HP Management Server is sufficiently powerful and has enough RAM, it is recommended to increase the maximum memory setting to 1024 or even higher.

The recommended max. amount of RAM is 1024mb or 2048mb if there is enough physical memory available.

In order to change the configuration setting affecting the RAM utilization of the JRE running Administration UI please edit:

```
/opt/OV/OMU/adminUI/conf/servicemix/wrapper.conf
```

Search for this block:

```
[...]
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=512
```

and change it to

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1024
```

Please restart Administration UI using the following command:

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

Do no decrease the value below the initial setting – this will also decrease performance and Administration UI may not function properly anymore.

Solaris Zone Wrapper Problem

As discussed in section Solaris Zones on page 6 a rare case has been recorded in an Solaris zone environment in which the Administration UI application startup regularly failed.

Generally, the installation of Administration UI in a Solaris whole-root non-global zone is supported.

But in that instance each Administration UI failed with the following error message inside

```
#/opt/OV/OMU/adminUI/logs/wrapper.log
[...]
INFO | jvm 1 | 2009/09/11 11:43:01 | java.net.SocketException: Address already in use
[...]
```

The problem is that sometimes the bundled wrapper binaries inside Administration UI seem to have a problem inside a Solaris zone.

The solution is to replace the existing wrapper binaries by the newest ones.

Please download the matching Community binaries package for your Solaris SPARC system from:

http://wrapper.tanukisoftware.org/doc/english/

At the moment (Sept 2009) the current version is 3.3.6.

In a next step you need to extract the following three binaries from this package:

```
bin/wrapper
lib/wrapper.jar
lib/libwrapper.so
```

These three files have to be copied to the following locations (overwriting the existing ones):

```
wrapper --> /opt/OV/OMU/adminUI/
wrapper.jar --> /opt/OV/OMU/adminUI/bin
libwrapper.so --> /opt/OV/OMU/adminUI/bin
```

Please perform a clean, start operation of Administration UI using:

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

Oracle RAC Cluster Support

In order to support an Oracle RAC cluster it is necessary to modify three Administration UI configuration files after the Administration UI installation is complete. Otherwise, listing or modifying HPOM objects is not possible. Instead an error will be returned that no connection to the Oracle database is possible.

Please ask your Oracle database administrator for the correct virtual(!) hostnames, port and SID. Example:

Oracle RAC cluster consists of the following two servers:

- physical hostname: astrid14
- virtual hostname: astrid14-vip
- physical hostname: astrid15
- virtual hostname: astrid15-vip
- Port: 1521
- SID: openview

It is important to use the virtual hostnames!

There are three configuration files which have to be modified. Each of them has to be updated with the correct Oracle RAC JDBC connection string (!):

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

Each of these configuration files contains a JDBC connection string which could for example look like this:

```
ovodb.url=jdbc:oracle:thin:@astrid15:1521:openview
```

This default string has to be replaced by the following one. Its syntax is:

```
ovodb.url=jdbc:oracle:thin:@(DESCRIPTION=(FAILOVER=ON)(ADDRESS_LIST=(
LOAD_BALANCE=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=virtual-hostname1)(PORT=
xxxx))(ADDRESS=(PROTOCOL=TCP)(HOST=virtual-hostname2)(PORT=xxxx)))(CO
NNECT_DATA=(SERVICE_NAME=SID)))
```

According to our example the string in each configuration file should look like this:

```
ovodb.url=jdbc:oracle:thin:@(DESCRIPTION=(FAILOVER=ON)(ADDRESS_LIST=(
LOAD_BALANCE=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=astrid14-vip)(PORT=1521)
)(ADDRESS=(PROTOCOL=TCP)(HOST=astrid15-vip)(PORT=1521)))(CONNECT_DATA
=(SERVICE_NAME=openview)))
```

Please note, that you have to enter the two correct virtual hostnames, port and the correct SID.

Please remember to restart Administration UI after these modifications via:

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

Disabling the WebApp’s HTTP Port (9662)

In order to access Administration UI through a web-browser, two access options exist: 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 order to enforce usage of HTTPS, it is possible to disable HTTP access via port 9662. This is achieved by binding port 9662 to “localhost”.

In order to implement this change the following steps have to be applied (This setup assumes, that Administration UI is up and running):

- (1) Edit the following file:

  ```
  # /opt/OV/OMU/adminUI/conf/jetty.xml
  ```

At the beginning of the file search for this block:

```
<!-- default http connector -->
<bean class="org.mortbay.jetty.bio.SocketConnector">
```

After this block add this line:

```
<property name="host" value="localhost"/>
```

The block should look like this after the modification:

```
<!-- default http connector -->
<bean class="org.mortbay.jetty.bio.SocketConnector">
  <property name="host" value="localhost"/>
  <property name="port" value="9662"/>
  <property name="headerBufferSize" value="12000"/>
```

- (2) Edit the following file:

  ```
  /opt/OV/OMU/adminUI/conf/config.properties
  ```

Change the hostname to localhost, so the configuration block will look like this:

```
....
vendor = blue elephant systems GmbH

backend = rhel-support_server
hostname = localhost
server.port = 9661
```

- 3) Edit the following file:

  ```
  /opt/OV/OMU/adminUI/conf/usermgmt.properties
  ```

  Change the URL so it looks like this:

  ```
  xmldb.dbUrl=xmldb:exist://localhost:9662/exist/xmlrpc/db/
  ```

- (4) Restart Administration UI via the command:

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

Please note, that if a Administration UI patch is applied, this modification has to be re-applied.

9 External Software

Overview

This section lists additional, external software products that are integrated in Administration UI and describes how you can configure the software to suit the demands of your environment. All the software products described in this section are optional unless you choose to install and configure functionality on which a Administration UI feature depends:

Authentication Software

Authentication of Administration UI users happens inside the Administration UI WebApp server part, to which the user's web browser connects.

With the current product version, Administration UI supports authentication using LDAP, LDAPS, Active Directory Server or any authentication service which can be integrated into PAM.

NOTE: Authentication covers only the process of validating the user account with a password. It does not include any authorization control (user's capabilities). Authorization is implemented exclusively in Administration UI by defining Administration UI user roles.

Therefore, whenever setting up a new Administration UI user, make sure that the account exists in both Administration UI and the external authentication system. Furthermore, make sure that the Administration UI user is member of at least one Administration UI group which has at least one Administration UI user role assigned.

To use an external authentication software like LDAP or PAM in Administration UI additional software (for example, the LDAP server) may be required on the Administration UI WebApp. Install and configure this software as needed. More details are presented below.

PAM integration

To authenticate Administration UI users through PAM (Pluggable Authentication Modules), no extra software is needed. Administration UI already includes the open-source module jpam (see `http://jpam.sourceforge.net` for details).

However, PAM is just an interface linking software providing authentication services (like LDAP, Kerberos, UNIX passwd) to consumer applications like Administration UI. Therefore, possibly software modules implementing the actual authentication service may be needed.

To configure PAM, perform the following steps:

1.Decide, which authentication method to use. If needed, install required software modules and configure them. Test the authentication service standalone, i.e. outside of the Administration UI context.

2.Configure all Administration UI user accounts in the authentication service.

3.Configure PAM to route Administration UI authentication requests to the desired authentication service. The PAM service name is **midas**.

4.Activate the external authentication service in the conf/auth.properties file:

```
# vi /opt/OV/OMU/adminUI/conf/auth.properties
# configuration properties for authentication and authorization
components
#auth-filter.enabled=false
caches.timeout=7200000
usermodel-router.authResource=file:conf/auth.xml
# eof
```

5.Switch Administration UI to PAM authentication by configuring the property in the conf/auth.xml file. The file has to look like this:

```
# vi /opt/OV/OMU/adminUI/conf/auth.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN" "http://
www.springframework.org/dtd/spring-beans.dtd">
<beans>

  <bean id="targetServices" class="java.util.ArrayList">
    <constructor-arg>
      <list>
        <value>pam</value>
        <value>usermgmt</value>
      </list>
    </constructor-arg>
  </bean>

</beans>
```

6.Deploy the midas-wapam-sa.zip service assembly (command must be typed in one single line!):

```
# cp /opt/OV/OMU/adminUI/assemblies/midas-wapam-sa.zip \
     /opt/OV/OMU/adminUI/deploy
```

7.Restart the WebApp:

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

Configuring the actual authentication software depends on this software itself and the OS the Administration UI WebApp is running on. In the following example, the default authentication mechanism on a Linux system is used.

Example: UNIX passwd

By default, the default authentication mechanism on Linux is UNIX passwd, which in turn is always available (normally) and there is no need to install and configure anything.

Create a user account and set the password, if not done yet, for example the user tge:

```
# useradd tge
# passwd tge
Changing password for tge.
New Password: *******
Reenter New Password: *******
Password changed.
```

Other UNIX-related parameters like home directory or shell are not needed for Administration UI.

Configure PAM to route Administration UI authentication requests to UNIX passwd by configuring the following in /etc/pam.conf:

```
[...]
midas    auth    required       libpam_unix.so.1
midas    account required       libpam_unix.so.1
[...]
```

For further details like advanced PAM capabilities (for example using multiple and/or optional authentication services) refer to the OS-specific PAM documentation.

LDAP integration

Administration UI supports user authentication through LDAP (Lightweight Directory Access Protocol). Administration UI includes the open-source component “Acegi Security System for Spring Project” (see `http://acegisecurity.org` for details).

New is LDAPS and the support of user search, which is needed for an Active Directory Server.

Currently, only basic authentication of user accounts is supported. No additional LDAP features like group membership etc. are used.

To configure LDAP authentication in Administration UI, perform the following steps:

1. Configure all Administration UI user accounts on the LDAP/Active Directory Server.

2. Configure the desired LDAP server in the Administration UI properties file `/opt/OV/OMU/adminUI/conf/ldap.properties` as shown in the following example:

```
# The LDAP URL
# Format: ldap://<host>:<port>/<base dn>
ldap.url=ldap://ldap-test:389/dc=bes-intern,dc=com
#ldap.url=ldaps://ldap-test:636/dc=bes-intern,dc=com
#ldap.url=ldaps://winsrv2008ad:636/dc=elephant-test,dc=org
```

For unencrypted access use `ldap.url=ldap://...` and for encrypted access use here as well `ldap.url=ldaps://...`
This applies both to a standard LDAP and an Active Directory Server.

In the next block enter the login credentials:

```
# Manager DN for login
ldap.managerDn=cn=Manager,dc=bes-intern,dc=com
#ldap.managerDn=cn=administrator,cn=users,dc=elephant-test,dc=org
# Manager password
ldap.managerPassword=******
```

For standard LDAP the default setting is `ldap.authenticationMode=BIND_WITH_DN`. Otherwise, no configuration changes are necessary here. Leave everything else commented out:

```
# The mode which is used for the authentication
# Allowed values are:
# BIND_WITH_DN:Use the authenticationDnPatterns for identifying a user
# USER_SEARCH : Use the authenticationSearchBase and
# authenticationSearchFilter for identifying a user
ldap.authenticationMode=BIND_WITH_DN
# The search base for searching users for authentication
# This property is used in combination with the ldap.authenticationSearchFilter
# and is used e.g. for a Active Directory search
#ldap.authenticationSearchBase=CN=Users
# The filter for searching users for authentication
# This property is used in combination with the ldap.authenticationSearchBase
# and is used e.g. for a Active Directory search
#ldap.authenticationSearchFilter=(sAMAccountName={0})
```

To use an Active Directory Server or user identification via user search, see the next page.

If you want to use an Active Directory Server or identify a user via user search, the following configuration has to be used. First of all the `ldap.authenticationMode` setting must be set to `USER_SEARCH`. Depending on the Active Directory Server configuration, the login name field also needs to be defined. In our example the field attribute is called `sAMAccountName`. Please note, that the `USER_SEARCH` function can also be used in LDAP, but generally the easier setup is done by using `BIND_WITH_DN` (see the previous page).

```
# The mode which is used for the authentication
# Allowed values are:
# BIND_WITH_DN : Use the authenticationDnPatterns for identifying a user
# USER_SEARCH : Use the authenticationSearchBase and
# authenticationSearchFilter for identifying a user
ldap.authenticationMode=USER_SEARCH
# The search base for searching users for authentication
# This property is used in combination with the ldap.authenticationSearchFilter
# and is used e.g. for a Active Directory search
ldap.authenticationSearchBase=CN=Users
# The filter for searching users for authentication
# This property is used in combination with the ldap.authenticationSearchBase
# and is used e.g. for a Active Directory search
ldap.authenticationSearchFilter=(sAMAccountName={0})
```

If the certificate originates from a proper third-party certification authority (like Verisign), no other change should be necessary (untested).

If a secure encrypted URL string is used, but without a certificate from a proper third-party certification authority, it is necessary to import the certificate also into the local Administration UI truststore. In order to do so the following two lines need to be enabled:

```
# The path to the truststore for trusted certificates for secure LDAP
ldap.truststore=conf/servicemix/truststore.jks

# The truststore password for secure LDAP
ldap.trustPassword=password
```

The import of the certificate (needs to be in the .cer format) is done via the following command (command must be typed in one single line!):

```
# /opt/OV/OMU/adminUI/jre/bin/keytool -import -alias ldapserver_a \
-keystore /opt/OV/OMU/adminUI/conf/servicemix/truststore_endpoint.jks \
 -file /tmp/ldap_server.cer
Enter keystore password: *******
[...]
Trust this certificate? [no]: yes
Certificate was added to keystore
```

The default password for the Administration UI truststore is: password

3. Activate the external authentication service in the `conf/auth.properties` file like this:

```
# vi /opt/OV/OMU/adminUI/conf/auth.properties

# configuration properties for authentication and authorization components
#auth-filter.enabled=false
caches.timeout=7200000
usermodel-router.authResource=file:conf/auth.xml
# eof
```

4. Switch Administration UI to LDAP authentication by configuring the `conf/auth.xml` as follows:

```
# vi /opt/OV/OMU/adminUI/conf/auth.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE beans PUBLIC "-//SPRING//DTD BEAN//EN" "http://
www.springframework.org/dtd/spring-beans.dtd">
<beans>

 <bean id="targetServices" class="java.util.ArrayList">
 <constructor-arg>
      <list>
        <value>ldap</value>
        <value>usermgmt</value>
      </list>
    </constructor-arg>
  </bean>

</beans>
```

Whether LDAP, LDAPS or an Active Directory Server is used, leave the value set to “ldap” here.

5. Deploy the midas-waldap-sa.zip service assembly (enter the command in one single line!):

```
# cp /opt/OV/OMU/adminUI/assemblies/midas-waldap-sa.zip \
     /opt/OV/OMU/adminUI/deploy
```

6. Restart the WebApp:

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

DST – Daylight Saving Time Patches

The Administration UI installer includes for convenience reasons a bundled JDK version 1.6.

Please note, that for future JDK DST changes or JDK hotfixes you need to update the JDK in Administration UI yourself. These JDK updates or hotfixes will not be included in any Administration UI patch.

You can use Sun's tzupdater for this purpose.

For the latest version please visit: http://java.sun.com/javase/downloads/

To check your existing Java version you can use the command below:

```
#/opt/OV/OMU/adminUI/jre/bin/java -version
```

In order to update your JDK/JRE image bundled in Administration UI after an installation, please perform the following steps:

1. stop Administration UI via:

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

2. invoke the update tool via:

   ```
   #/opt/OV/OMU/adminUI/jre/bin/java -jar tzupdater.jar -u -v
   ```

3. verify with:

   ```
   #/opt/OV/OMU/adminUI/jre/bin/java -jar tzupdater.jar -t -v
   ```

4. start Administration UI via:

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

(intentionally left blank)