Oracle® Application Server

Release Notes

10*g* Release 2 (10.1.2) for hp-ux Itanium and Linux Itanium

B15871-05

May 2006

ORACLE®

Oracle Application Server Release Notes, 10*g* Release 2 (10.1.2) for hp-ux Itanium and Linux Itanium

B15871-05

Contents

3 General Management and Security Issues

4 Oracle Application Server FIPS 140-2 Settings

5 Oracle Application Server Containers for J2EE (OC4J)

6 Oracle HTTP Server

7 Oracle Application Server TopLink

8 Oracle Application Server Web Cache

9 Oracle Enterprise Manager

Preface

This document contains release notes for Oracle Application Server on hp HP-UX Itanium and Linux Itanium systems.

Audience

This document is intended for users who are comfortable running some system administration operations, such as creating users and groups, adding users to groups and installing operating system patches on the computer where Oracle Application Server is going to be installed.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following Oracle resources:

- *Oracle Application Server Documentation on Oracle Application Server Disk 1*
- *Oracle Application Server Documentation Library 10g* Release 2 (10.1.2)

Printed documentation is available for sale in the Oracle Store at

`http://oraclestore.oracle.com`

To download free release notes, installation documentation, white papers, or other collateral, please visit the Oracle Technology Network (OTN). You must register online before using OTN; registration is free and can be done at:

`http://www.oracle.com/technology/membership`

If you already have a username and password for OTN, then you can go directly to the documentation section of the OTN Web site at:

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction

This chapter provides an introduction to Oracle Application Server Release Notes, 10*g* Release 2 (10.1.2). It includes the following topics:

1.1 Latest Release Information

This document is accurate at the time of publication. Oracle will update the release notes periodically after the software release. You can access the latest information and additions to these release notes on Oracle Technology Network at:

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

1.2 Purpose of this Document

This document contains the release information for Oracle Application Server 10*g* Release 2 (10.1.2). It describes issues associated with Oracle HTTP Server, Configuration, OC4J, Oracle Application Server TopLink (OracleAS TopLink), Oracle Application Server Web Cache (OracleAS Web Cache), and Oracle Enterprise Manager.

Oracle recommends that you review contents of this document before installing, or working with the product.

1.3 Operating System Requirements

Oracle Application Server installation and configuration will not be successful unless you meet the hardware and software prerequisites before installation. Refer to *Oracle Application Server 10g Installation Guide* for a complete list of operating system requirements.

1.4 Certification Information

The latest certification information for Oracle Application Server 10*g* Release 2 (10.1.2) is available at

`http://metalink.oracle.com`

1.5 Licensing Information

Licensing information for Oracle Application Server 10*g* Release 2 (10.1.2) is available at

`http://oraclestore.oracle.com`

Detailed information regarding license compliance for Oracle Application Server 10*g* Release 2 (10.1.2) is available at

`http://www.oracle.com/technology/products/ias/index.html`

1.6 Installation Issues

This section describes issues with installation of Oracle Application Server. It includes the following topics:

- Section 1.6.1, "The lsnodes Command Fails on Non-RAC HP-UX Systems"
- Section 1.6.2, "Installation Guide Errata"

1.6.1 The lsnodes Command Fails on Non-RAC HP-UX Systems

After completing the installation, the `install*.err` files in the *`oraInventory`*`/logs` directory may contain errors similar to following line and with java exception stack details:

```
lsnodes: cannot get local node number
```

This error is harmless and can be safely ignored. It does not affect any functionality.

Similar errors may also happen when applying bug fixes using the OPatch utility. However, the patch succeeds and the error can be safely ignored.

1.6.2 Installation Guide Errata

The *Oracle Application Server Installation Guide for hp HP-UX Itanium, and Linux Itanium* states that the `oraInst.loc` file is located in the `/etc` directory on Linux Itanium systems. This is incorrect. The `oraInst.loc` file is located in the `/var/opt/oracle/` directory on Linux Itanium systems. This mistake occurs in the following sections of the *Installation Guide*:

- "Section 2.5.1 - Create a Group for the Inventory Directory"
- "Section 2.6 - Operating System User"
- "Appending A.3 - Pre-Installation"

1.7 General Management Issues

This section describes Management issues. It includes the following topic:

- Section 1.7.1, "Cloning and Recovery Performance Issue on HP-UX Itanium"

- Section 1.7.2, "Incorrect Archivelog Mode Instructions"

1.7.1 Cloning and Recovery Performance Issue on HP-UX Itanium

On HP-UX, the Distributed Configuration Management importArchive, cloning and recovery operation can be very slow if the archive file you are using is large. For example a 70 MB archive could take many hours to import.

To resolve this problem, download patch 4122657 from Oracle*MetaLink*:

```
http://metalink.oracle.com
```

Refer to Readme file provided with the patch for full instructions describing how to resolve this issue.

1.7.2 Incorrect Archivelog Mode Instructions

In Section 19.2.2, "Enabling ARCHIVELOG Mode" of the *Oracle Application Server 10g Administrator's Guide*, in Step 1. of "To enable ARCHIVELOG mode:", the following command example:

```
alter system set log_archive_dest='xxx' scope=spfile;
```

should be:

```
alter system set log_archive_dest_n = "location=<your_desired_backup_directory>"
scope=spfile;
```

where `n` is a number between 1 and 10 and `location` is your backup directory location.

1.8 Version Compatibility

This release of Oracle Application Server operates with other versions of Oracle Application Server and with Oracle Application Server on other platforms. Refer to the compatibility matrix for the other platform in the *Oracle Application Server Upgrade and Compatibility Guide* for further information on version compatibility. For example, if you want to use the middle tier on Linux Itanium with an infrastructure on Linux x86, see the *Oracle Application Server Upgrade and Compatibility Guide for UNIX* that is supplied with Oracle Application Server for Linux x86 for more information on version compatibility.

2

Installation and Upgrade Issues

This chapter describes installation and upgrade issues and their workarounds associated with Oracle Application Server. It includes the following topics:

2.1 Installation Issues

This section describes issues with installation of Oracle Application Server. It includes the following topics:

2.1.1 LDAP Replication Using SSL Mode is not Supported

LDAP replication using SSL Mode is not supported when you select the "Use SSL communications to this Internet Directory" option during Oracle Internet Directory replication installation.

If you want to perform LDAP replication using SSL Mode, the workaround is to perform your installation in non-SSL mode first. Then change the Oracle Internet Directory instances to operate in SSL mode using the steps described in the *Oracle Application Server 10g Administrator's Guide*.

2.1.2 Harmless Message in the oraInstall.err Log File

The following error appears in the `oraInstall.err` log file after certain installations:

```
java.io.FileNotFoundException:
/net/stnfs3/vol/shiphomes/solaris/dailyShiphomes/iashybrid/10.1.2/daily/041221.002
0/Disk1/stage/Patches/oracle.rdbms.dbscripts/10.1.0.3.1/1/DataFiles/sql.jar
```

This error can be safely ignored.

2.1.3 Locales zh_TW.EUC and zh_TW in Traditional Chinese Environments Not Supported in the OracleAS Portal Component

If you try to install the OracleAS Portal component on a computer where the locale is set to zh_TW.EUC or zh_TW in Traditional Chinese environments, the installer will pause indefinitely because of the Java encoder behavior for these locales.

The workaround is to use the zh_TW.BIG5 locale in these environments. This requirement applies during installation only. After installation, you can reset the locale to the original locale.

2.1.4 Installer Does Not Detect Kernel Parameter Changes on Linux

During the installation, the Product-specific Prerequisite Checks screen appears. If the kernel parameters requirements are not met, a warning screen appears prompting you to change the kernel parameters and click **Retry**. However, clicking **Retry** does not allow you to continue. To work around this problem, exit the installer and start the installation again.

2.1.5 Problems with Oracle Application Server Repository Creation Assistant on Linux

If you need to install a OracleAS Metadata Repository into a Oracle9*i* release 9.2.0.6 Real Application Clusters database on Linux, Oracle recommends that you complete the following steps before using Oracle Application Server Repository Creation Assistant:

1. Apply patch no. 4084712 to the release 9.2.0.6 Oracle database. This patch can be downloaded from:

   `http://metalink.oracle.com`
2. Change the max_enabled_roles parameter for the release 9.2.0.6 database to at least 100.

   To change the value to 100:

   a. Enter the following SQL command:

      ```
      SQL> ALTER system SET max_enabled_roles=100 scope=spfile;
      ```

   b. Restart the database.

   c. Check the value of the max_enabled_roles parameter using the following command:

```
SQL> select name,value from v$parameter where name='max_enabled_roles';
```

2.1.6 The lsnodes Command Fails on Non-RAC HP-UX Systems

After completing the installation, the `install*.err` files in the *`oraInventory`*`/logs` directory may contain errors similar to following line and with java exception stack details:

```
lsnodes: cannot get local node number
```

This error is harmless and can be safely ignored. It does not affect any functionality.

Similar errors may also happen when applying bug fixes using the OPatch utility. However, the patch succeeds and the error can be safely ignored.

2.1.7 Rerun OC4J Configuration Assistant If It Fails During an OracleAS Cluster (Identity Management) Installation

In Oracle Application Server Clusters (Identity Management) installations, the installer creates a DCM cluster for the Oracle Internet Directory, OracleAS Single Sign-On, and Oracle Delegated Administration Services components.

As part of the cluster creation operation, which is performed by the OracleAS Cluster Assistant, the assistant also restarts the components. DCM invokes OPMN to restart the components.

Because Oracle Internet Directory is integrated with OPMN, OPMN starts up and monitors `oidmon`. In turn, oidmon starts up Oracle Internet Directory. However, OPMN returns as soon as oidmon is up; it does not wait for Oracle Internet Directory to start up. This causes a problem because the next configuration assistant, the OC4J Configuration Assistant, requires Oracle Internet Directory to be up and running. If Oracle Internet Directory is still not running, the OC4J Configuration Assistant fails.

The workaround is to ensure that Oracle Internet Directory is successfully restarted, then rerun the OC4J Configuration Assistant.

2.1.8 Configuring Red Hat Enterprise Linux AS/ES 3.0 Systems Using ssh

If you use ssh to connect to a Red Hat Enterprise Linux AS/ES 3.0 system where you are installing Oracle Application Server, complete the following steps on that system before performing any of the tasks described in the "Requirements" chapter of the *Installation Guide*:

1. Modify the `/etc/ssh/sshd_config` file to set the UsePrivilegeSeparation parameter to `no`. For example, make sure the following line exists in the file:

   ```
   UsePrivilegeSeparation no
   ```

2. Reboot the system.
3. Start an ssh session to the system and perform the tasks described in the *Installation Guide.*

2.1.9 Warning Message from Oracle Universal Installer

You may receive the following warning message when running Oracle Universal Installer:

```
Warning : Some Patch Bundles were not found on the system. Please ensure that
either June 2003 Quality Pack GoldQPK11i has been installed or verify that
```

```
the system is at a higher bundle level.
```

You can ignore this warning.

2.1.10 Deconfiguration Script Does Not Remove Entries from OracleAS Metadata Repository

If you try to deconfigure an Identity Management instance using the deconfiguration script you will not be able to remove entries from the OracleAS Metadata Repository. This occurs when the Identity Management instance is connected to an OracleAS Metadata Repository that has been loaded by OracleAS RepCA, The OracleAS Metadata Repository cannot be reused until the following SQL queries are manually run to remove the entries:

- `SQL> execute dbms_ias_version.set_component_loading(component_id=>'MRC', component_name=>'Oracle Application Server Metadata Repository Version', schema_name=>'SYS')`
- `SQL> execute dbms_ias_version.set_component_loaded(component_id=>'MRC')`
- `SQL> execute dbms_ias_version.set_component_valid(component_id=>'MRC')`

2.1.11 Problem Running bulkload.sh Utility

When you run the bulkload.sh utility to create Oracle Internet Directory entries from data residing in or created by other applications, you may observe the following error message:

```
"SQL*Loader-951: Error calling once/load initialization ORA-39778: the parallel
load option is not allowed when loading lob columns".
```

This issue is caused by bug 3931084. Obtain and apply the patch for bug 3931084 to your Oracle Application Server installation. You can download the patch from Oracle*Metalink* (http://metalink.oracle.com).

The following are known configurations when the patch for bug 3931084 should be applied before running the bulkloa.sh utility:

- Oracle Application Server 10*g* Release 2 (10.1.2) with Oracle9*i* Database Enterprise Edition 9.2.0.X
- Oracle Application Server 10*g* Release 2 (10.1.2) with Oracle Database 10*g* Enterprise Edition 10.1.0.4

2.1.12 Software Patches for HP Itanium

Table 2-2 of *Oracle Application Server Installation Guide* 10*g* Release 2 (10.1.2) for hp HP-UX Itanium, and Linux Itanium incorrectly lists some of the software patches required for the installation. The list of patches is as follows:

Patches required for higher versions:

- PHSS_29658: Aries cumulative patch
- PHSS_29660: linker + fdp cumulative patch

Paches required when ANSI C is installed on your computer:

- PHSS_30227: HP C Compiler (A.05.52)
- PHSS_30226: aC++ Compiler (A.05.52)
- PHSS_29657: u2comp/be/plugin library Patch

2.2 Upgrade Issues

This section describes issues with the upgrade of Oracle Application Server. It includes the following topics:

2.2.1 Problems Upgrading Oracle HTTP Server on HP-UX

The following message might be displayed if you are upgrading a middle-tier installation:

```
FastCGI: failed to connect to (dynamic) server
"/opt/oracle/inst/Apache/Apache/fcgi-bin/echo": path
"/opt/oracle/inst/Apache/Apache/logs/fastcgi/dymanic/aac1cec5416b961cf002c5526b415
9" is too long for a Domain socket
```

On HP-UX, the path for sockets used by FastCGI is limited to 108 characters. If the message is displayed, use the `FastCgiIpcDir` directive to specify a path name that is significantly shorter than 108 characters, such as `/tmp` as follows:

1. Edit the `http.conf` file for the Oracle HTTP Server that you are trying to upgrade and set the `FastCgiIpcDir` directive to a short path such as `/tmp`.
2. Run the following command:

   ```
   dcmctl updateConfig -ct ohs
   ```

3. Restart the Oracle HTTP Server.
4. Restart the Upgrade process.

2.2.2 Login Link Inoperable

After you perform an upgrade of Oracle Application Server 10*g* from version 9.0.4 to version 10.1.2, the Oracle Enterprise Manager login link on the welcome page no longer works. During installation, the port number specified for Oracle Enterprise Manager for version 9.0.4 installation is not updated in the version 10.1.2 welcome pages.

There is no workaround for this issue at this time.

2.2.3 Remaining OracleAS Infrastructure Instance in Farm

After you complete an upgrade of OracleAS Infrastructure in a farm, the pre-upgrade instance of the infrastructure still remains in the farm. There is currently no way to remove the pre-upgrade instance. The remaining instance will not cause any operational problems with the upgraded infrastructure.

2.2.4 Failure of File-Based Farm Repository Configuration Assistant

If you select **Stop**, and then select **Retry** during operation of the File-Based Farm Repository Configuration Assistant in the Oracle Universal Installer, the configuration assistant fails and displays the following message:

"This instance is already a member of a farm. An Oracle Application Server instance cannot be moved directly from one farm to another."

There is presently no workaround for this issue.

2.2.5 Problems Running Oracle Universal Installer When Installing Required OracleAS Portal Patch

If you are upgrading a Release 2 (9.0.2) OracleAS Metadata Repository and you are using OracleAS Portal, then you must apply an OracleAS Portal patch before upgrading the OracleAS Metadata Repository.

> **See Also:** Section 6.3.1.1, "Downloading and Installing the OracleAS Portal 10g (9.0.4) Repository Upgrade Software" in the *Oracle Application Server 10g Upgrading to 10g (9.0.4)*

However, while using Oracle Universal Installer to install the required patch, Oracle Universal Installer may quit unexpectedly. To prevent this problem from occurring, do the following:

1. Use a text editor to open the `oraparam.ini` file, which is located in the following directory in the application server Oracle home:

   ORACLE_HOME`/oui`

2. Locate the following entry in the `oraparam.ini` file:

   ```
   JRE_MEMORY_OPTIONS=" -mx96m"
   ```

3. Modify the entry as follows:

   ```
   JRE_MEMORY_OPTIONS=" -mx160m"
   ```

4. Save your changes and close the `oraparam.ini` file.
5. Restart Oracle Universal Installer and install the patch as documented in the *Oracle Application Server 10g Upgrading to 10g (9.0.4)*.

2.2.6 Problem Running the mod_osso Configuration Assistant When Upgrading an Oracle Internet Directory in a Partial Replication Environment

When you are upgrading Identity Management in an environment where you are using Oracle Internet Directory partial replication, you may encounter a problem while running the upgrade with Oracle Universal Installer: the `mod_osso` Configuration Assistant may fail.

If this problem occurs, do not quit Oracle Universal Installer. Instead, leave the program running and perform the following workaround in a separate window:

1. Using a text editor, open the following file in the Oracle home of the replica you are upgrading:

   ORACLE_HOME/config/infratool_mod_osso.properties

2. Modify the contents of the file so it reads as follows:

```
DCMRESYNC=oracle.ias.configtool.configimpl.DcmResync$0
JAZN=oracle.security.jazn.util.JAZNConfigTool$0
HTTPD=oracle.ias.configtool.configimpl.HttpdSsoConfig$0
MODOSSO=oracle.ias.configtool.configimpl.SsoConfig$0
```

3. Save your changes and close the `infratool_mod_osso.properties` file.
4. Return to Oracle Universal Installer and try running the configuration assistant again.

2.2.7 Upgrading a Portal and Wireless Installation from 9.0.2.3 to 10.1.2 on HP-UX.

After upgrading a Portal and Wireless installation from 9.0.2.3 to 10.1.2, Oracle HTTP Server may fail to start and the following messages may be displayed:

```
OpenWallet failed with error 28759
[Tue Jan 11 20:39:27 2005] [error] mod_ossl: Failed to open the wallet [Hint:
incorrect path, incorrect password, bad wallet, ...]
```

This issue is due to the loading sequence of mod_ossl and php4. To avoid this problem make sure that the php4_module is loaded before the ossl_module:

1. Open the `$ORACLE_HOME/Apache/Apache/conf/httpd.conf` file in a text editor.
2. Search for the following text, which loads ossl_module.:

```
<IfDefine SSL>
    LoadModule ossl_module libexec/mod_ossl.so
</IfDefine>
```

3. Add the following line before the ossl_module load entry:

```
LoadModule php4_module libexec/libphp4.so
```

4. Remove any other line that loads php4_module.
5. Start the Oracle HTTP Server.

2.2.8 Problems or Issues While Upgrading Specific Components

If you experience problems or issues while upgrading a particular application server component, refer to the component chapter in these release notes for more information.

2.3 Documentation Errata

This section describes documentation errata. It includes the following topic:

- Section 2.3.1, "Safari Browser Not Supported"

2.3.1 Safari Browser Not Supported

The Safari browser is not supported in this release of Oracle Application Server 10*g*.

This is stated incorrectly in the *Oracle Application Server 10g Installation Guide*.

2.3.2 Extra Screen During Cluster Installation

Table 12-5 "Steps for Installing OracleAS Cluster (Identity Management) on Subsequent Nodes" of the *Oracle Application Server 10g Installation Guide* does not contain an entry for the Specify LDAP Virtual Hosts and Ports screen. This screen appears before the Specify OID Login screen prompting you to enter the hostname and port for LDAP virtual hosts.

2.3.3 Checking Software Requirements

Section 4.2.1 of the Installation Guide asks you to use the following command:

```
# /usr/sbin/swlist | grep QPK
```

However, this command may not list patches that were release later than June 2003 Quality Pack GoldQPK11i. Use the following command to list system software:

```
# /usr/sbin/swlist -l bundle | grep -i gold
```

If the system meets the software requirement because a later version of a package is installed, the installer may report a warning. It is safe to ignore that warning.

2.3.4 Incorrect Disk Space Requirements

Chapter 4 of the Installation Guide incorrectly lists the disk space requirements for some installations on Linux systems. A Portal and Wireless installation requires 1.1 GB and a J2EE Web Cache installation requires 700 MB.

2.3.5 Host Name Limit of 255 Characters

The information about hardware requirements in Chapter 4 of the Installation Guide should mention that for Hostname, host names must not exceed 255 characters, and this is not checked by the installation software.

2.3.6 Additional Database Option Requirement

In addition to the required options listed in Table 8, "Required Database Options" in Section 1.5.9, "Database Options" in the *Oracle Application Server Repository Creation Assistant User's Guide*, you must also include Oracle XML DB. If you do not have all of the required options, OracleAS RepCA will not run properly.

3

General Management and Security Issues

This chapter describes management and security issues associated with Oracle Application Server. It includes the following topics:

- Section 3.1, "Oracle Process Manager and Notification Server Issues"
- Section 3.2, "Distributed Configuration Management Issues"
- Section 3.3, "Other Management Issues"
- Section 3.4, "Additional Troubleshooting Topics"
- Section 3.5, "Documentation Errata"

3.1 Oracle Process Manager and Notification Server Issues

This section describes Oracle Process Manager and Notification Server (OPMN) issues. It includes the following topic:

- Section 3.1.1, "Error Message When Executing opmnctl Commands"

3.1.1 Error Message When Executing opmnctl Commands

When you execute either an `opmnctl stopall` or `opmnctl startall` command, the oidctl log file contains the following error message:

```
*** Instance Number already in use. ***
*** Please try a different Instance number. ***
```

This error message is benign and can be ignored.

This error message typically appears for OracleAS Infrastructure 10*g* installations with Oracle Internet Directory.

3.2 Distributed Configuration Management Issues

This section describes Distributed Configuration Management (DCM) issues. It includes the following topic:

- Section 3.2.1, "A Note About Port Assignments for the Oracle Application Server File-based Farm: Instance Communication Across Firewalls"
- Section 3.2.2, "Cloning and Recovery Performance Issue on HP-UX"

3.2.1 A Note About Port Assignments for the Oracle Application Server File-based Farm: Instance Communication Across Firewalls

You should understand the implications of the default port assignments for Distributed Configuration Management communication, in the case of environments that require inter-instance communication across a firewall.

The Oracle Universal Installer assigns the ports described in Table 3–1 by default when the instance is installed.

Table 3–1 Oracle Universal Installer Default Port Assignments

Quantity	Purpose/Description
1	DCM Discovery Port. The first instance installed on a computer is assigned port 7100 for this; the second instance installed on a computer is assigned 7101, and so on. This is defined in the *ORACLE_HOME*/dcm/config/dcmCache.xml file, in the discoverer element (for example, <discoverer discovery-port ="7100" original-"true" xmlns=""/>
50	Range of ports for inter-instance communication: 7120 to 7179. These are defined in the *ORACLE_HOME*/dcm/config/dcmCache.xml file, in the port element (for example, <port lower="7120" upper="7179">.) After installation, you will probably want to limit the number of ports open on the firewall. The actual port needs for inter-instance communication are: ■ 1 for the Oracle Enterprise Manager Application Server Control on each instance ■ 1 for the DCM daemon on each instance ■ 1 for each dcmctl client operating on each instance

If the ports in the range 7100 to 7179 were open on the firewall before installation, the instances in the farm will be able to communicate immediately after installation. Note that:

- If you want the port assignments to be of a different numeric range from these, then, before installation, you must assign a DCM Discovery Port using the staticports.ini file, and select the **Manual** option during installation. (See the *Oracle Application Server 10g Installation Guide*, Chapter 4, section titled "Using Custom Port Numbers (the "Static Ports" Feature)" for more information.) The range of ports will then be assigned accordingly, as specified in Table 3–1.
- After installation of all instances, configure the firewall to close the unused ports within the assigned range on each instance.

3.2.2 Cloning and Recovery Performance Issue on HP-UX

On HP-UX, the Distributed Configuration Management importArchive, cloning and recovery operation can be very slow if the archive file you are using is large. For example a 70 MB archive could take many hours to import.

To resolve this problem, download patch 4113396 from Oracle*MetaLink*:

http://metalink.oracle.com

Refer to Readme file provided with the patch for full instructions describing how to resolve this issue.

3.3 Other Management Issues

This section describes other management issues. It includes the following topics:

3.3.1 Management of Cold Failover Cluster Middle Tiers

For Cold Failover Cluster middle tiers, administration of Oracle Ultra Search using the Oracle Ultra Search administration links cannot be completed using Oracle Enterprise Manager Application Server Control(Application Server Control). The link from Application Server Control (Portal:Portal > Ultrasearch URL) does not lead to the Administration pages. Instead you will receive a Single Sign-on error.

However, the Oracle Ultra Search administration links are accessible from the OracleAS Portal pages. To get to the Oracle Ultra Search administration links:

1. Log-on to OracleAS Portal

   ```
   http://virtualhostname:port/pls/portal
   ```

2. Click **Administer**.
3. Click **Ultra Search Administration** to access the service.

3.3.2 OracleAS Disaster Recovery: Problem with Pfiles and the OracleAS Guard asgctl Instantiate Farm To Operation

Whenever a pfile is used, such as when it is required with an Oracle Application Server Cold Failover Cluster (OracleAS CFC) or when the OracleAS Administrator creates a pfile, for example, to tune the Infrastructure database and change parameters, there is a problem immediately following an OracleAS Guard asgctl instantiate farm operation when Oracle Fail Safe tries to use the pfile to try to start the ORCL instance or in any other case when the pfile is called into use to start the ORCL instance. For OracleAS CFC, Oracle Fail Safe fails to bring up the ORCL instance and generates an ORA-16033 error. In the other case, the ORCL instance fails to come up.

The problem is that during the OracleAS Guard asgctl instantiate farm operation the pfile is getting overwritten by the spfile and after this operation completes and when the pfile is called back into use it is no longer there. The workaround is to backup the pfile before running the OracleAS Guard asgctl instantiate farm operation, and immediately after this operation completes restore the pfile to its original location.

In the Oracle Application Server Disaster Recovery chapter in the *Oracle Application Server 10g High Availability Guide*, in the sections that show an instantiate farm operation, such as in Section 7.5.2 Standby Instantiation, just before Step 1 in the procedure to perform a standby instantiation operation, a new note should be added that states: If you are using a pfile, make a backup copy of your pfile before proceeding to perform an asgctl instantiate farm operation. Then immediately following Step 5 in this same section, another note should be added that states: Immediately after performing an asgctl instantiate farm operation, restore your pfile to its original location before performing any other tasks. The other sections in this chapter where these notes should be added and where the use of the OracleAS Guard instantiate farm operation is shown include Section 7.6.1.2.1 Site Failover Operations, Section 7.8.1.5 Instantiating the Farm at the Secondary Site, and Section 7.8.5 Reference Section: OracleAS Guard asgctl Command-line Commands where the instantiate farm to command is described.

3.3.3 OracleAS Disaster Recovery: In Some Scenarios, the DSA (OracleAS Guard) Component Does Not Get Registered with OPMN During the Oracle Application Server Installation

If, during the Oracle Application Server installation, you do not have a default shell, the DSA (OracleAS Guard) component registration with Oracle Process Manager and Notification Server (OPMN) fails. The script `$ORACLE_HOME/dsa/bin/addopmn.sh`, which registers the DSA component with OPMN gets run, but because there is no shell invoker (`#!/bin/sh`) specified at the beginning of the script, this `addopmn.sh` script does not get run in certain shell environments.

If you run the following OPMN command and do not see the ias-component and process-type named DSA, it means the DSA component did not get registered during the install:

```
> <ORACLE_HOME>/opmn/bin/opmnctl status
```

To workaround this problem after the installation, run the following command at the UNIX command prompt to register the DSA component with OMPN:

```
> /bin/sh <ORACLE_HOME>/dsa/bin/addopmn.sh
```

Another workaround to this problem is to put "#!/bin/sh" as the first line in the `addopmn.sh` script, then run the script as follows to register the DSA component with OPMN:

```
> <ORACLE_HOME>/dsa/bin/addopmn.sh
```

If you run the following OPMN command and see the ias-component and process-type named DSA, it means the DSA component is registered with OPMN.

```
> <ORACLE_HOME>/opmn/bin/opmnctl status
```

3.3.4 Globalization Support Settings May be Changed During Cloning

When you run the `clone.pl` script, Oracle Universal Installer creates the file `index.html` in the `$Oracle_home\Apache\Apache\htdocs` directory. As a result of the creation of this file, locale settings are overwritten.

To workaround this, rename the file to `index.html.html`.

3.3.5 Cloning and Undeploying OC4J Applications

On the source Oracle home during the prepare phase of the cloning process, do not attempt to undeploy OC4J applications while the `prepare_clone.pl` script is running.

See the *Oracle Application Server 10g Administrator's Guide* for more information about cloning.

3.3.6 Use Trusted Certificates When Enabling SSL Between mod_oc4j and OC4J

You must use trusted certificates on both ends when enabling SSL between mod_oc4j and OC4J.

Otherwise, you will get the following error when accessing the HTTPS port:

```
500 Internal Server Error
```

3.3.7 Welcome Pages Display in English in Cloned Installations

After cloning an installation using Oracle Universal Installer, the Welcome Pages in the cloned installation display in English, regardless of the locale selection.

To resolve this problem, perform the following steps in the cloned Oracle home:

```
cd $ORACLE_HOME/Apache/Apache/htdocs
mv index.html index.html.html
```

3.3.8 Benign Decoding Errors When Running ldapaddmt

Chapter 11, "Changing from a Test to a Production Environment," in the *Oracle Application Server 10g Administrator's Guide* contains steps for migrating Oracle Internet Directory data to a production environment.

These steps include running the `ldapaddmt` command, and examining the `add.log` file. The `add.log` file may contain a "Decoding Error" message. This is benign and can be ignored.

3.3.9 Missing Files During restore_config Operation

Running `restore_config` may result in missing files messages such as:

```
Could not copy file C:\Product\OracleAS\Devkit_1129/testdir/ to
C:\Product\OracleAS\Devkit_1129\backup_restore\cfg_bkp/2004-12-01_03-26-22.
```

During a `restore_config` operation, a temporary configuration backup is taken so that, if the restore fails, the temporary backup can be restored returning the instance to the same state as before the restore.

If some files are deleted (including files/directories specified in config_misc_files.inp) before a restore operation, then, during the temporary backup, messages are displayed

indicating that certain files are missing. These error/warning messages should be ignored since the missing files are restored as part of the `restore_config` operation.

3.3.10 DCM Failure Following Patch Application

Following application of RDBMS 10.1.0.4 patchset (patch number 4163362) to the *ORACLE_HOME* of Oracle Application Server 10*g*, DCM will fail with an `ADM-100992` error message. There is a DCM compatibility problem with the newer XDK that is introduced when installing the patchset or patch. The failure may not manifest itself until some time later after patchset or patch application.

To correct this issue:

- Create a DCM archive and export it on the file system for backup.
- Obtain and apply the patch for Bug:4370593 to your Oracle Application Server installation.

  Download the patch from Oracle Metalink (`http://metalink.oracle.com`). The Automatic Release Update (ARU) patch number is 7485905.

3.3.11 Mixed Version (9.0.4 and 10.1.2) Deployment of Oracle Business Intelligence Discoverer, OracleAS Reports Services, and OracleAS Portal

In Oracle Application Server 10*g* (10.1.2), there is currently not an installation type that enables deployment of OracleAS Portal with OracleAS Reports Services and Oracle Business Intelligence Discoverer (OracleBI Discoverer). The following sections describe how to enable this type of deployment with either a 9.0.4 or 10.1.2 OracleAS Infrastructure 10*g*:

- Section 3.3.11.1, "Deployment of OracleAS Portal and OracleAS Reports Services (9.0.4) with OracleBI Discoverer (10.1.2)"
- Section 3.3.11.2, "Deployment of OracleAS Reports Services (9.0.4) with OracleAS Portal and OracleBI Discoverer (10.1.2)"

3.3.11.1 Deployment of OracleAS Portal and OracleAS Reports Services (9.0.4) with OracleBI Discoverer (10.1.2)

To enable deployment of OracleAS Portal and OracleAS Reports Services (9.0.4) with OracleBI Discoverer (10.1.2) (shown in Figure 3–1), perform the following steps:

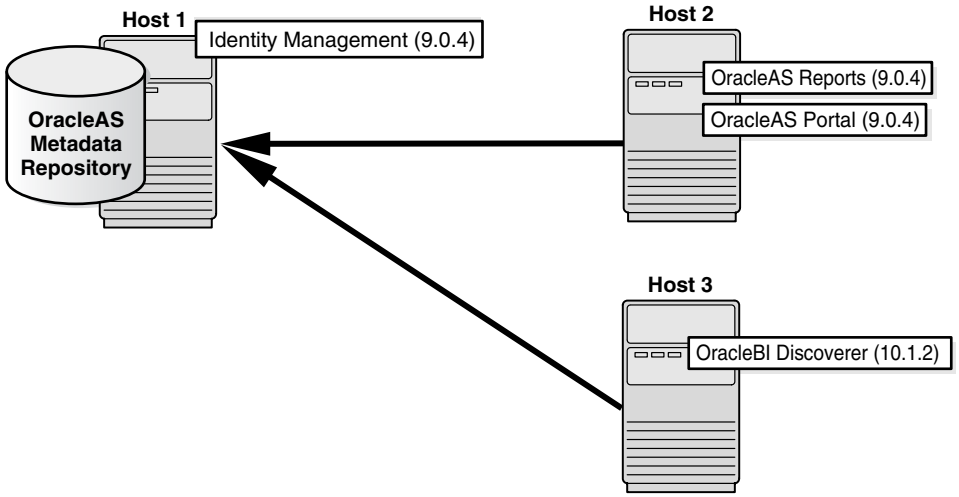
1. Install and configure OracleAS Infrastructure 10*g* Identity Management plus OracleAS Metadata Repository on Host 1.
2. Install and configure the Oracle Application Server 10g (9.0.4) Business Intelligence and Forms install type, with OracleAS Portal and OracleAS Reports Services selected, on Host 2.
3. Install and configure the version of OracleBI Discoverer (10.1.2), available from the Oracle Application Server 10g Release 2 (10.1.2.0.0) Business Intelligence installation disc, on Host 3.

   Refer to the *Oracle Business Intelligence Installation Guide* and the *Oracle Business Intelligence Discoverer Configuration Guide* for information on installation and configuration of the OracleBI Discoverer instance.
4. Run the `upgradeMR.sh` script, located in *ORACLE_HOME*`/discoverer/util`, to upgrade the `discoverer5` schema. The upgradeMR.sh script only upgrades the `discoverer5` schema.

5. Associate the instance on Host 3 to the OracleAS Metadata Repository on Host 1.

   Refer to the *Oracle Business Intelligence Discoverer Configuration Guide* for information on how to associate the Business Intelligence instance.

Figure 3–1 Deployment of OracleAS Portal and OracleAS Reports Services (9.0.4) with OracleAS Discoverer (10.1.2)



3.3.11.2 Deployment of OracleAS Reports Services (9.0.4) with OracleAS Portal and OracleBI Discoverer (10.1.2)

To enable deployment of OracleAS Reports Services (9.0.4) with OracleAS Portal and OracleBI Discoverer (10.1.2) (shown in Figure 3–2), perform the following steps:

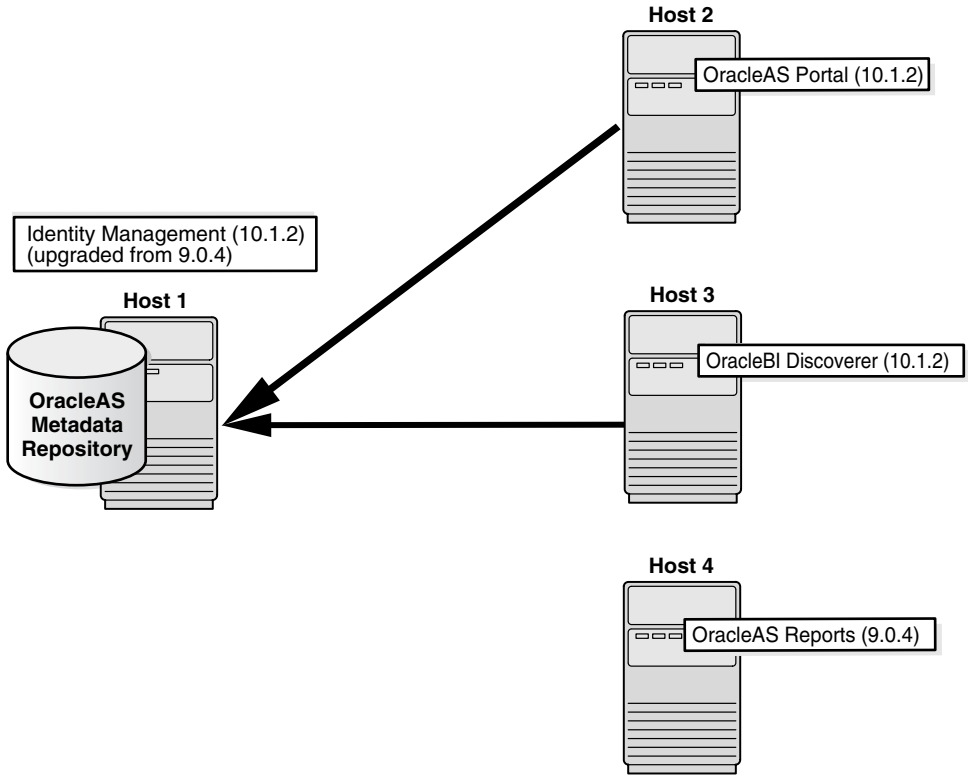
1. Install and configure Oracle Application Server 10*g* (9.0.4) Infrastructure Identity Management plus OracleAS Metadata Repository on Host 1.
2. Following installation of the Identity Management instance, upgrade the version from 9.0.4 to 10.1.2.

   For information on performing an upgrade refer to the *Oracle Application Server Upgrade and Compatibility Guide*.
3. Install and configure OracleAS Portal (10.1.2) on Host 2.
4. Install and configure OracleBI Discoverer (10.1.2) on Host 3.

   Refer to the *Oracle Business Intelligence Installation Guide* and the *Oracle Business Intelligence Discoverer Configuration Guide* for information on installation and configuration of the OracleBI Discoverer instance.
5. Associate the instance on Host 3 with the infrastructure installation on Host 1.
6. Install and configure OracleAS Reports Services (9.0.4) on Host 4.

After completing the listed steps, the OracleAS Metadata Repository is upgraded from 9.0.4 to 10.1.2. The OracleAS Portal schema contains all the portlets, including the OracleAS Reports Services portlets.

Figure 3–2 Deployment of OracleAS Reports Services (9.0.4) with OracleAS Portal and OracleAS Discoverer (10.1.2)



3.4 Additional Troubleshooting Topics

This section contains the following troubleshooting topic:

- Section 3.4.1, "OracleAS Guard "instantiate farm" Command Requires DNS Hostname, Not Alias"

3.4.1 OracleAS Guard "instantiate farm" Command Requires DNS Hostname, Not Alias

Problem

If you run the "instantiate farm" command with a hostname alias as the parameter, you get a `java.lang.OutOfMemory` error. For example, if you have a host named `host1`, and your `/etc/hosts` file contains this line:

```
166.166.166.167 host1.us.oracle.com infra
```

then you can refer to `host1` using "infra" because "infra" is an alias for `host1`.

However, you cannot use `infra` (which is an alias) as the parameter value to "instantiate farm". You must use `host1` (the DNS hostname) instead.

```
ASGCTL> instantiate farm to infra      - Results in java.lang.OutOfMemory error.

ASGCTL> instantiate farm to host1      - OK.
```

Solution

Use the DNS hostname as the parameter for the "instantiate farm" command.

3.5 Documentation Errata

This section describes documentation errata. It includes the following topic:

3.5.1 Missing Element in Common Configuration Example

Example 3-1 in the *Oracle Process Manager and Notification Server Administrator's Guide* is missing the following sub-element for the `ipaddr` element:

`local="ip"`

Required: true
Default: none
Valid Values: IP address (in ###.###.###.### format) or host name to which ONS will bind its local port. IP address or host name to which ONS will bind its local port. All local OPMN requests are routed through the local port, and all local applications connect to ONS through the local port to send and receive notifications.

3.5.2 Incomplete Sentence

Section 4.5, "Oracle HTTP Server 2" of the *Oracle Process Manager and Notification Server Administrator's Guide* contains the following incomplete sentence:

"Oracle does not support the for each child MPM."

The sentence should be:

"Oracle does not support the perchild MPM."

3.5.3 Reference to Nonexistent Files

Section 3.2 of the *Oracle Application Server 10g Administrator's Guide* refers to scripts on an OracleAS RepCA and Utilities CD-ROM. This is incorrect.

Because of improvements to OPMN, there is no longer any need for the scripts and they are not shipped with Oracle Application Server 10*g*.

3.5.4 Incorrect Archivelog Mode Instructions

In Section 19.2.2, "Enabling ARCHIVELOG Mode" of the *Oracle Application Server 10g Administrator's Guide*, in Step 1. of "To enable ARCHIVELOG mode:", the following command example:

```
alter system set log_archive_dest='xxx' scope=spfile;
```

should be:

```
alter system set log_archive_dest_n = "location=<your_desired_backup_directory>"
scope=spfile;
```

where `n` is a number between 1 and 10 and `location` is your backup directory location.

3.5.5 Incorrect Figure Reference in Oracle Application Server 10g High Availability Guide

The following two incorrect figure references occur in Section 5.3.2.3 OracleAS Cold Failover Cluster (Identity Management) of the *Oracle Application Server 10g High Availability Guide*:

- In the following paragraph, the reference to Figure 5-8 should be in the last sentence of the paragraph:

  "This database can be a Real Application Clusters database that is already installed in the hardware cluster (shown in Figure 5-8). Alternatively, the database can be in a cold failover cluster configuration."

  Should be:

  "This database can be a Real Application Clusters database that is already installed in the hardware cluster. Alternatively, the database can be in a cold failover cluster configuration (shown in Figure 5-8)."

- The following paragraph is incorrect and should be ignored:

  "Both Oracle Identity Management and OracleAS Metadata Repository are active in Node 1. In Node 2, all components are passive, on standby, unless the database that contains the OracleAS Metadata Repository is a Real Application Clusters database. In this case, the database instance is active on Node 2."

4

Oracle Application Server FIPS 140-2 Settings

Oracle Application Server 10*g* (9.0.4) received FIPS 140-2 Level 2 certification. The security policy for this certification is available at `http://csrc.nist.gov/cryptval/140-1/140sp/140sp447.pdf`.

This chapter describes how to configure Oracle Application Server components to comply with the FIPS 140-2 advanced security standard. For more information about this standard, refer to the Cryptographic Modules Validation Program Web site at the following address:

`http://csrc.nist.gov/cryptval/`

The following topics are covered in this chapter:

4.1 Configuration

Any component in any Oracle Application Server instance that uses SSL can be configured to be FIPS compliant. Specifically, the Oracle Application Server components that can be configured are:

- Oracle HTTP Server
- OracleAS Web Cache
- Oracle Internet Directory
- `mod_oc4j`

The security policy document includes requirements for secure configuration of the host operating system.

4.1.1 Setting the SQLNET.SSLFIPS_140 Parameter

All of these components can be configured to run in FIPS mode by setting the `SQLNET.SSLFIPS_140` parameter to TRUE in the `sqlnet.ora` file:

```
SQLNET.SSLFIPS_140=TRUE
```

By default, this parameter is set to FALSE.

Make sure that the sqlnet.ora file is either located in the *ORACLE_HOME*/network/admin directory, or is pointed to by the TNS_ADMIN environment variable. This procedure can be repeated in any Oracle home for any applicable component.

Note: You must add or edit the SQLNET.SSLFIPS_140 parameter in the sqlnet.ora file with a text editor. You cannot use Oracle Net Manager to set this parameter.

4.1.2 Selecting Cipher Suites

A cipher suite is a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During an SSL handshake, for example, the two nodes negotiate to see which cipher suite they will use when transmitting messages back and forth.

Only the cipher suites listed below are approved for FIPS validation:

- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA

These SSL cipher suites are automatically configured for Oracle Internet Directory and mod_oc4j. For Oracle HTTP Server, specify the SSLCipherSuite directive in the corresponding httpd.conf file as follows:

```
SSLCipherSuite <FIPS_approved_cipher_suite[:additional_FIPS_approved_cipher_
suites]>
```

See Also: The "Using mod_ossl Directives" section in "Chapter 10, Managing Security" in the *Oracle HTTP Server Administrator's Guide*.

Please note that multiple cipher suites can be specified, delimited with the colon (:) character. In order to use the FIPS approved cipher suites for OracleAS Web Cache, ensure that the Strong Crypto option is not enabled.

If an application uses separate virtual hosts, ensure that the SSLCipherSuite directive is set appropriately in the corresponding configuration file. For example, OracleAS Certificate Authority uses two additional virtual hosts, meaning the SSLCipherSuite directives in the ocm_apache.conf file (located in the same directory as the httpd.conf file) must be configured with the approved cipher suites.

4.2 Post-Installation Checks

After the installation, the following permissions must be verified in the operating system:

- Execute permissions must be set on all Oracle executable files to prevent execution of Oracle Cryptographic Libraries by users who are unauthorized to do so in accordance with the system security policy.

- Read and write permissions must be set on all Oracle executable files to prevent accidental or deliberate reading or modification of Oracle Cryptographic Libraries by any user.

To comply with FIPS 140-2 Level 2 requirements, the system security policy must include procedures to prevent unauthorized users from reading, modifying, or executing Oracle Cryptographic Libraries processes and the memory those processes are using in the operating system.

4.3 Verifying FIPS Connections

To check if FIPS mode is enabled, tracing can be added to the `sqlnet.ora` file. FIPS self-tests messages can be found in the trace file. Add the following lines to `sqlnet.ora` to enable tracing:

```
trace_directory_server=<trace_dir>
trace_file_server=<trace_file>
trace_level_server=<trace_level>
```

For example:

```
trace_directory_server=/private/oracle/owm
trace_file_server=fips_trace.trc
trace_level_server=6
```

Trace level 6 is the minimum trace level required to check the results of the FIPS self-tests.

5

Oracle Application Server Containers for J2EE (OC4J)

This chapter discusses release notes for the following topics:

- Section 5.1, "Configuration Issues and Workarounds"
- Section 5.2, "Release Notes for EJB"
- Section 5.3, "Release Notes for OC4J Services"
- Section 5.4, "Release Notes for JSP"
- Section 5.5, "Release Notes for Documentation Errata"

You can access Oracle manuals mentioned in this document at the following URL:

`http://www.oracle.com/technology/index.html`

5.1 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds for OC4J. It contains the following topics:

- Section 5.1.1, "Oracle JDBC OCI Driver Problem on Linux Itanium and Windows Itanium"
- Section 5.1.2, "OC4J OutofMemory Errors"

For information on configuring OC4J, refer to the *Configuration Guide for OC4J* at

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

5.1.1 Oracle JDBC OCI Driver Problem on Linux Itanium and Windows Itanium

When accessing the Oracle Database, the Oracle Application Server uses either the type 2 JDBC-OCI driver or the type 4 JDBC-Thin driver. However, on Linux Itanium and Windows Itanium platforms, using Sun JVM (Hotspot), we have identified a bug reference 6227954 (http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6227954) which prevents the Oracle Application Server from using the JDBC-OCI driver. Oracle and Sun are actively and jointly working toward the resolution of this issue. Meanwhile, as a workaround, we recommends that Oracle Application Server customers use the Oracle JDBC-Thin driver, in Sun JVM environment, on Itanium-2 systems.

5.1.2 OC4J OutofMemory Errors

If the heap size of the default Java virtual machine (JVM) of OC4J is too small for applications that you deploy, then you might get `OutofMemory` errors from your OC4J processes. If you review the log files for the OC4J instance in the directory `$ORACLE_HOME/opmn/logs`, then you might find errors similar to the following:

```
java.lang.OutOfMemoryError
```

To work around this problem, increase the specified heap memory by changing the Java command line options for the OC4J Instance.

Using Application Server Control Console, navigate to the OC4J instance homepage and perform the following steps:

1. Stop the OC4J Instance.
2. Navigate to the Server Properties page.
3. In the Command Line Options area of the Server Properties page, the heading Multiple VM Configuration, set the options for Java.

   For example, enter the following to set the JVM heap sizes to 512 Megabytes:

   ```
   -Xmx512m
   ```

4. Click **Apply**.
5. Start the OC4J instance.

For more information, refer to the *Oracle Application Server 10g Performance Guide*.

5.2 Release Notes for EJB

This section describes release notes for Enterprise Java Beans (EJB). It covers the following topics:

- Section 5.2.1, "Deprecated orion-ejb-jar.xml Attributes"
- Section 5.2.2, "Big EAR File Deployment Runs Out of Memory"
- Section 5.2.3, "EJB Wrapper Code Compilation Fails When Running in zh_CN.GB18030 Locale."

5.2.1 Deprecated orion-ejb-jar.xml Attributes

The following `orion-ejb-jar.xml` attributes are deprecated in releases 9.0.4.1 and 10.1.2:

- `max-instances-per-pk`
- `min-instances-per-pk`
- `disable-wrapper-cache`
- `disable-wrapper-cache`

In addition, the following `locking-mode` attribute setting is deprecated:

```
locking-mode="old_pessimistic"
```

5.2.2 Big EAR File Deployment Runs Out of Memory

`OutOfMemory` exceptions occur when deploying Enterprise Archive File (EAR) files with a large number of EJBs.

As part of the deployment process, wrapper code classes are generated for each EJB. The size of these classes is proportional to the number of business methods on the bean. As a performance optimization, OC4J compiles all wrapper code classes in one compiler invocation. An error can occur if the amount of generated wrapper code is excessive for available memory.

A workaround for the problem is to direct the deployment process to compile each EJB module's wrapper code individually. You can do this by starting OC4J as follows:

```
-Dejbdeploy.batch=false
```

Note: The preceding workaround should only be used when this specific exception occurs. The workaround may result in an increased deployment time for the application.

5.2.3 EJB Wrapper Code Compilation Fails When Running in zh_CN.GB18030 Locale.

The compilation of EJB wrapper code fails when running in `zh_CN.GB18030` locale. When running in `zh_CN.GB18030` locale, parts of the source code of EJB wrapper may be generated with missing characters. This causes compilation errors. The missing characters in the generated source code are due to a Sun bug documented at the following URL:

`http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4954023`

The workaround is to use a different locale. Refer to the Sun bug 4954023 for details.

5.3 Release Notes for OC4J Services

This section describes release notes for OC4J services. OC4J Services include:

- Java Naming and Directory Interface (JNDI)
- Java Message Service (JMS)
- Data Sources
- Oracle Remote Method Invocation (ORMI)
- J2EE Interoperability (IIOP)
- Java Transaction API (JTA)
- J2EE Connector Architecture (J2CA)
- Java Object Cache

The section contains the following release notes:

- Section 5.3.1, "ORMI - OC4J Only Creates IPv4 Sockets"
- Section 5.3.2, "Security of ORMI Protocol"
- Section 5.3.3, "Enabling IIOP in OC4J"

5.3.1 ORMI - OC4J Only Creates IPv4 Sockets

OC4J only creates Internet Protocol version 4 (IPv4) sockets. Even on stack machines of dual network (with both IPv4 and IPv6 stacks available), OC4J creates only IPv4 sockets. This may cause a problem if client-issued requests are from a IPv6 system. This is indicated by connection-refused messages from the server to the IPv6 client. To

avoid this problem, start the client process with the system property `java.net.preferIPv4Stack=true`. This forces the client to only issue IPv4 requests, allowing it to communicate with the server.

5.3.2 Security of ORMI Protocol

It should be noted that the ORMI protocol is not secure. All communication over ORMI is not encrypted including security credentials. Customers who want to encrypt ORMI traffic should use ORMI over HTTPS, which will encrypt all communication between the client and the server.

5.3.3 Enabling IIOP in OC4J

This section describes the steps necessary to enable Internet Inter-ORB Protocol (IIOP) applications in OC4J. After performing the steps you should be able to:

- Access a remote EJB over IIOP
- Secure EJB invocations with IIOP over SSL
- Secure corba name lookups by remote clients with IIOP over SSL

To minimize deployment and configuration changes, the document uses the demo `helloworld` EJB application available through the installation and on OTN:

`http://www.oracle.com/technology/sample_code/tech/java/ejb_corba/index.html`

Building and deploying the `helloworld` application with a default OC4J installation results in an application that is only accessible over ORMI. To enable IIOP for a given application, you must perform the following changes to OC4J's server configuration and the client application. The required changes include:

- Configure the `IIOPServerExtensionProvider`
- Change the `java.naming.provider.url`
- Deploy the application using the `-iiopClientJar` argument

The steps are as follows:

- Getting Started
- Configuring IIOP in OC4J
- Configuring the JNDI provider URL
- Building and Deploying the Application

The following sections describe the steps in detail:

Getting Started

Expand the EJB demos in your development environment. The `helloworld` application should be available at the `<install-dir>/demo/ejb/helloworld` directory with the following structure:

```
|-------dist
|-------etc
|       |-------application-client.xml
|       |-------application.xml
|       |-------ejb-jar.xml
|       |-------jndi.properties
|-------src
|       |-------ejb
```

```
|       |       |-------client
|       |       |       |-------HelloClient.java
|       |       |-------helloworld-ejb
|       |               |-------Hello.java
|       |               |-------HelloBean.java
|       |               |-------HelloHome.java
|       |               |-------HelloLocal.java
|       |               |-------HelloLocalHome.java
|------build.xml
```

Applications other than the `helloworld` example can be ignored for the remaining document, but changes required for enabling IIOP will not affect the applications. This document shows the installation of the demos to the root partition, so the application is under `/demo/ejb/helloworld`.

The supplied `Ant` build file provides targets for compiling the `src`, building the `jar` and ear, and running the client application. It is assumed that you are familiar with `Ant` build files. If you are unfamiliar with `Ant`, then please refer to Apache's Ant documentation site:

http://ant.apache.org/manual/index.html

Configuring IIOP in OC4J

Edit the `server.xml` file as follows:

```
  <install-dir>j2ee/home/config/internal-settings.xml
```

Ensure that the server.xml file contains the following line:

```
<sep-config path="./internal-settings.xml" />
```

If the line is missing, or commented out, remove the comments or add the line subsequent to the following line:

```
<rmi-config path="./rmi.xml" />
```

This configures `IIOPServerExtensionProvider` for OC4J.

Now edit the `internal-settings.xml` file to configure your IIOP settings as follows:

```
  <install-dir>j2ee/home/config/internal-settings.xml
```

Ensure that the file contains the following settings:

```
<server-extension-provider name="IIOP"
   class="com.oracle.iiop.server.IIOPServerExtensionProvider">
   <sep-property name="port" value="5555" />
   <sep-property name="host" value="localhost" />
   <sep-property name="ssl" value="false" />
   <sep-property name="trusted-clients" value="*" />
</server-extension-provider>
```

If necessary, you can modify the host and port to match your development environment. If your file contains entries for SSL, then temporarily comment them out as follows:

```
<!--
   <sep-property name="ssl-port" value="5556" />
   <sep-property name="ssl-client-server-auth-port" value="5557" />
   <sep-property name="keystore" value="keystore.jks" />
   <sep-property name="keystore-password" value="->pwForSSL" />
```

```
   <sep-property name="truststore" value="truststore.jks" />
   <sep-property name="truststore-password" value="->pwForSSL" />
-->
```

Now OC4J is configured for IIOP. The final step to enable IIOP on the server side is to start OC4J with the JVM argument: `-DgenerateIIOP=true`. This can be done through the command line for OC4J standalone, and in the `${ORACLE_HOME}/opmn/opmn.xml` file for Oracle Application Server installations.

Configuring the JNDI provider URL

Edit the `jndi.properties` file as follows for the `helloworld` application:

```
<install-dir>/demo/ejb/helloworld/etc/jndi.properties

java.naming.factory.initial=com.evermind.server.ApplicationClientInitialContextFac
tory
java.naming.provider.url=corbaname:iiop:localhost:5555#helloworld
#java.naming.provider.url=ormi://localhost:23791/helloworld
java.naming.security.principal=admin
java.naming.security.credentials=welcome
```

Comment out the line containing the ORMI provider URL, and add a line matching the `corbaname` provider URL in the example.

Building and deploying the application

From the `<install-dir>/demo/ejb/helloworld` directory, run the default Ant target to build the application:

```
<install-dir>/demo/ejb/helloworld > ant
```

First start OC4J if you have not done so already, and then execute the following deploy command:

```
java -jar ${J2EE_HOME}/admin.jar ormi://localhost:23791 admin welcome -deploy
-file dist/helloworld.ear -deploymentName helloworld -iiopClientJar
dist/helloworld_iiop_client.jar
```

This deploys the `helloworld` application and generates the client EJB JAR containing the client IIOP stubs in `dest/helloworld_iiop_client.jar`.

Running the application

Edit the `<install-dir>/demo/ejb/common.xml` file, and ensure that the environment settings for `ORACLE_HOME`, `JAVA_HOME`, and `J2EE_HOME` match your environment.

Execute `ant run`.

You should refer to the appropriate `Hello ...` response from the client application. To verify that communication is running over IIOP, you can set the following JMV arguments on both the client and server:

```
-Diiop.runtime.debug=true
```

Enable IIOP over SSL on the server

Edit the `internal-settings.xml` file and uncomment or add the SSL settings (indicated by the bold lines in the following example):

```
<server-extension-provider name="IIOP"
```

```
   class="com.oracle.iiop.server.IIOPServerExtensionProvider">
   <sep-property name="port" value="5555" />
   <sep-property name="host" value="localhost" />
   <sep-property name="ssl" value="true" />
   <sep-property name="trusted-clients" value="*" />
   <sep-property name="ssl-port" value="5556" />
   <sep-property name="ssl-client-server-auth-port" value="5557" />
   <sep-property name="keystore" value="keystore.jks" />
   <sep-property name="keystore-password" value="yourPWD" />
   <sep-property name="truststore" value="truststore.jks" />
   <sep-property name="truststore-password" value=" yourPWD " />
</server-extension-provider>
```

If necessary, you can modify the host and port to match your environment. The keystore and truststore files may refer to the same physical file. The file names mentioned are only for illustration. If you do not have a keystore file, then you can use the following Sun example for using the keytool:

http://java.sun.com/docs/books/tutorial/security1.2/summary/tools.html

Add the absolute path and filename to the keystore and truststore properties in the example.

Enable SSL on the client

Edit the `jndi.properties` file for the `helloworld` application:

```
<install-dir>/demo/ejb/helloworld/etc/jndi.properties
java.naming.factory.initial=com.evermind.server.ApplicationClientInitialContextFac
tory
java.naming.provider.url=corbaname:iiop:localhost:5556#helloworld
java.naming.security.principal=admin
java.naming.security.credentials=welcome
```

In the provider URL, change the port to the SSL port from `internal-settings.xml`.

Create a file called `ejb_sec.properties` for the `helloworld` application:

```
oc4j.iiop.trustedServers=*
nameservice.useSSL=true
oc4j.iiop.trustStoreLoc=<path to server's keystore>
oc4j.iiop.trustStorePass=<password for server's keystore file>
```

This file communicates the requirements for applications security to the OC4J client bootstrap classes. The properties in this example indicate that SSL should be used for EJB lookups, and that all servers supporting SSL should be trusted. The truststore setting is a quick way of using the same keystore configured for OC4J instead of importing the certificate in the servers keystore to a second truststore file.

Run the application with IIOP over SSL

Execute `ant run`.

You should refer to the appropriate `Hello ...` response from the client application. To verify that communication is running with IIOP over SSL, set the `-Diiop.runtime.debug=true` for both the client and server.

5.4 Release Notes for JSP

This section describes known issues for JSP. It includes the following topics:

5.4.1 JSP Compilation Problems on HP-UX Itanium

If you try to compile JSP code containing references to the `sun.tools.javac.Main` class the following message is displayed and the code does not compile on HP-UX Itanium:

```
oracle.jsp.provider.jspcomplieexception
```

Use either of the following methods to avoid this problem:

- Do not include `tools.jar` in the CLASSPATH variable.
- Set the use_old_compiler initialization parameter to false in the `global-web-application.xml` file

5.5 Release Notes for Documentation Errata

This section describes known errors in the OC4J documentation in Oracle Application Server 10g Release 2 (10.1.2). It contains the following topics:

5.5.1 OC4J User's Guide Errata

This section describes known errors in the *Oracle Application Server Containers for J2EE User's Guide*. It includes the following topics:

5.5.1.1 An OC4J Process Is Not Contained in an OC4J Instance

The following incorrect statement appears in the *Oracle Application Server Containers for J2EE User's Guide* Chapter 8, OC4J Clustering:

"Each OC4J process is contained in an OC4J instance and inherits its configuration from the OC4J instance. All applications deployed to an OC4J instance are deployed to all OC4J processes in the OC4J instance."

The statement is incorrect because an OC4J process as such can only be contained in other processes and an OC4J instance is not a process.

The correct statement in this case is:

"Each OC4J process is associated to an OC4J instance and inherits its configuration from that OC4J instance. All applications deployed to an OC4J instance are started in all the OC4J processes associated to that OC4J instance."

5.5.1.2 Correct Cross Reference for Metric-Based Load Balancing Information

In the description of the `<metric-collector>` element of the `server.xml` file in Appendix B - Additional Information of the *Oracle Application Server Containers for J2EE User's Guide*, the following incorrect cross reference is given:

"For details on using the `<metric-collector>` element and using metric-based load balancing with mod_oc4j, see the *Oracle Application Server 10g Performance Guide*."

Replace the incorrect cross-reference with the following correct cross-reference:

For details on using metric-based load balancing with `mod_oc4j`, refer to the *Oracle HTTP Server Administrator's Guide*.

5.5.2 Oracle XML API Reference Errata

This section describes known errors in *Oracle XML API Reference*. It includes the following topics:

- Section 5.5.2.1, "Add Information for formDocument() Method"

5.5.2.1 Add Information for formDocument() Method

In the *Oracle XML API Reference Guide*, Chapter 15, "Package Dom APIs for C++", add the following entries:

- On page 15-22, in Table 15-7 *"Summary of DOMImplRef Methods; Dom Package"*, add an entry for `formDocument()` method, description: "Forms a document reference given a pointer to the document."
- On page 15-24, add the following method description:

  `formDocument()`

  Description

  Forms a document reference given a pointer to the document.

  Syntax

```
DocumentRef< Node>* formDocument( Node* node);

-------------------------------------------------
```

  Parameter **Description**

```
-------------------------------------------------
```

  node Pointer to the document node.

```
-------------------------------------------------
```

  Returns

  `DocumentRef< Node>*` pointer to the document reference.

5.5.3 OC4J Services Guide Errata

This section describes known errors in *OC4J Services Guide*. It includes the following topics:

- Section 5.5.3.1, "Correct SQLServer Data Source Example"

5.5.3.1 Correct SQLServer Data Source Example

On page 4-24 in *"Example DataDirect Data Source Entries"*, the *Oracle Application Server Containers for J2EE Services Guide* shows the following example as a data source entry for SQLServer. However, the example is incorrect, a colon is missing.

```
@ url="jdbc:sqlserver//hostname:port;User=test;Password=secret"
```

The correct example is as follows:

```
@ url="jdbc:sqlserver://hostname:port;User=test;Password=secret"
```

5.5.4 OC4J Security Guide Errata

This section describes known errors in the OC4J Security Guide. It includes the following topics:

- Section 5.5.4.1, "Allowed Values for establish.trust Elements"
- Section 5.5.4.2, "The external.synchronization Property Is No Longer Supported"
- Section 5.5.4.3, "Define Roles in Lower Case for Third-Party LDAP Logins"
- Section 5.5.4.4, "Removing Realm Names From Principals"

5.5.4.1 Allowed Values for establish.trust Elements

Chapter 15, "Configuring CSIv2" incorrectly describes the values of the `<establish-trust-in-target>` and `<establish-trust-in-client>` elements. The `<establish-trust-in-target>` element can accept only the supported values and none. It cannot take the value required. The `<establish-trust-in-client>` element can take the values required, supported, and none.

5.5.4.2 The external.synchronization Property Is No Longer Supported

The `<jazn>` property external.synchronization is no longer supported.

5.5.4.3 Define Roles in Lower Case for Third-Party LDAP Logins

In Chapter 9, "Configuring External LDAP Providers", you should be aware of the following issue.

Applications that use third-party LDAP providers must define all deployment roles using lowercase only. Using uppercase letters in role names will cause authorization failures. When you define deployment roles in orion-application.xml, be sure to map all logical roles to lower-case names only.

The following snippet demonstrates valid and invalid deployment role names.

```
<security-role-mapping name="sr_developer">  <!- Logical role -->
   <group name="developers" />   <!-  Valid deployment role -->
</security-role-mapping>
<security-role-mapping name="jr_developer"> <!-  Logical role -->
   <group name="JuniorDevelopers" /> <!- Invalid deployment role;
                                                                    causes
authorization failure -->
</security-role-mapping>
```

5.5.4.4 Removing Realm Names From Principals

In Chapter 4, "Overall Security Configuration", the section "Removing Realm Names From Principals" is incomplete. The `jaas.user.simplename` property, `<propertyname="jaas.username.simple" value="true" />`, may be set only in the following instance-specific `jazn.xml` file:

```
$ORACLE_HOME/j2ee/$INSTANCE/config/jazn.xml
```

This property affects only the specified OC4J instance. Setting this property in orion-application.xml has no effect.

6

Oracle HTTP Server

This chapter describes issues associated with Oracle HTTP Server. It includes the following topics:

6.1 General Issues and Workarounds

This section describes general issues and workarounds. It includes the following topic:

6.1.1 OC4J Plug-in Usage with Standalone and Core Installation

To use the Oracle Application Server Containers for J2EE (OC4J) plug-in with the OC4J standalone product without OPMN, only static routing to specific hosts and ports is allowed within the OC4J plug-in. OC4J must be configured to use Apache JServ Protocol (AJP). Using static routing with hosts and ports means that only `Oc4jMount` directives such as the following are supported:

```
Oc4JMount /j2ee/* ajp13://localhost:6001,localhost:6002
```

To enable AJP in the OC4J configuration, a line such as the following must be present in the `default-web-site.xml` file in the OC4J configuration:

```
<web-site port="3000" protocol="ajp13" display-name="OracleAS Java Web Site">
```

In this example, where the `web-site port` value specifies the port at which the OC4J process will listen for incoming AJP requests.

6.2 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds. It contains the following topic:

6.2.1 FastCGI Sockets Path Length Error

On most platforms, the path for sockets used by FastCGI is limited to 108 characters. If an error such as the following is encountered, use the `FastCgiIpcDir` directive to specify a path name that is significantly shorter than 108 characters, such as `/tmp`:

```
Thu Oct 16 12:55:06 2003] [error] [client 148.87.9.44] [ecid: 82608810576,1]
FastCGI: failed to connect to (dynamic) server
"/opt/oracle/inst/Apache/Apache/fcgi-bin/echo": path
"/opt/oracle/inst/Apache/Apache/logs/fastcgi/dymanic/aac1cec5416b961cf002c5526b415
9"
is too long for a Domain socket
```

6.2.2 Oracle HTTP Server Does Not Start After Enabling Port Tunneling or SSL in mod_oc4j

Oracle HTTP Server might not start if you modify its configuration to enable port tunneling (iASPT), or SSL in `mod_oc4j`. Following are the possible solutions for this issue:

- Recommended solution: if `mod_perl` is not needed, disable it by commenting out the `LoadModule perl_module libexec/libperl.so` line from `httpd.conf`.
- If `mod_perl` is needed, ensure that you are running the latest patch set from Sun, and move the `LoadModule` line for `mod_perl` until after the include of `mod_oc4j.conf` in `httpd.conf`.

6.2.3 Redirects Break If OracleAS Web Cache is Turned Off or is Disabled

By default, Oracle HTTP Server sends redirects to the OracleAS Web Cache listening port. If OracleAS Web Cache is not running or is disabled, then redirects from Oracle HTTP Server (and any OC4J application behind Oracle HTTP Server) will not work. If you are not planning to run OracleAS Web Cache, then edit httpd.conf and ssl.conf, changing the Port directive so that it matches the Listen directive instead of the OracleAS Web Cache listening port.

7

Oracle Application Server TopLink

This chapter describes the general issues and workarounds in Oracle Application Server TopLink 10*g* (9.0.4.5). It includes the following topics:

7.1 Known Issues

The following issues exist in OracleAS TopLink 10*g* (9.0.4.5):

7.1.1 oracle.sql.TIMESTAMP

When using Oracle JDBC 9.0.1 driver, `resultSet.getTimestamp(int)` returns `oracle.sql.TIMESTAMP`, instead of `java.sql.Timestamp`. As a result, `oracle.sql.TIMESTAMP` is stored in DatabaseRow. Although OracleAS TopLink converts `oracle.sql.TIMESTAMP` to `java.sql.Timestamp` at a later stage for a successful read, serialization on an attribute of `ValueHolderInterface` type representing an object mapped to `TIMESTAMP` field will fail because `DatabaseRow` is an attribute of `ValueHolder` and `oracle.sql.TIMESTAMP` is not serializable.

7.1.2 XML Parser Dependencies

This section describes the following XML parser dependency issues:

- Section 7.1.2.3, "Crimson XML Parser Issue"

7.1.2.1 OC4J XML Parser Dependency

By default, both OC4J and OracleAS TopLink use the OracleAS XML Parser for Java v2. When using OC4J and OracleAS TopLink together, ensure that both use the same version of OracleAS XML Parser for Java v2. Failure to do so may result in XML parsing failures and application errors.

To determine what version of OracleAS XML Parser for Java v2 is used in your OracleAS TopLink installation:

1. Display the comment associated with the `<ORACLE_HOME>/lib/xmlparserv2.jar` file (where `<ORACLE_HOME>` is the directory in which you installed OracleAS TopLink).

   a. On Microsoft Windows, configure WinZip to display comments by selecting **Option**s and then **Configuration**. Select the **Miscellaneous** tab, and ensure that the **Show comments when opening Zip files** check box is checked. Open the `<ORACLE_HOME>\lib\xmlparserv2.jar` file with WinZip.

   b. On UNIX, use the following file:

      ```
      unzip -l <ORACLE_HOME>/lib/xmlparserv2.jar
      ```

   The comment shows the build that this version of OracleAS XML Parser for Java v2 belongs to.

2. Ensure that this build is the same as the build associated with the OracleAS XML Parser for Java v2 used in OC4J.

7.1.2.2 OracleAS TopLink 10*g* (9.0.4.5) with BEA WebLogic Application Server, 8.1

When you install OracleAS TopLink in conjunction with the Oracle Application Server 10*g* Release 2 (10.1.2) installation, changes introduced to the OracleAS XML Parser for Java v2 in 10*g* Release 2 (10.1.2) can cause issues for users that use OracleAS TopLink 10*g* (9.0.4.5) in conjunction with BEA WebLogic Application Server, 8.1 (BEA **`CR136750`**).

You will encounter `NoSuchMethodError` associated with the constructor of the `javax.xml.namespace.QName` class. To resolve this problem, users must download the Sun Web Services Development Kit from Sun and place the `jax-qname.jar` file on their classpath before both the `toplink.jar` and the `weblogic.jar` entries.

To download the Sun Web Services Development Kit, navigate to `http://www.sun.com/`

7.1.2.3 Crimson XML Parser Issue

Crimson (`http://xml.apache.org/crimson/`) is the XML parser supplied in the Java 2 Platform Standard Edition (J2SE) and in some JAXP reference implementations.

If you use Crimson with the JAXP API to parse XML files whose system identifier is not a fully qualified URL, then XML parsing will fail with a not valid URL exception.

Other XML parsers defer validation of the system identifier URL until it is specifically referenced.

If you are experiencing this problem, then consider one of the following alternatives:

- Ensure that your XML files use a fully qualified system identifier URL.
- Use another XML parser such as the OracleAS XML Parser for Java v2.

7.1.3 UTF-8 Encoding Exceptions

In 10*g* (9.0.4.5), OracleAS TopLink only supports UTF-8 encoding. The `SAXParseException` with OracleAS TopLink Exception **Error Code 9006** occurs if you attempt to read a non-UTF-8 formatted XML file.

7.1.4 Prepared Statements may Fail to Execute After a Loss of Communication to the Database

If you configure a `Login` or `Query` to use statement caching and communication to the database is lost and restored, then previously cached statements may fail to execute.

For example, it is a common practice to define an exception handler and register it with a `Session` using `Session.setExceptionHandler()`. When the exception handler is invoked to handle a loss of communication and the handler re-establishes the connection to the database, any attempt to reexecute a previously cached statement will fail.

7.1.5 Using Oracle Application Server TopLink with IBM WebSphere 5.1

When using OracleAS TopLink with WebSphere Application Server 5.1, we recommend that applications should be configured and deployed with their class loader mode set to `PARENT_LAST`.

To configure an application with its class loader mode set to `PARENT_LAST`, select one of the following options:

- Remove (or rename) the *<JAVA_HOME>*`/lib/jaxp.properties` file, where `<JAVA_HOME>` refers to *<WebShpere_Install>*`/java/jre`.
- Place the **xerces** library included in the WebSphere installation after `xmlparserv2.jar` in the same shared library. This file is located in *<WebShpere_Install>*`/java/jre/lib/xml.jar`.

7.1.6 OracleAS TopLink Mapping Workbench

The following issues exist in OracleAS TopLink Mapping Workbench 10*g* (9.0.4.5):

7.1.6.1 Mapping Inherited Attributes

You cannot map inherited attributes on a descriptor whose superclass has no descriptor. You can select the root descriptor, but cannot map its attributes.

In order to map the project, import the superclass into the project. OracleAS TopLink Mapping Workbench creates a descriptor for the superclass. Then, deactivate this descriptor or remove it from the project.

7.1.6.2 Changing Classes in Code

If you change a descriptor to an interface or abstract class in code (outside of OracleAS TopLink Mapping Workbench), then when you refresh the class in OracleAS TopLink Mapping Workbench, you may get an `ExternalClassNotFoundException`.

For example, a project contains two descriptors: **Employee** and **EmployeeInterface**. Both are classes and **Employee** extends **EmployeeInterface**. Outside of OracleAS TopLink Mapping Workbench you edit the **EmployeeInterface** code to change it to an interface and make **Employee** implement the interface. When you refresh the classes in OracleAS TopLink Mapping Workbench, you will receive the error.

To avoid this situation, refresh **EmployeeInterface** first, then refresh **Employee**.

7.1.6.3 Refreshing Descriptors with Dependent Classes

When you refresh a descriptor, the OracleAS TopLink Mapping Workbench does not refresh dependent classes if they are not included in the OracleAS TopLink Mapping Workbench project.

For example, if you define a descriptor with an after load class and method which is not included in the OracleAS TopLink Mapping Workbench project and you change the after load class outside of the OracleAS TopLink Mapping Workbench, then when you refresh the descriptor, the OracleAS TopLink Mapping Workbench does not pick up the change.

To workaround this issue, add all dependent classes to the OracleAS TopLink Mapping Workbench project. Because you do not map them, right-click each dependent class and deselect the **Activate Descriptor** option. Now when you refresh the project, the OracleAS TopLink Mapping Workbench refreshes both descriptors and dependent classes.

7.1.6.4 OracleAS TopLink Sessions Editor Preferences

Before changing any other general preferences (such as the text editor location), you must select a default **Look and Feel** in the **General Preferences** dialog and click **OK**. Then reopen the **General Preferences** dialog and make any additional changes.

7.1.6.5 Classpath with Spaces in Directory Names

On the Microsoft Windows platform, if your classpath contains directories with names that have spaces in them, then the OracleAS TopLink Mapping Workbench may fail to start and displays the error `Cannot Find Main Class`.

If this is the case, then consider removing spaces from directory names in the JDBC, Oracle home, and JRE classpaths.

7.1.6.6 Icon Size

Changing the icon size of the OracleAS TopLink Mapping Workbench toolbar may cause the application to fail at the next start-up. You must edit the `workbench.xml` file and change `small-icon=false` to `true`.

7.1.6.7 Generating Source Code

If you attempt to generate source code for a descriptor but cancel the process before the OracleAS TopLink Mapping Workbench writes the new source code, a dialog indicates that the source code was successfully updated. However, if you cancelled the process, the OracleAS TopLink Mapping Workbench did not overwrite any existing code.

In 10*g* (9.0.4.5), the OracleAS TopLink Mapping Workbench does not support generating Project Java Source for Descriptors mapped to inner classes.

If you attempt to generate source code from a table with BLOBs, the generated Java code may contain errors in the type definition and method parameters. You must edit the source code to eliminate the errors.

7.1.6.8 Improper Set Method for Array Type Attributes

OracleAS TopLink Mapping Workbench does not generate proper set method for array type attributes.

7.1.7 Using the OracleAS TopLink Web Client

The following issues exist with the OracleAS TopLink Web client:

7.1.8 OracleAS TopLink Examples

The following issues exist in the OracleAS TopLink Examples:

- Section 7.1.8.1, "IBM WebSphere BMP Examples"

7.1.8.1 IBM WebSphere BMP Examples

The duplicate entries of `ibm-application*.xmi` in `bmp.ear` cause a `Save Failure Exception` when deploying the BMP example on IBM WebSphere 5.0.2. To correct this, comment out the following element inside `build.ear` in the `build.xml` file:

```
<metainf dir="${config.dir}">
    <include name="ibm-application*.xmi"/>
</metainf>
```

7.1.8.2 Configuring Examples for RedHat

Running the `configureExamples.sh` on RedHat Enterprise Server 3.0 may cause a **missing class for multipleCopy** error. To correct this, modify the `build.xml` file to contain the absolute path to the `toplink_customtasks.jar`. For example:

```
<taskdef name="multipleCopy"
    classname="org.apache.tools.ant.taskdefs.MultipleCopy"
    classpath="<COMPLETE_ABSOLUTE_PATH>/customtasks.jar"/>
```

where *<COMPLETE_ABSOLUTE_PATH>* = `/home/iasuser/mwtesting/ant/lib/toplink_customtasks.jar`

7.1.9 Problem On Red Hat Enterprise Linux AS/ES 3.0 Systems

Before running the configureExamples.sh script on a Red Hat Enterprise Linux AS/ES 3.0 system, complete the following steps:

1. Open the `$ORACLE_HOME/toplink/examples/build.xml` file in a text editor.

2. Search for the following string:

```
<taskdef name="multipleCopy"
```

3. Edit the section as follows, where *oracle_home* is the absolute path to the Oracle Home directory:

```
<taskdef name="multipleCopy"
classname="org.apache.tools.ant.taskdefs.MultipleCopy"
classpath="oracle_home/ant/lib/toplink_customtasks.jar"/>
```

For example, if `/opt/oracle` is the Oracle Home, edit the section as follows:

```
<taskdef name="multipleCopy"
classname="org.apache.tools.ant.taskdefs.MultipleCopy"
classpath="/opt/oracle/ant/lib/toplink_customtasks.jar"/>
```

7.2 Documentation Errata

This section describes the known errors in the documentation. It includes the following topics:

7.2.1 Parameterized SQL

The *Oracle Application Server TopLink Application Developer's Guide* incorrectly states that you cannot use batch writing and parameterized SQL together.

7.2.2 Sequencing Examples

The sequencing code examples (Example A-2 and Example A-3) in the *Oracle Application Server TopLink Application Developer's Guide* are incorrect. Example 3-22 and Example 3-23 illustrate the correct code examples for using sequencing with stored procedures.

7.2.3 Configuring the OracleAS TopLink Web Client

In the "Configuring the Web Client" section of the *Oracle Application Server TopLink Application Developer's Guide*, the correct path to the `web.xml` file should be:

`<ORACLE_HOME>/toplink/config/toplinkwc`.

When using the Web Client with OC4J, replace the path indicated in the document:

`<ORACLE_HOME>/toplink/examples/oc4j/904/server/`

with your local <*J2EE_HOME*> directory.

To deploy to BEA WebLogic, you must also define a reference to this datasource in the `<ORACLE_HOME>/toplink/config/toplinkwc/weblogic.xml` file, as follows:

```
<reference-descriptor>
  <resource-description>
    <res-ref-name>jdbc/DataSourceName</res-ref-name>
    <jndi-name>jdbc/DataSourceName</jndi-name>
```

```
  </resource-description>
</reference-descriptor>
```

In the "Configuring the Application Server" section, the first step of the procedure (where you are instructed to copy the `toplinkwc.ear` file to an application server-specific directory) is not required. When you run the `assembleWebClient` script located in the `<ORACLE_HOME>/toplink/bin` directory, the system assembles and deploys the `toplinkwc.ear` file for you, as specified in the `build.properties` file.

7.2.4 OracleAS TopLink Mapping Workbench Tutorial

When completing the tutorials in the *Oracle Application Server TopLink Mapping Workbench User's Guide*, be aware of the following changes:

- To use sequencing, in addition to creating the sequence table from the OracleAS TopLink Mapping Workbench, you must also create the sequence table in the database.
- When creating the sequence table, use size 38 for both `SEQ_NAME` and `SEQ_COUNT`.
- When implementing inheritance for the `BaseProject` descriptor, ensure that the **Read Subclass On Query** option is selected.
- Figure B-49 incorrectly omits the `BaseProject` class indicator type. Although `BaseProject` is an abstract class and does not require an indicator value, it is listed on the Inheritance tab.
- In Example B-4, the line:

  ```
  president.addPhoneNumber(homeNumber);
  ```

  should be:

  ```
  president.addPhoneNumber(homePhone);
  ```

8

Oracle Application Server Web Cache

This chapter describes the issues associated with Oracle Application Server Web Cache (OracleAS Web Cache). It includes the following topics:

8.1 Known Issues

This section describes known issues for OracleAS Web Cache. It includes the following topic:

8.1.1 OracleAS Web Cache Manager Displays Error on SUSE Linux Enterprise Server 9

If you start OracleAS Web Cache using the OracleAS Web Cache Manager on SUSE Linux Enterprise Server 9, the following error is displayed:

```
Error communicating with remote admin server
```

However, OracleAS Web Cache starts successfully and the error can be safely ignored.

8.2 Configuration Issues and Workarounds

This section describes configuration issues and their workarounds for OracleAS Web Cache. It includes the following topics:

8.2.1 Reloading Issue with Cache Operations Success Message in Internet Explorer Browser

When you submit a successful operation in the Cache Operations page (**Cache Operations** in **Operations**) in OracleAS Web Cache Manager, a success dialog appears.

When you click **OK** to acknowledge the message, on versions of Internet Explorer running on Macintosh, the success dialog reloads the OracleAS Web Cache Manager interface into the dialog itself.

8.2.2 Failure When Submitting Global URL Parameters to Ignore in OracleAS Web Cache Manager

In some cases, when you submit parameters to ignore in the Global URL Parameters to Ignore dialog box of OracleAS Web Cache Manager, the submission is ignored and the Global URL Parameters to Ignore dialog box continues to display. You access the Global URL Parameters to Ignore dialog box when you select **Edit Global URL Parameters to Ignore** from the Site Definitions page of OracleAS Web Cache Manager (**Origin Servers**, Sites, and **Load Balancing** > **Site Definitions**).

To workaround this behavior, navigate to the Sites page of Oracle Enterprise Manager Application Server Control (**Web Cache Home** page > **Administration** tab > **Properties** > **Application** > **Sites**), and select the **Global URL Parameters** option in the Defaults and Global Settings section to configure parameters to exclude.

8.2.3 Invalidation Timeout Issue During Invalidation Propagation to a Cache Cluster Member

Invalidation has a default timeout of 300 seconds for the propagation of invalidation requests. If a node is not running and is configured as a cache cluster member in a cache cluster, then OracleAS Web Cache correctly recognizes the node failure. However, invalidation requests are still sent to the shutdown node as part of an invalidation propagation, resulting in a 300-second timeout for those requests. A message similar to the following is reported in response to the invalidation request:

```
Can't connect to the web cache's invalidation listening port.
```

To avoid the long timeout, remove the cache cluster member from the cluster.

> **See Also:** Section "Removing Caches from a Cluster" in Chapter 10, "Configuring Cache Clusters," in the *Oracle Application Server Web Cache Administrator's Guide*

8.2.4 Failure to Invalidate Content in Configurations with Uppercase Site Host Names

In Oracle Application Server 10*g* Release 2 (10.1.2), advanced invalidation requests fail for configurations that specify an uppercase or mixed case host name in the site definition for the site itself or any of its aliases. For example, you specify `WWW.COMPANY.COM` or `WWW.Company.COM` instead of `www.company.com` in the site definition.

To workaround this issue, change the host name value used in the sites and site aliases configuration to lowercase. For example, change `WWW.COMPANY.COM` to `www.company.com`. You specify the site configuration in the Sites page of Application Server Control (Navigate to the **Web Cache Home** page. In the **Administration** tab, Select **Properties**. Select Applications and then Sites) or the Site Definitions page of OracleAS Web Cache Manager (**Origin Servers, Sites, and Load Balancing** > **Site Definitions**).

8.3 Documentation Errata

This section describes the documentation errata.

8.3.1 Incorrect Note in *Oracle Application Server Web Cache Administrator's Guide*

Section "Listing Popular Requests and Cache Contents" in Chapter 15, "Using Diagnostics Tools," in the *Oracle Application Server Web Cache Administrator's Guide* contains the following note:

> **Note:** OracleAS Web Cache Manager lists only those objects that are valid. Although the cache may contain objects that are expired or that have been invalidated, those objects are not included in these lists.

Disregard this note. The output for popular requests also includes cached but expired objects.

9

Oracle Enterprise Manager

This chapter describes issues with Oracle Enterprise Manager. It includes the following topics:

9.1 General Issues and Workarounds

This section describes general issues and their workarounds for Oracle Enterprise Manager Application Server Control. It includes the following topics:

9.1.1 Setting Globalization Support and Operating System Locale Environment Variables

If you launch a command line tool such as `emctl` in a non-English setup environment to start a process, then ensure the operating system locale and the `NLS_LANG`

environment variable settings are configured properly and consistently. This is applicable to the `emctl` command line utility that is available with Oracle Application Server installations as well as with the `emctl` utility available with Central Console installations.

If these environment variables are not set prior to Oracle Application Server or Central Console installations, then non-ASCII characters will appear incorrectly in Application Server Control or Central Console, respectively. To prevent this problem from occurring, set these two environment variables prior to installation. If you cannot set the environment variables prior to installation, then set the two environment variables after installation, and restart the Management Agent.

Refer to the following sections for details on how to check and set the values for the environment variables:

- Section 9.1.1.1, "Checking the Operating System Locale"
- Section 9.1.1.2, "Setting the Operating System Locale"
- Section 9.1.1.3, "Checking the NLS_LANG Environment Variable"
- Section 9.1.1.4, "Setting the NLS_LANG Environment Variable"

9.1.1.1 Checking the Operating System Locale

Ensure that the `LC_ALL` or `LANG` environment variables are set with the appropriate value. To check the current setting, issue the following command:

```
$PROMPT> locale
```

9.1.1.2 Setting the Operating System Locale

If you are using `bash` or `zsh`, then to set the locale environment variable of the operating system, issue the `export` command. For example:

```
export LANG=zh_CN
```

In this example, the variable is being set to `Simplified Chinese`. For the specific value in each operating system, refer to the documentation specific to the operating system.

If you are using `csh` or `tcsh`, then issue the `setenv` command:

```
setenv LANG zh_CN
```

9.1.1.3 Checking the NLS_LANG Environment Variable

Ensure that the `NLS_LANG` environment variable is set to an appropriate and compatible value with the operating system locale setting. In addition, ensure that the Grid Control Management Repository database character is set if Grid Control is being used to centrally manage the Oracle Application Server. For the specific value of the language or the character set, refer to the *Globalization Support Guide* of the Oracle product you are using.

If the platform is a Windows-based operating system, then the default `NLS_LANG` setting in the registry should be used as is. In addition, check to see if the `NLS_LANG` setting exists in `$ORACLE_HOME/opmn/conf/opmn.xml` on UNIX or *`ORACLE_HOME`*`\opmn\conf\opmn.xml` on Windows. For example, the following content should appear in the `opmn.xml` file:

```
<environment>
     <variable id="TMP" value="/tmp"/>
     <variable id="NLS_LANG" value="JAPANESE_JAPAN.JA16SJIS"/>
```

```
</environment>
```

If the NLS_LANG setting exists, then ensure that the NLS_LANG setting in the opmn.xml file is identical to the NLS_LANG environment variable.

9.1.1.4 Setting the NLS_LANG Environment Variable

If you are using bash or zsh, then to set the NLS_LANG environment variable, issue the export command. For example:

```
export NLS_LANG="Simplified Chinese_China.ZHS16GBK"
```

In this example, the variable is set to Simplified Chinese. For the specific value in each operating system, refer to documentation specific to the operating system.

If you are using csh or tcsh, then issue the setenv command. For example:

```
setenv NLS_LANG "Simplified Chinese_China.ZHS16GBK"
```

9.1.2 Timestamp on Log Files May Not Be Accurate

The log file timestamps shown by the operating system which are displayed in Log Viewer of the Application Server Control are not always correct. The log file may contain recent log messages but the timestamp available from operating system is normally older than the last message written to the file.

9.1.3 Errors When Configuring Components or Adding or Removing OC4J Instances

While installing Oracle Management Agent 10.1.0.2 on a computer which has one or more instances of Oracle Application Server 10*g* (10.1.2), you may encounter errors in Application Server Control if you modify your component configuration. For example, you may receive errors if you create or remove an OC4J instance or if you configure an Oracle Application Server component after you have installed the application server.

To work around this problem, install Oracle Management Agent 10.1.0.3 or later patchsets.

9.1.4 Problems with the Progress Page When Using a Macintosh Browser

When you perform an operation with Application Server Control, such as creating a OC4J instance, Enterprise Manager displays a progress page that indicates that the operation is still in progress.

When using the Apple Safari browser on a Macintosh computer, the progress page continues to display even after the operation is complete. As a result, the operation confirmation page is not displayed.

To solve this problem, set the EM_OC4J_OPTS environment variable to the following value and restart the Application Server Control:

```
-Doracle.sysman.emSDK.eml.util.iAS.waitForCompletion=true
```

> **See Also:** Appendix "Managing and Configuring Application Server Control" of the *Oracle Application Server 10g Administrator's Guide* for more information about using the EM_OC4J_OPTS environment variable

9.1.5 Error when Clicking Topology Link from Host Page

In the Host page of Application Server Control, when clicking the **Topology** link, the following error appears:

```
Could not determine the oracle home for this component
```

To workaround this error, navigate to the Farm page, and click the **Topology** link from that page.

9.1.6 Error when using the ADF BUSINESS COMPONENT Link on the Host Page

In the Host page of Application Server Control, when clicking the **ADF BUSINESS COMPONENTS** target in the Targets section, the following error appears:

```
Error: Failed to connect to OC4J null instance now, please click refresh page to
try again!
```

To avoid this error, navigate to the OC4J Administration page, and click the **ADF Business Components** link in the Related Links section.

9.1.7 Posting Data From the Logging Pages

After you configure security for Application Server Control, you may see intermittent issues with form data updates in the Logging pages. These issues may occur with Microsoft Internet Explorer browsers after you install the 832894 (MS04-004) security update or the 821814 hotfix. Microsoft Internet Explorer has known issues regarding using a form on a HTTPS Web page. Problem related to these updates have been seen in the Advanced Search feature of the Search Log Repository page.

To work around this problem, download the Microsoft `Q831167.exe` package and any other recommended related patch recommend by Microsoft.

See Also:

(http://support.microsoft.com/default.aspx?kbid=831167)

9.1.8 Additional Step when Removing an Application Server Target from the Central Console

If an Oracle Application Server 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) target is removed from the Central Console, the Infrastructure page in the Application Server Control will still show Central Management as **Configured**.

To reset the Central Management section of the page, delete the following file from `centralagents.lst` in the application server Oracle home:

- In UNIX, `$ORACLE_HOME/sysman/emd/centralagents.lst`
- In Windows *ORACLE_HOME*`\sysman\emd\centralagents.lst` (Windows)

9.1.9 Grid Control Agent 10.1.0.3

Oracle does not support Grid Control Agent (10.1.0.3) running on HP-UX Itanium or Linux Itanium monitoring an Application Server 10*g* Release 2 (10.1.2).

9.1.10 Security Considerations When Changing Schema Passwords with the Application Server Control

You can use the Application Server Control Console to change the password for a component schema in the OracleAS Metadata Repository.

However, when you perform this task in the Application Server Control Console, the new password you enter will be saved in clear text format in the following log file:

ORACLE_HOME/sysman/log/em-web-access.log

In addition, if the Application Server Control has not been secured, the new schema password will be transmitted unencrypted from the client-side browser to the machine where the Console is running.

> **See Also:** "Configuring Security for the Application Server Control Console" in the chapter " Enabling SSL in the Infrastructure" in the *Oracle Application Server 10g Administrator's Guide* for more information about the benefits of configuring security for the Application Server Control

To avoid these potential security issues, perform the following procedure before changing a schema password in the Application Server Control Console:

1. Stop the Application Server Control.

   You can stop the Application Server Control by entering the following command in the Application Server Control Oracle home:

   ORACLE_HOME/bin/emctl stop iasconsole

   > **See Also:** The "Starting and Stopping" chapter of the *Oracle Application Server 10g Administrator's Guide*

2. Secure the Application Server Control by entering the following command:

   ORACLE_HOME/bin/emctl secure iasconsole

   > **See Also:** "Configuring Security for Enterprise Manager Application Server Control Console" in Appendix A of the *Oracle Application Server 10g Administrator's Guide*

3. Use a text editor to open the following configuration file in the application server Oracle home:

   ORACLE_HOME/sysman/j2ee/config/emd-web-site.xml

4. Locate the following entry in the `emd-web-site.xml` file:

   ```
   <!-- Access Log, where requests are logged to -->
   <access-log path="../../log/em-web-access.log" />
   ```

5. Modify the `access-log path` entry so it describes the format of each log entry, as follows:

   ```
   <!-- Access Log, where requests are logged to -->
   <access-log path="../../log/em-web-access.log"
      format="$ip - [$time] '$path' $status $size"/>
   ```

6. Save and close the `emd-web-site.xml` file.
7. Start the Application Server Control.

   You can start the Application Server Control by entering the following command in the Application Server Control Oracle home:

   ```
   ORACLE_HOME/bin/emctl start iasconsole
   ```

   See Also: The "Starting and Stopping" chapter of the *Oracle Application Server 10g Administrator's Guide*

9.1.11 Problems Viewing OracleAS Portal Metrics When OracleAS Portal is Configured for Secure Sockets Layer (SSL)

When you use Application Server Control to monitor an instance of OracleAS Portal that has been configured to use Secure Sockets Layer (SSL), some performance metrics for OracleAS Portal may not display.

To correct this problem you must allow the Application Server Control to recognize the Certificate Authority that was used by the Web Site to support HTTPS. You must add the Certificate of that Certificate Authority to the list of Certificate Authorities recognized by the Application Server Control.

To configure Application Server Control to recognize the Certificate Authority:

1. Obtain the Certificate of the Web Site's Certificate Authority, as follows:
   a. In Microsoft Internet Explorer, connect to the HTTPS URL of the application server you are attempting to monitor.
   b. Double-click the lock icon at the bottom of the browser screen, which indicates that you have connected to a secure Web site.

      The browser displays the Certificate dialog box, which describes the Certificate used for this Web site. Other browsers offer a similar mechanism to view the Certificate detail of a Web Site.
   c. Click the **Certificate Path** tab and select the first entry in the list of certificates.
   d. Click **View Certificate** to display a second Certificate dialog box.
   e. Click the **Details** tab on the Certificate window.
   f. Click **Copy to File** to display the Certificate Manager Export wizard.
   g. In the Certificate Manager Export wizard, select **Base64 encoded X.509 (.CER)** as the format you want to export and save the certificate to a text file with an easily-identifiable name, such as `portal_certificate.cer`.
   h. Open the certificate file using your favorite text editor.

      The content of the certificate file will look similar to the content shown in Example 15–1.
2. Update the list of Certificate Authorities, as follows:
   a. Locate the `b64InternetCertificate.txt` file in the following directory of the Oracle Application Server Oracle home:

      ```
      ORACLE_HOME/sysman/config/
      ```

      This file contains a list of Base64 Certificates.

b. Edit the `b64InternetCertificate.txt` file and add the contents of the Certificate file you just exported to the end of the file, taking care to include all the Base64 text of the Certificate including the BEGIN and END lines.

3. Copy the text file that contains the certificate (for example, the file you named `portal_certificate.cer` earlier in this procedure) to the OracleAS Portal middle tier.

4. Use the `orapki` utility to update the `monwallet` Oracle wallet by using the following command:

```
ORACLE_HOME/bin/orapki wallet add
    -wallet ORACLE_HOME/sysman/config/monwallet
    -trusted_cert
    -cert certificate_location
```

When you are prompted for a password, enter the password for the `monwallet` wallet. The default password is "welcome".

In the example, replace *certificate_location* with the full path to the text file that contains the certificate you saved earlier in this procedure and that you copied to the OracleAS Portal middle tier. For example:

```
/dua0/oracle/portal_certificate.cer
```

5. Restart the Application Server Control.

After you restart the Application Server Control, Enterprise Manager detects your addition to the list of Certificate Authorities and you can successfully monitor the OracleAS Portal metrics using the secure Application Server Control Console.

Example 9–1 Example Content of an Exported Certificate

```
-----BEGIN CERTIFICATE-----
MIIDBzCCAnCgAwIBAgIQTs4NcImNY3JAs5edi/5RkTANBgk
... base64 certificate content ...
------END CERTIFICATE------
```

9.1.12 Database Management in OracleAS Cold Failover Cluster (Infrastructure) Configurations

In both non-distributed and distributed OracleAS Cold Failover Cluster (Infrastructure) configurations, you can run the Database Console only from the node where you installed the OracleAS Metadata Repository. For example, if your hardware cluster consists of node A and node B, and you performed the installation from node A, then you can only run the Database Console from node A. The reason for this is that the Database Console uses the physical hostname instead of the virtual hostname.

If node A fails, you will not be able to run Database Console from node B. To manage the OracleAS Metadata Repository database from node B, you have to use other tools, such as SQL*Plus.

9.2 Documentation Errata

This section describes documentation errata. It includes the following topics:

9.2.1 Online Help for the Application Server Control All Metrics Page

Most of the component home pages within Application Server Control include an **All Metrics** link. When you click this link, Enterprise Manager displays the All Metrics page, which provides a comprehensive list of all the performance metrics you can monitor for the selected component.

In some cases, you can click a metric name on the All Metrics page to display the Metric Details page, and then click **Help** to get more information about the selected metric.

However, for some metrics, clicking **Help** will display a `Topic not found` error. This problem will be addressed in a future version of Oracle Application Server.

In the rest of the cases, the online help provided for a particular metric might refer to features available only when you are centrally managing your application server instance with Central Console. For example, the online help might refer to thresholds, alerts, or the display of historical data about a metric. In those cases, you can access these additional monitoring features by installing and configuring Central Console.

See Also:

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

9.2.2 Error in Online Help Topic About Regular Expressions

In the Application Server Control online help topic "About Regular Expressions," the example for the asterisk (*) character shows:

```
OC4J*.
```

The example should instead show the following:

```
OC4J.*
```

Index