Oracle® Application Server

Upgrade and Compatibility Guide

10*g* (10.1.4.0.1) for UNIX

B28188-01

July 2006

Oracle Application Server Upgrade and Compatibility Guide, 10*g* (10.1.4.0.1) for UNIX

B28188-01

Primary Author: Peter LaQuerre

Contributors: Jaya Chaudhary, Saheli Dey, Paul Dickson, Stuart Duggan, Pramodini Gattu, Tim Harkness, Pavana Jain, Mathias Kullberg, Kishore Kumar, Stephen Mann Lee, Bill Norcott, Jayachanthar Ponnusamy, Lalithashree Rajesh, Pardha Reddy, Mike Rubino, Amit Sharma, Satishkumar Venkatasamy

Contents

4 Backup Strategies and System Availability During an Upgrade

Part II Performing the Upgrade

5 Upgrading 10*g* (9.0.4) Middle Tiers to 10*g* Release 2 (10.1.2)

6 Upgrading the Database That Hosts the OracleAS Metadata Repository

7 Using Oracle Universal Installer to Upgrade Oracle Identity Management

8 Using MRUA to Upgrade the OracleAS Metadata Repository

9 Component-Specific Post-Upgrade Procedures

10 Verifying the Upgrade and Decommissioning the Source Oracle Homes

Part III Appendices for Specialized Environments and Troubleshooting

A Performing an Oracle Identity Management Multimaster and Fan-Out Replication Upgrade

B Upgrading High Availability Configurations

C Using the Data Migration Method of Upgrading OracleAS Identity Management

D Reviewing the Upgrade Log Files

E OracleAS Metadata Repository Upgrade Error Messages

Preface

This preface contains the following information about this guide:

- Audience
- What’s New for Oracle Application Server 10g (10.1.4.0.1)
- Documentation Accessibility
- Related Documents
- Conventions

Audience

This document is intended for Oracle Application Server administrators who want to upgrade their Oracle Application Server environment to Oracle Application Server 10*g* (10.1.4.0.1).

What’s New for Oracle Application Server 10*g* (10.1.4.0.1)

For a list of the new features available for Oracle Application Server 10*g* (10.1.4.0.1), refer to "What's New in Oracle Application Server Administration?" in the *Oracle Application Server Administrator’s Guide*.

For more information about the new features available for Oracle Internet Directory and the other Oracle Identity Management components, refer to *Oracle Identity Management Infrastructure Administrator’s Guide*.

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, see these Oracle resources:

- Oracle Application Server Documentation Library
- Oracle Application Server Platform-Specific Documentation

To download free release notes, documentation, white papers, and other collateral, please visit the Oracle Technology Network (OTN):

`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.

Part I

Before You Begin

This part contains the following chapters:

1 Overview of the Upgrade Process

Use this chapter to get a high-level overview of the upgrade steps. This chapter contains the following sections:

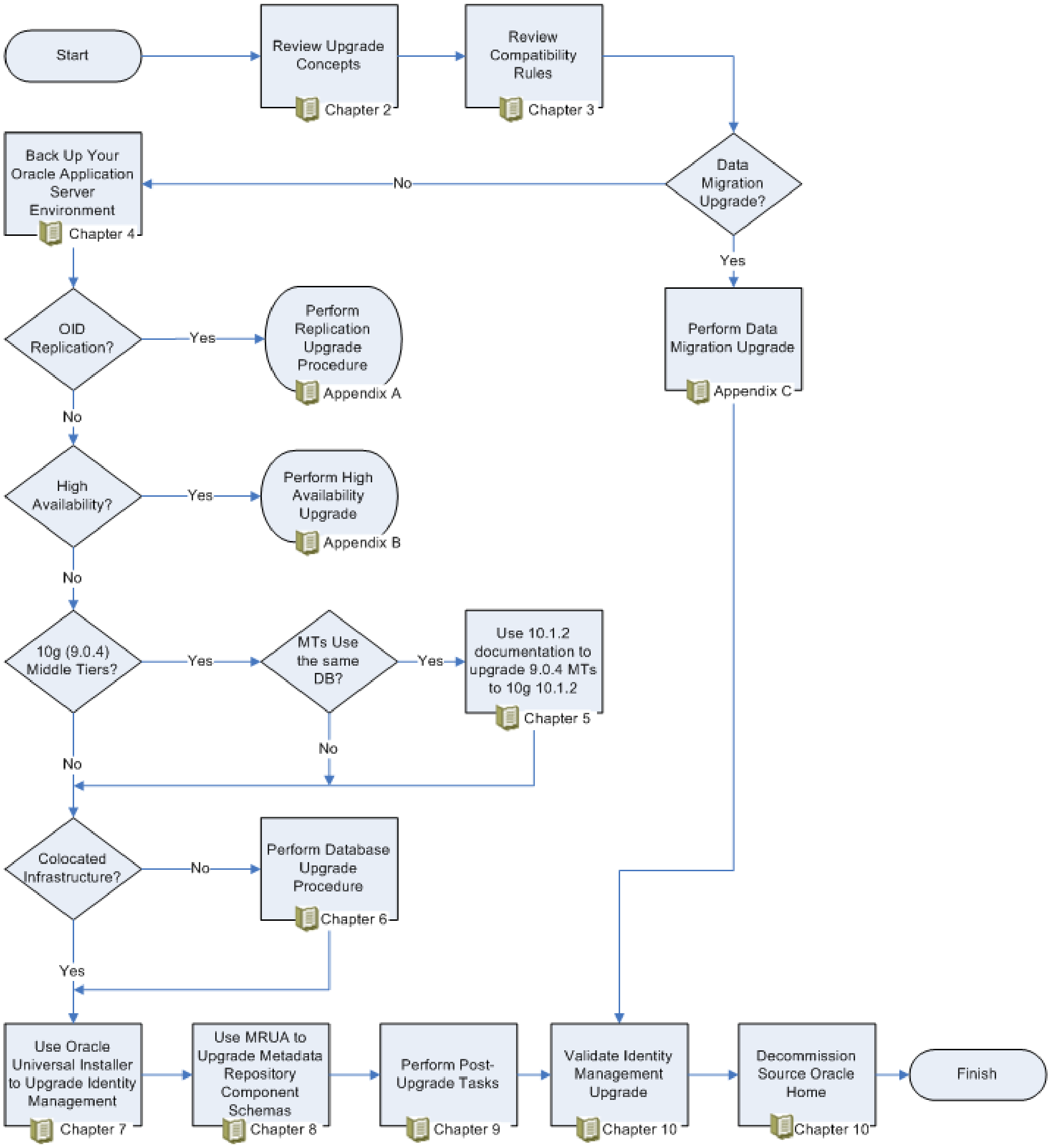
- Flow Chart of the Oracle Application Server Upgrade Process
- Table Describing the Steps in the Upgrade Process Flow Chart

1.1 Flow Chart of the Oracle Application Server Upgrade Process

Figure 1–1 provides a high-level flow chart showing all the steps required in order to upgrade your Oracle Application Server environment to Oracle Identity Management 10*g* (10.1.4.0.1).

Where applicable, the flow chart provides references to the chapter in the book where you can find the instructions to perform each step.

Figure 1–1 Overall Process Flow for Oracle Identity Management 10g (10.1.4.0.1) Upgrade


Start
Review Upgrade Concepts
Chapter 2
Review Compatibility Rules
Chapter 3
Data Migration Upgrade?
No
Yes
Back Up Your Oracle Application Server Environment
Chapter 4
Perform Data Migration Upgrade
Appendix C
OID Replication?
Yes
Perform Replication Upgrade Procedure
Appendix A
No
High Availability?
Yes
Perform High Availability Upgrade
Appendix B
No
10g (9.0.4) Middle Tiers?
Yes
MTs Use the same DB?
Yes
Use 10.1.2 documentation to upgrade 9.0.4 MTs to 10g 10.1.2
Chapter 5
No
No
Colocated Infrastructure?
No
Perform Database Upgrade Procedure
Chapter 6
Yes
Use Oracle Universal Installer to Upgrade Identity Management
Chapter 7
Use MRUA to Upgrade Metadata Repository Component Schemas
Chapter 8
Perform Post-Upgrade Tasks
Chapter 9
Validate Identity Management Upgrade
Chapter 10
Decommission Source Oracle Home
Chapter 10
Finish

1.2 Table Describing the Steps in the Upgrade Process Flow Chart

Refer to Table 1–1 for an explanation of the steps within the flow chart.

Table 1–1 Description of the Steps in the Upgrade Process Flow Chart

Step	Description	More Information
Review Upgrade Concepts	Before you begin, make sure you are familiar with the basic concepts of the Oracle Application Server upgrade, including typical upgrade scenarios and the basic rules of upgrade.	Chapter 2, "Oracle Application Server Upgrade Concepts"
Review Compatibility Rules	Make sure your upgraded 10*g* (10.1.4.0.1) components will be able to work with any other Oracle Application Server components that already exist in your environment.	Chapter 3, "Understanding Version Compatibility"
Data Migration Upgrade?	The Data Migration method of upgrading Oracle Identity Management is an alternative approach to upgrading the Oracle Identity Management data stored in the OracleAS Infrastructure database. Instead of using Oracle Universal Installer to upgrade to 10*g* (10.1.4.0.1), you use command-line utilities to export your existing Oracle Identity Management data and then restore it into a newly installed 10*g* (10.1.4.0.1) OracleAS Infrastructure database. Use this step in the flow chart to review Appendix C and consider the data migration method of upgrade and whether or not it is the best upgrade method for your environment.	Appendix C, "Using the Data Migration Method of Upgrading OracleAS Identity Management"
Back Up Your Oracle Application Server Environment	Review the recommended backup strategies for your Oracle Application Server environment, as well as the system availability expectations during the upgrade.	Chapter 4, "Backup Strategies and System Availability During an Upgrade"
OID Replication?	If you are running Oracle Internet Directory in a replicated environment, review the special instructions for upgrading the OracleAS Identity Management components in such an environment.	Appendix A, "Performing an Oracle Identity Management Multimaster and Fan-Out Replication Upgrade"
High Availability?	If you are upgrading a 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) high availability environment, review the special instructions for upgrading those supported environments.	Appendix B, "Upgrading High Availability Configurations"
10*g* (9.0.4) Middle Tiers?	If you have installed any 10*g* (9.0.4) middle tiers in your Oracle Application Server environment, you might have to upgrade those middle tiers to 10*g* Release 2 (10.1.2) before you proceed.	Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)"
MTs Use Same DB?	If your 10*g* (9.0.4) middle tiers use the same OracleAS Metadata Repository as your OracleAS Identity Management components, then you must upgrade those middle tiers to 10*g* Release 2 (10.1.2). On the other hand, if the 10*g* (9.0.4) middle tiers use a OracleAS Metadata Repository that is stored in a separate database, then you can skip to the next step in the Upgrade process.	Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)"

Table 1–1 (Cont.) Description of the Steps in the Upgrade Process Flow Chart

Step	Description	More Information
Colocated Infrastructure?	If the OracleAS Identity Management installation you are upgrading is not part of a colocated Infrastructure, you must first upgrade the database that hosts the OracleAS Metadata Repository. Otherwise, if OracleAS Identity Management is part of a colocated Infrastructure, you can skip this step.	Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository"
Use Oracle Universal Installer to Upgrade Identity Management	To upgrade OracleAS Identity Management to 10*g* (10.1.4.0.1), you use Oracle Universal Installer. During the installation, Oracle Universal Installer locates any existing installations on your system. You can then select the option to upgrade the existing OracleAS Identity Management installations to 10*g* (10.1.4.0.1).	Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management"
Use MRUA to Upgrade Metadata Repository Component Schemas	After you upgrade OracleAS Identity Management, you can then upgrade the rest of the component schemas in the OracleAS Metadata Repository. This step ensures that the schemas are upgraded to the same version you would have if you had installed a new 10*g* (10.1.4.0.1) OracleAS Identity Management Oracle home.	Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository"
Perform Post-Upgrade Tasks	Depending upon the OracleAS Identity Management components and features you are using, you might have to perform a set of post-upgrade procedures.	Chapter 9, "Component-Specific Post-Upgrade Procedures"
Validate Identity Management Upgrade	After the OracleAS Identity Management upgrade, you should verify that the upgrade was successful and that your OracleAS Identity Management components are working properly.	Section 10.1, "Task 1: Verify the Oracle Identity Management Upgrade"
Decommission Source Oracle Home	After you confirm that the upgrade was successful, you can consider decommissioning and removing the previous installations. However, be sure to carefully review the decommisioning documentation before you remove the source Oracle home.	Section 10.2, "Task 2: Decommission the OracleAS Identity Management Source Oracle Home"

2

Oracle Application Server Upgrade Concepts

This chapter describes basic concepts you should understand before you upgrade your OracleAS Identity Management services to Oracle Application Server 10*g* (10.1.4.0.1).

This chapter contains the following sections:

- Reviewing Your Current Oracle Application Server Installations
- Introduction to the Upgrade Tools
- Upgrade Rules to Follow
- Supported Upgrade Paths for Oracle Application Server 10g (10.1.4.0.1)
- Verifying Support for Third-Party Products

2.1 Reviewing Your Current Oracle Application Server Installations

The following sections provide some guidelines for analyzing your current Oracle Application Server configurations so you can select the best possible upgrade process:

- Identifying the Existing Oracle Homes to Upgrade
- About Upgrading Oracle Access Manager
- Reviewing Your Current OracleAS Infrastructure Configuration
- Determining Whether Your Database is a Seed Database or OracleAS RepCA Database
- Using Application Server Control to Review Your Oracle Application Server Environment

2.1.1 Identifying the Existing Oracle Homes to Upgrade

Your existing Oracle Application Server installations consist of:

- Oracle Application Server middle-tier installations
- Oracle Application Server Metadata Repository installations
- Oracle Application Server Identity Management installations

You deploy and run your applications on Oracle Application Server middle tiers. The OracleAS Metadata Repository and OracleAS Identity Management installations provide the infrastructure services that are used by the middle tiers. Infrastructure services can be shared by multiple middle tiers.

In many cases, your Oracle Application Server environment consists of multiple middle-tier installations, one OracleAS Metadata Repository installation, and one

OracleAS Identity Management installation. The middle-tier, OracleAS Metadata Repository, and OracleAS Identity Management installations exist in multiple Oracle homes and across multiple hosts.

As a result, when you upgrade to a new version of Oracle Application Server, you must upgrade multiple Oracle homes, including the middle-tier Oracle homes, as well as any Infrastructure Oracle homes you have installed. In addition, the upgrade of these Oracle homes must be performed in a particular order.

2.1.2 About Upgrading Oracle Access Manager

If your system environment includes Oracle Access Manager (previously known as Oblix NetPoint or Oracle COREid), you can upgrade to Oracle Access Manager 10*g* (10.1.4.0.1) by following the instructions in the *Oracle Access Manager Upgrade Guide*.

The *Oracle Access Manager Upgrade Guide*, along with the other Oracle Access Manager books, is part of the Oracle Application Server 10*g* (10.1.4.0.1) documentation library.

The upgrade procedures for Oracle Access Manager are documented separately from the Oracle Application Server upgrade procedures because the two products are installed separately.

For more information about Oracle Access Manager, refer to *Oracle Access Manager Introduction*.

For an example of how you can integrate Oracle Access Manager into your Oracle Application Server environment, refer to the *Oracle Application Server Enterprise Deployment Guide*.

2.1.3 Reviewing Your Current OracleAS Infrastructure Configuration

Most importantly, the process you use to upgrade your Oracle Application Server installations varies depending on how you installed and configured your OracleAS Infrastructure services. Specifically, the OracleAS Metadata Repository and OracleAS Identity Management can be in a single Oracle home or in separate Oracle homes.

For the purposes of upgrade, the following list describes the typical OracleAS Infrastructure configurations:

- Figure 2–1 illustrates a configuration where the OracleAS Metadata Repository and OracleAS Identity Management are in the same Oracle home.

  This configuration is the result of selecting the **Identity Management and OracleAS Metadata Repository** installation type during the Oracle Application Server installation procedure. This configuration is one of three OracleAS Infrastructure installation types available in Oracle Application Server 10*g* (9.0.4) and 10*g* Release 2 (10.1.2).

  This configuration is referred to as a **colocated Infrastructure** because both the OracleAS Metadata Repository and OracleAS Identity Management are located in the same Oracle home.

- Figure 2–2 illustrates a configuration where the OracleAS Metadata Repository and OracleAS Identity Management are installed in separate Oracle homes.

  This configuration is the direct result of installing the OracleAS Metadata Repository installation type in one Oracle home and OracleAS Identity Management in a different Oracle home.

This configuration is referred to as a **non-colocated Infrastructure** because the OracleAS Metadata Repository and the OracleAS Identity Management are not in the same Oracle home.

Figure 2–1 Colocated Infrastructure - OracleAS Metadata Repository and OracleAS Identity Management in the Same Oracle Home -

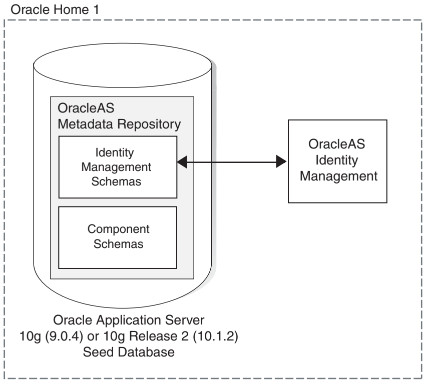
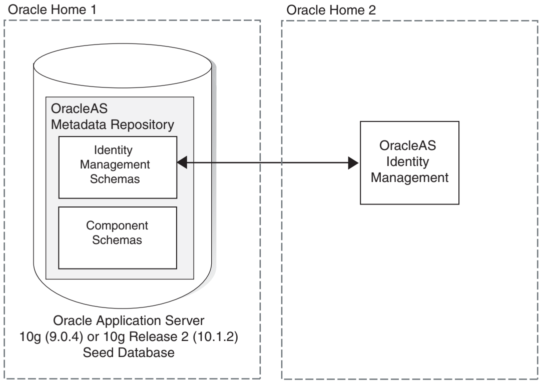


Figure 2–2 Non-Colocated Infrastructure - OracleAS Metadata Repository and OracleAS Identity Management in Separate Oracle Homes



2.1.4 Determining Whether Your Database is a Seed Database or OracleAS RepCA Database

As you begin the upgrade process, it is important to know how your OracleAS Metadata Repository was installed into your database. Specifically, consider the following to determine the type of OracleAS Metadata Repository database you will be upgrading. Each type of OracleAS Metadata Repository database is upgraded differently:

- If you used the Oracle Application Server installation procedure to create a new database for the OracleAS Metadata Repository, you can use Oracle Universal Installer to install Oracle Application Server 10*g* (10.1.4.0.1) and upgrade the database automatically.

  This type of OracleAS Metadata Repository database is referred to as a **seed database**, because the database was created automatically by the Oracle Application Server installation procedure specifically for hosting the OracleAS Metadata Repository.

- If you used OracleAS RepCA to install the OracleAS Metadata Repository in an existing database, you must upgrade the database yourself.

This type of OracleAS Metadata Repository database is referred to as an **OracleAS RepCA database,** because you used OracleAS RepCA to install the repository in an existing database that you installed and configured yourself.

> **See Also:** Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository"

2.1.5 Using Application Server Control to Review Your Oracle Application Server Environment

To learn more about your Oracle Application Server environment, you can use the Oracle Enterprise Manager 10*g* Application Server Control:

1. Open your Web browser and enter the Oracle Application Server URL for one of your Oracle Application Server instances.

   For example:

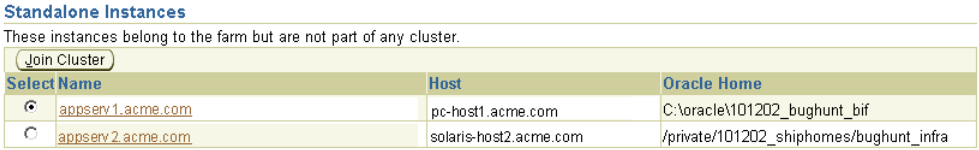
   ```
   http://host1.acme.com:1156/
   ```

   If you don't know the Application Server Control URL, you can find it in the following file in the Oracle Application Server Oracle home:

   ```
   ORACLE_HOME/install/readme.txt
   ```

2. If the Oracle Application Server instance is an OracleAS Infrastructure installation or a middle tier that is using an OracleAS Metadata Repository, the first page you see in the Application Server Control Console is the Farm page.
3. Review the contents of the Farm page, which includes a list of the Oracle Application Server instances that are part of the Farm (Figure 2–3).

Figure 2–3 Viewing the Instances in an OracleAS Farm



Standalone Instances

These instances belong to the farm but are not part of any cluster.

Select	Name	Host	Oracle Home
●	appserv1.acme.com	pc-host1.acme.com	C:\oracle\101202_bughunt_bif
○	appserv2.acme.com	solaris-host2.acme.com	/private/101202_shiphomes/bughunt_infra

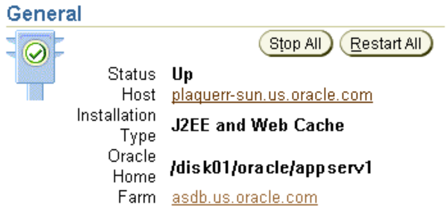
4. Click the name of one of the Oracle Application Server instances to view the Oracle Application Server Home page for the instance.
5. Review the General section of the Oracle Application Server Home page for information.

   In particular, note the following general characteristics of the instance:

   - The name of the Oracle Application Server host
   - The Oracle Application Server version
   - The installation type selected when the instance was installed
   - The directory where the Oracle home resides
   - The name of the farm, which is corresponds to the name of the database that is hosting the OracleAS Metadata Repository

   Figure 2–4 shows an example of the General section of the Oracle Application Server 10*g* Release 2 (10.1.2.0.2) Application Server Home page.

Figure 2–4 Using the General Section of the Application Server Home Page to Gather Information About the Oracle Application Server Environment



Status Up
Host plaquerr-sun.us.oracle.com
Installation Type J2EE and Web Cache
Oracle Home /disk01/oracle/appserv1
Farm asdb.us.oracle.com

2.2 Introduction to the Upgrade Tools

Oracle Application Server 10*g* (10.1.4.0.1) provides several tools to help you upgrade your Oracle Application Server installations to the latest version. Each tool has a specialized role in upgrading a component or in accomplishing a key step in the upgrade process.

Table 2–1 introduces the Upgrade tools you will use to upgrade your Oracle Application Server installations.

Table 2–1 Summary of the Oracle Application Server Upgrade Tools

Upgrade Tool	Description
Oracle Universal Installer	Oracle Universal Installer is the application you use to install Oracle Application Server, as well as most other Oracle software products. When you install an Oracle Identity Management 10*g* (10.1.4.0.1) Infrastructure component, the installation procedure checks to see if you have installed a previous version of the OracleAS Infrastructure. If a previous version is found, Oracle Universal Installer prompts you to upgrade the OracleAS Infrastructure installation
Metadata Repository Upgrade Assistant (MRUA)	MRUA is the tool you use to upgrade the Oracle Application Server component schemas in the OracleAS Metadata Repository, except the OracleAS Identity Management schemas. MRUA is distributed on the separate OracleAS Metadata Repository Upgrade Assistant and Utilities CD–ROM, which is part of the Oracle Application Server 10*g* (10.1.4.0.1) CD Pack. You run MRUA directly from the OracleAS Metadata Repository Upgrade Assistant and Utilities CD–ROM.
Oracle Application Server Backup and Recovery Tool or other backup utilities	For middle tiers and seed databases, you can use the Oracle Application Server Backup and Recovery Tool to perform backups. The Backup and Recovery Tool is described in the *Oracle Application Server Administrator's Guide*. For OracleAS RepCA databases, see the Oracle Database documentation for the platform and version of the database that hosts your OracleAS Metadata Repository. For example, if you are using a Oracle9*i* (9.0.1.3) database, see *Oracle9i Backup and Recovery Concepts* in the Oracle9*i* Documentation Library, which is available on the Oracle Technology Network (OTN): `http://www.oracle.com/technology/documentation/`

Table 2–1 (Cont.) Summary of the Oracle Application Server Upgrade Tools

Upgrade Tool	Description
Oracle Application Server Upgrade Assistant	You use the OracleAS Upgrade Assistant to upgrade your middle tier Oracle homes to the latest version of Oracle Application Server. This upgrade tool is not distributed with Oracle Identity Management 10*g* (10.1.4.0.1) because 10*g* (10.1.4.0.1) upgrades only your Oracle Application Server Infrastructure components and not your middle tiers. However, as part of the 10*g* (10.1.4.0.1) upgrade procedure, you might have to use the 10*g* Release 2 (10.1.2) OracleAS Upgrade Assistant. For more information, see Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)".

2.3 Upgrade Rules to Follow

The following sections describe the basic rules you must follow as you determine a plan for upgrading each of your Oracle Application Server components:

- Middle Tiers Must Be Upgraded Before OracleAS Metadata Repository
- Upgrade Cannot Be Performed Across Hosts or Platforms

2.3.1 Middle Tiers Must Be Upgraded Before OracleAS Metadata Repository

You must upgrade your application server instances in the proper order.

Specifically, you must upgrade your middle tiers before you can upgrade the OracleAS Metadata Repository. This is because your OracleAS Metadata Repository cannot be a higher version then your middle tier installations.

This rule applies to the 10*g* (10.1.4.0.1) only if you are running any 10*g* (9.0.4) middle tiers and those middle tiers are using the same OracleAS Metadata Repository as Oracle Identity Management. In that specific case, you must upgrade the middle tiers before using the Metadata Repository Upgrade Assistant (MRUA) to upgrade the OracleAS Metadata Repository. This is because MRUA upgrades the component schemas in the OracleAS Metadata Repository to 10*g* Release 2 (10.1.2).

> **See Also:** Appendix 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)"

2.3.2 Upgrade Cannot Be Performed Across Hosts or Platforms

The 10*g* (10.1.4.0.1) upgrade procedure is designed to upgrade OracleAS Identity Management 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) Oracle home to a new Oracle Identity Management 10*g* (10.1.4.0.1) Oracle home installed on the same host and on the same operating system platform.

You cannot upgrade an existing 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) installation on one host computer to a 10*g* (10.1.4.0.1) installation on another host computer.

Similarly, you cannot upgrade from one platform (for example, Microsoft Windows) to another platform (for example, Linux).

And finally, you cannot perform an upgrade remotely; instead, you must be logged in to the computer where both the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) source Oracle home and the 10*g* (10.1.4.0.1) destination Oracle home are installed.

2.4 Supported Upgrade Paths for Oracle Application Server 10*g* (10.1.4.0.1)

Table 2–2 lists the supported starting points for an upgrade to Oracle Application Server 10*g* (10.1.4.0.1).

Table 2–2 Supported Upgrade Paths for Oracle Identity Management 10g (10.1.4.0.1)

Starting Point	Description
Oracle Application Server 10*g* (9.0.4)	You can upgrade the OracleAS Identity Management components of an Oracle Application Server 10*g* (9.0.4) Oracle home to 10*g* (10.1.4.0.1), as long as you comply with the following restrictions before you begin the upgrade: ■ Be sure to apply the latest 10*g* (9.0.4) patchset. At the time this document was published, the latest patchset was 10g (9.0.4.3). However, be sure to refer to Oracle*MetaLink* for the latest patchsets and certification information. ■ If you have installed any 10*g* (9.0.4) middle tiers that are using the same OracleAS Metadata Repository as the OracleAS Identity Management components, you must first upgrade the middle tiers to 10*g* Release 2 (10.1.2). For more information, see Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)".
Oracle Application Server 10*g* Release 2 (10.1.2.0.0)	You can upgrade the OracleAS Identity Management components of a 10*g* Release 2 (10.1.2.0.0) Oracle home. However, before you begin the upgrade to 10*g* (10.1.4.0.1), you must apply the latest patchset. At the time this documentation was published, the latest patchset was 10*g* Release 2 (10.1.2.1.0). However, be sure to refer to Oracle*MetaLink* for the latest patchsets and certification information.
Oracle Application Server 10*g* Release 2 (10.1.2.0.1) Standard Edition One	You can upgrade the OracleAS Identity Management components of a 10*g* Release 2 (10.1.2.0.1) Standard Edition One Oracle home. However, before you begin the upgrade to 10*g* (10.1.4.0.1), you must apply the latest patchset. At the time this documentation was published, the latest patchset was 10*g* Release 2 (10.1.2.1.0). However, be sure to refer to Oracle*MetaLink* for the latest patchsets and certification information.
Oracle Application Server 10*g* Release 2 (10.1.2.0.2)	You can upgrade the OracleAS Identity Management components of a 10*g* Release 2 (10.1.2.0.2) to 10*g* (10.1.4.0.1). **Note:** You can upgrade directly from 10*g* Release 2 (10.1.2.0.2) to 10*g* (10.1.4.0.1). There is no need to apply any patchsets before this upgrade.
Oracle Application Server 10*g* Release 2 (10.1.2.0.2)	You can upgrade the OracleAS Identity Management components of a 10*g* Release 2 (10.1.2.0.2) to 10*g* (10.1.4.0.1). **Note:** You can upgrade directly from 10*g* Release 2 (10.1.2.0.2) to 10*g* (10.1.4.0.1). There is no need to apply any patchsets before this upgrade.
OracleAS Portal 10*g* Release 2 (10.1.4)	If you upgrade your Oracle Application Server 10*g* Release 2 (10.1.2) installation to OracleAS Portal 10*g* Release 2 (10.1.4), then you can upgrade the OracleAS Identity Management components of the installation to Oracle Identity Management 10*g* (10.1.4.0.1).

Note: You cannot upgrade directly from Oracle Internet Directory Version 9.2.x to Oracle Identity Management 10*g* (10.1.4.0.1). Instead, you must first upgrade Oracle Internet Directory 9.2.x to Oracle Application Server 10*g* (9.0.4) or 10*g* Release 2 (10.1.2).

Internet Directory Version 9.2.0.x was a standalone release that was distributed with the Oracle9i Release 2 (9.2.0.x) database.

2.5 Verifying Support for Third-Party Products

Before you upgrade to Oracle Identity Management 10*g* (10.1.4.0.1), be sure to consider the implications of the upgrade on any third-party software you are using with the Oracle Application Server components.

Specifically, be sure to check with your third-party vendors to be sure the third-party software you are using is certified to work with Oracle Identity Management 10*g* (10.1.4.0.1) and its components.

Note, in particular, that Oracle Identity Management 10*g* (10.1.4.0.1) will likely require an upgrade of the Oracle database used to host your OracleAS Metadata Repository, and that Oracle Identity Management 10*g* (10.1.4.0.1) provides updated versions of the Oracle Identity Management components.

3 Understanding Version Compatibility

This chapter provides information you need to understand how Oracle Identity Management 10*g* (10.1.4.0.1) operates with previous versions of Oracle Application Server.

Before you proceed with your upgrade, review the information in this chapter to be sure all upgraded components and features will work in your Oracle Application Server environment.

This chapter contains the following sections:

- Using the Release 3 (10.1.4.0.1) Compatibility Matrix
- Release 3 (10.1.4.0.1) Identity Management Compatibility Issues
- Release 3 (10.1.4.0.1) OracleAS Metadata Repository Compatibility Issues
- Release 3 (10.1.4.0.1) Database Version Compatibility Issues
- List of the Release 3 (10.1.4.0.1) Compatibility Issues

3.1 Using the Release 3 (10.1.4.0.1) Compatibility Matrix

The Oracle Identity Management Release 3 (10.1.4.0.1) compatibility matrix is shown in Table 3–1. Before you use the compatibility matrix, you should be familiar with the Oracle Application Server installation types.

> **See Also:** Section 2.1.1, "Identifying the Existing Oracle Homes to Upgrade"

For example, if you want to upgrade a 10*g* (9.0.4) OracleAS Identity Management installation to Release 3 (10.1.4.0.1), you can use the compatibility matrix as follows:

1. Locate the column in the table that represents 10*g* (10.1.4.0.1) OracleAS Identity Management.
2. Locate the row that represents the type and the version of the Oracle homes you are currently running.

   For example, if you are running 10*g* (9.0.4) middle tiers, locate the **9.0.4 Middle Tier** row of the table.

   The OracleAS Identity Management column of that row indicates that you can run 10*g* (9.0.4) middle tiers with an upgraded Release 3 (10.1.4.0.1) OracleAS Identity Management; however, there are potential problems and solutions you might have to consider before you can run this configuration.

3. If there are problems and solutions to consider, follow the reference in the intersecting table cell to learn more about which of the compatibility problems and solutions apply to the selected configuration.

> **Note:** Some of the workarounds and issues described in this chapter are the result of incompatibilities with the version of the database used to host the OracleAS Metadata Repository. For more information, see Section 3.4, "Release 3 (10.1.4.0.1) Database Version Compatibility Issues".

Table 3–1 Oracle Application Server Compatibility Topics

	10.1.4.0.1 OracleAS Identity Management	10.1.4.0.1 OracleAS Metadata Repository
9.0.4 Middle Tiers	Supported.	Not Supported. See Section 3.3.1.
9.0.4 OracleAS Identity Management	Not supported. See Section 3.5.3.	Supported.
9.0.4 OracleAS Metadata Repository	Supported, but only when upgrading OracleAS Identity Management from 10*g* (9.0.4) or 10*g* Release 2 (10.1.2). See Section 3.2.1	Not Applicable.
10.1.2.0.0 Middle Tiers	Supported.	Supported.
10.1.2.0.0 OracleAS Identity Management	Not supported. See Section 3.5.3.	Supported.
10.1.2.0.0 OracleAS Metadata Repository	Supported, but only when upgrading OracleAS Identity Management from 10*g* (9.0.4) or 10*g* Release 2 (10.1.2). See Section 3.2.1	Not Applicable.
10.1.2.0.1 Standard Edition One Middle Tier	Supported.	Supported.
10.1.2.0.1 Standard Edition One Identity Management	Not supported. See Section 3.5.3.	Supported.
10.1.2.0.1 Standard Edition One Metadata Repository	Supported, but only when upgrading OracleAS Identity Management from 10*g* (9.0.4) or 10*g* Release 2 (10.1.2). See Section 3.2.1.	Not Applicable
10.1.2.0.2 Middle Tiers	Supported.	Supported.
10.1.2.0.2 Identity Management	Supported.	Supported.
10.1.2.0.2 Metadata Repository	Supported, but only when upgrading OracleAS Identity Management from 10*g* (9.0.4) or 10*g* Release 2 (10.1.2). See Section 3.2.1	Not Applicable.

Table 3–1 (Cont.) Oracle Application Server Compatibility Topics

	10.1.4.0.1 OracleAS Identity Management	10.1.4.0.1 OracleAS Metadata Repository
10.1.3.0.0 Middle Tiers	Supported as a security provider and for OracleAS Single Sign-On.	Not Applicable because Oracle Application Server Release 3 (10.1.3) middle tiers do not require an OracleAS Metadata Repository.

3.2 Release 3 (10.1.4.0.1) Identity Management Compatibility Issues

The following sections list the compatibility issues you should be aware of when you are installing or upgrading to 10*g* (10.1.4.0.1) OracleAS Identity Management in a mixed version environment:

- Running 10g (10.1.4.0.1) Identity Management with a 10g (9.0.4) or 10g Release 2 (10.1.2) Metadata Repository

3.2.1 Running 10*g* (10.1.4.0.1) Identity Management with a 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) Metadata Repository

You cannot install Oracle Identity Management 10*g* (10.1.4.0.1) against an existing 10*g* (9.0.4) OracleAS Metadata Repository.

> **See Also:** Section 3.5.2, "Cannot Install 10g (10.1.4.0.1) Identity Management Against a 10g (9.0.4) or 10g Release 2 (10.1.2) OracleAS Metadata Repository"

However, when you upgrade OracleAS Identity Management to 10*g* (10.1.4.0.1), the upgrade procedure automatically upgrades the Identity Management schemas in the OracleAS Metadata Repository.

As a result, if you are running 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Identity Management against a 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Metadata Repository, you can upgrade OracleAS Identity Management to 10*g* (10.1.4.0.1) as long as the database that hosts the OracleAS Metadata Repository is a supported version.

Specifically, consider the following OracleAS Identity Management upgrade scenarios:

- If you are using a colocated Infrastructure, you can upgrade OracleAS Identity Management to Release 3 (10.1.4.0.1) because in this scenario, the OracleAS Identity Management upgrade procedure automatically upgrades the database to a supported version and upgrades the OracleAS Identity Management schemas. The other component schemas, however, are upgraded and verified only if you run the Metadata Repository Upgrade Assistant (MRUA).

  > **See Also:** Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository"

- If you are using a non-colocated Infrastructure, you can upgrade OracleAS Identity Management to Release 3 (10.1.4.0.1), but you must first ensure that the database that hosts the OracleAS Metadata Repository is a supported version. This means you will likely have to upgrade the database first, either by using Oracle Universal Installer (if it is a seed database) or by manually upgrading the database if it is a OracleAS RepCA database.

See Also: Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository"

3.3 Release 3 (10.1.4.0.1) OracleAS Metadata Repository Compatibility Issues

The following sections list the compatibility issues you should be aware of when you are installing or upgrading to a Release 3 (10.1.4.0.1) OracleAS Metadata Repository in a mixed version environment:

- Running a Release 3 (10.1.4.0.1) OracleAS Metadata Repository with 10g (9.0.4) Middle Tiers

3.3.1 Running a Release 3 (10.1.4.0.1) OracleAS Metadata Repository with 10*g* (9.0.4) Middle Tiers

You cannot run a Release 3 (10.1.4.0.1) OracleAS Metadata Repository with Oracle Application Server 10*g* (9.0.4) middle tiers.

This is because the Release 3 (10.1.4.0.1) OracleAS Metadata Repository contains the 10*g* Release 2 (10.1.2.0.2) component schemas, which are not compatible with 10*g* (9.0.4) middle tiers.

If you are upgrading from 10*g* (9.0.4), you must first upgrade your 10*g* (9.0.4) middle tiers to 10*g* Release 2 (10.1.2). Then, you can upgrade the OracleAS Metadata Repository to Release 3 (10.1.4.0.1).

See Also: Section 2.3.1, "Middle Tiers Must Be Upgraded Before OracleAS Metadata Repository"

3.4 Release 3 (10.1.4.0.1) Database Version Compatibility Issues

A discussion of version compatibility is not complete without mentioning the version of the database used for the OracleAS Infrastructure components.

For information on the supported database versions for Release 3 (10.1.4.0.1), see Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository".

3.5 List of the Release 3 (10.1.4.0.1) Compatibility Issues

The following sections describe the issues and workarounds you may encounter when running 10*g* (10.1.4.0.1) with earlier versions of Oracle Application Server:

- Problems Logging In to OracleAS Portal
- Cannot Install 10g (10.1.4.0.1) Identity Management Against a 10g (9.0.4) or 10g Release 2 (10.1.2) OracleAS Metadata Repository
- Release 3 (10.1.4.0.1) Identity Management General Compatibility Requirements

3.5.1 Problems Logging In to OracleAS Portal

If you install a 10*g* Release 2 (10.1.2) OracleAS Portal middle tier against a 10*g* (9.0.4) OracleAS Metadata Repository, you must run the OracleAS Upgrade Assistant from the 10*g* Release 2 (10.1.2) middle tier before you can access the OracleAS Portal using the 10*g* Release 2 (10.1.2) middle tier URL.

If you do not run the Upgrade Assistant, you can only access Portal using the 9.0.x middle tier URL.

An exception to this case is if no 9.0.x middle tier was ever installed against the 10*g* (9.0.4) OracleAS Metadata Repository. In this case, since the 10*g* Release 2 (10.1.2) middle tier is the first middle tier to be installed against the OracleAS Metadata Repository, you can access OracleAS Portal without running the Upgrade Assistant.

3.5.2 Cannot Install 10*g* (10.1.4.0.1) Identity Management Against a 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Metadata Repository

When you install Release 3 (10.1.4.0.1) Identity Management, you must identify a Release 3 (10.1.4.0.1) OracleAS Metadata Repository. This is because the Release 3 (10.1.4.0.1) OracleAS Identity Management components require the Release 3 (10.1.4.0.1) Identity Management schemas.

As a result of this requirement, you cannot specify a 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Metadata Repository while installing the Release 3 (10.1.4.0.1) OracleAS Identity Management.

3.5.3 Release 3 (10.1.4.0.1) Identity Management General Compatibility Requirements

The following sections provide information about the requirements you must consider when running Release 3 (10.1.4.0.1) Identity Management in an environment with multiple versions of Oracle Application Server:

- OracleAS Identity Management Components Must Be the Same Version as Their Required Schemas
- OracleAS Identity Management Components Must Use an Oracle Internet Directory Of the Same Version

3.5.3.1 OracleAS Identity Management Components Must Be the Same Version as Their Required Schemas

The OracleAS Metadata Repository contains schemas that are required by OracleAS Identity Management.

If you use the Oracle Universal Installer to upgrade Identity Management to 10*g* (10.1.4.0.1), then the upgraded Identity Management components can use a previous version of the OracleAS Metadata Repository for their Identity Management schemas. This is because the Identity Management schemas in the OracleAS Metadata Repository are updated as part of the Identity Management upgrade process.

However, if you install a new Identity Management Release 3 (10.1.4.0.1) Oracle home, then you cannot select a previous version of the OracleAS Metadata Repository to store the Identity Management schemas. Instead, when the installation procedure prompts you for an existing OracleAS Metadata Repository, you must specify an existing Release 3 (10.1.4.0.1) Metadata Repository. The Release 3 (10.1.4.0.1) OracleAS Metadata Repository you specify can be a freshly installed Release 3 (10.1.4.0.1) repository, or it can be a OracleAS Metadata Repository that was upgraded to Release 3 (10.1.4.0.1).

3.5.3.2 OracleAS Identity Management Components Must Use an Oracle Internet Directory Of the Same Version

OracleAS Identity Management consists of multiple components, such as Oracle Delegated Administration Services, Oracle Application Server Single Sign-On, Oracle

Application Server Certificate Authority, and Oracle Directory Integration Platform. These components require Oracle Internet Directory.

If you decide to install these individual OracleAS Identity Management Release 3 (10.1.4.0.1) components, you cannot install those components against a10*g* (9.0.4) or 10*g* Release 2 (10.1.2) Oracle Internet Directory.

Instead, you must first either upgrade the Oracle Internet Directory to Release 3 (10.1.4.0.1) or install a new Release 3 (10.1.4.0.1) Oracle Internet Directory.

4 Backup Strategies and System Availability During an Upgrade

This chapter provides guidelines for planning an upgrade. It consists of the following sections:

- Backup Strategies Before Upgrade
- Planning for System Downtime

4.1 Backup Strategies Before Upgrade

Before you start the upgrade process, you should have a clear understanding of the backup requirements. These requirements vary somewhat, depending upon whether you are upgrading a middle tier, an OracleAS Metadata Repository, or OracleAS Identity Management.

The following sections provide more information:

- Backup Strategies for OracleAS Metadata Repository Upgrades
- Backup Strategies for Identity Management Upgrades

4.1.1 Backup Strategies for OracleAS Metadata Repository Upgrades

In most cases, when you upgrade a OracleAS Metadata Repository, you must first upgrade the database that hosts the repository to database version supported by 10*g* (10.1.4.0.1).

> **See Also:** Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository"

4.1.1.1 Backing Up the Database Before Upgrading the Database Version

As with any database upgrade, standard procedure dictates that you back up your source OracleAS Metadata Repository before you upgrade the database version. For more information, see the Oracle Database documentation for your platform and database version.

4.1.1.2 Backing Up the Database Before Running MRUA

To upgrade the component schemas, you use the Metadata Repository Upgrade Assistant (MRUA). This upgrade of the component schemas is performed "in place," which means that MRUA alters the application server component schemas that exist in the database. It does not create a new copy of the schemas or the data they contain. The changes made by MRUA are irreversible.

As a result, before you run MRUA, you should perform a backup of the database that contains the schemas. This backup will allow you to restore your database to its original state before you run MRUA.

> **See Also:** *Oracle Application Server Administrator's Guide* for information about the Oracle Application Server Backup and Recovery Tool, which is designed to help you back up and recover your Oracle Application Server installations
>
> *Oracle Database Backup and Recovery Basics* in the Oracle Database 10*g* documentation library for information and guidelines for backing up your Oracle database

4.1.2 Backup Strategies for Identity Management Upgrades

The OracleAS Identity Management upgrade involves upgrading the configuration and data files in the Oracle home of the OracleAS Identity Management installation, as well as upgrading the OracleAS Identity Management schemas stored in the OracleAS Metadata Repository database.

Consider the following backup strategies when upgrading your OracleAS Identity Management installations:

- When you upgrade OracleAS Identity Management, you use the Oracle Universal Installer and the Oracle Application Server 10*g* (10.1.4.0.1) installation procedure. The installation procedure automatically installs a new 10*g* (10.1.4.0.1) destination Oracle home and copies configuration data from the source Oracle home to the destination Oracle home.

  As a result, the source Oracle home is not modified by the OracleAS Identity Management upgrade process and no additional or new backup strategies are required, other than those you already use to protect your application server data.

- The installation procedure also upgrades the OracleAS Identity Management schemas in the OracleAS Metadata Repository. These schemas include the Oracle Internet Directory and OracleAS Single Sign-On schemas.

  The upgrade of the OracleAS Identity Management schemas is performed "in place," which means that the procedure alters the OracleAS Identity Management schemas that exist in the database. It does not create a new copy of the schemas or the data they contain. The schemas changes made by the OracleAS Identity Management upgrade are irreversible.

  As a result, you should back up the OracleAS Metadata Repository database that contains the OracleAS Identity Management schemas before you upgrade.

4.1.3 Backup Strategies After Upgrading Your Oracle Application Server Instances

After you have completed and verified the upgrade of your Oracle Application Server environment, consider backing up your Oracle Application Server installations so you can easily restore your environment to the newly upgraded state.

In particular, consider backing up the newly upgraded OracleAS Metadata Repository database immediately after the upgrade process. After this initial post-upgrade backup, you can begin your regularly scheduled database backup routine. The initial backup after the upgrade will ensure that you can restore your environment to the newly upgraded state without repeating the upgrade process.

In addition, after you have moved your development or deployment activities to the newly upgraded Oracle Application Server installations, be sure to modify your regular backup routine to include the new Oracle Application Server Oracle homes.

4.2 Planning for System Downtime

This section contains information that will help you answer the following questions as you plan the Oracle Application Server upgrade:

- How much downtime should be allocated to upgrade and to troubleshooting the upgrade?
- What parts of the system are subject to downtime?
- When will the downtime occur?

Refer to the following sections for more information:

- Estimated Time Required to Upgrade
- Example Execution Times for the Metadata Repository Upgrade Assistant

4.2.1 Estimated Time Required to Upgrade

The duration of upgrade preparation tasks and upgrade processing is of concern when considering downtime. This section provides estimates of the duration of the upgrade of a basic configuration.

For more information, see Table 4–1, " Infrastructure Upgrade Duration Estimates"

Table 4–1 Infrastructure Upgrade Duration Estimates

Operation	Metadata Repository	Identity Management	Colocated Infrastructure[1]
Database backup: The database should be backed up with the user's preferred procedure.	1 hour	Not applicable.	Not applicable
Oracle home backup: The Infrastructure Oracle home should be backed up.	Not applicable.	1 hour	1 hour
Database upgrade: If the Metadata Repository was created with OracleAS RepCA and the database is not a supported version, you must upgrade the database manually to a supported version.	Not applicable	Not applicable	Not applicable
Installation and upgrade with Oracle Universal Installer Depending upon the installation type you are upgrading, the Oracle Universal Installer installs new OracleAS Identity Management components and, if the Oracle home contains an OracleAS Metadata Repository, automatically upgrades the OracleAS Metadata Repository database to the supported version.	3 hours[2]	30 minutes	3 hours, 30 minutes
Database backup before running MRUA	1 hour	Not applicable	1 hour
OracleAS Metadata Repository upgrade with MRUA: Component schemas in the Metadata Repository are upgraded.	1 hour See Section 4.2.2, "Example Execution Times for the Metadata Repository Upgrade Assistant" for more information.	Not applicable	1 hour See Section 4.2.2, "Example Execution Times for the Metadata Repository Upgrade Assistant" for more information.
Identity Management post-upgrade: Perform all post-upgrade tasks.	Not Applicable.	1 hour	1 hours
Total:	6 hours	2 hours, 30 minutes	7 hours, 30 minutes

[1] The upgrade duration of the Metadata Repository and Identity Management may be shorter than that of the sum of the durations required to upgrade each piece individually, since common tasks need only be executed once.

[2] Note that if the OracleAS Metadata Repository is being used only to support middle tiers that are part of a database-based Oracle Application Server Farm, the J2EE and Web Cache middle tiers that use the OracleAS Metadata Repository can continue operating during the OracleAS Metadata Repository upgrade.

4.2.2 Example Execution Times for the Metadata Repository Upgrade Assistant

The time required to run MRUA to upgrade the component schemas in the OracleAS Metadata Repository will vary, depending upon your hardware and the amount of data in your OracleAS Metadata Repository. However, testing of MRUA has shown the following typical execution times on the following hardware and software platforms:

- 1 hour, 40 minutes on a Sun UltraSPARC 60, dual CPU, running Solaris 2.9
- 45 minutes on a 2.4GHz Pentium 4, running Windows 2000 Service Pack 4

Part II

Performing the Upgrade

This part contains the following chapters:

- Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)"
- Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository"
- Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management"
- Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository"
- Chapter 9, "Component-Specific Post-Upgrade Procedures"
- Chapter 10, "Verifying the Upgrade and Decommissioning the Source Oracle Homes"

5

Upgrading 10*g* (9.0.4) Middle Tiers to 10*g* Release 2 (10.1.2)

If you are upgrading from Oracle Application Server 10*g* (9.0.4) and you have installed and configured any 10*g* (9.0.4) middle tier Oracle homes, then you might have to upgrade the middle tiers to Oracle Application Server 10*g* Release 2 (10.1.2) before you proceed with OracleAS Identity Management upgrade.

For more information, see the following sections of this chapter:

- Task 1: Determine Whether or Not to Upgrade Your 10g (9.0.4) Middle Tiers
- Task 2: Locate Instructions for Upgrading Middle Tiers to 10g Release 2 (10.1.2)

> **Note:** If you are using 10*g* Release 2 (10.1.2) middle tiers, you can skip this chapter and go directly to Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository".

5.1 Task 1: Determine Whether or Not to Upgrade Your 10*g* (9.0.4) Middle Tiers

You must upgrade your 10*g* (9.0.4) middle tiers if all of the following statements are true:

- You have installed any 10*g* (9.0.4) middle tiers using the Portal and Wireless, Business Intelligence and Forms, or Forms and Reports Services installation types.
- Those middle tiers use the same OracleAS Metadata Repository database as the OracleAS Identity Management Oracle home you are about to upgrade.

If both of the previous statements apply, then the middle tier upgrade is necessary because as part of the 10*g* (10.1.4.0.1) upgrade, you upgrade the 10*g* (9.0.4) OracleAS Metadata Repository component schemas to 10*g* Release 2 (10.1.2.0.2). Oracle Application Server 10*g* (9.0.4) middle tiers are not compatible with 10*g* Release 2 (10.1.2) component schemas.

As a result, all middle tiers that use the Oracle Identity Management 10*g* (10.1.4.0.1) OracleAS Metadata Repository, must be upgraded to 10*g* Release 2 (10.1.2) before you run the Metadata Repository Upgrade Assistant (MRUA).

Figure 5–1 shows a typical scenario where the 10*g* (9.0.4) middle tiers use the same OracleAS Metadata Repository as Oracle Identity Management. In this case, you must upgrade your 10*g* (9.0.4) middle tiers before you run MRUA on the OracleAS Metadata Repository.

Figure 5–2 shows the scenario where the 10*g* (9.0.4) middle tiers use their own OracleAS Metadata Repository. In this scenario, the 10*g* (9.0.4) middle tiers are not affected by the 10*g* (10.1.4.0.1) upgrade. In this case, you do not need to upgrade the 10*g* (9.0.4) middle tiers before running MRUA on the OracleAS Metadata Repository that hosts the Oracle Identity Management schemas.

Figure 5–1 Example of 10g (9.0.4) MIddle Tiers that Use the Same OracleAS Metadata Repository as Oracle Identity Management

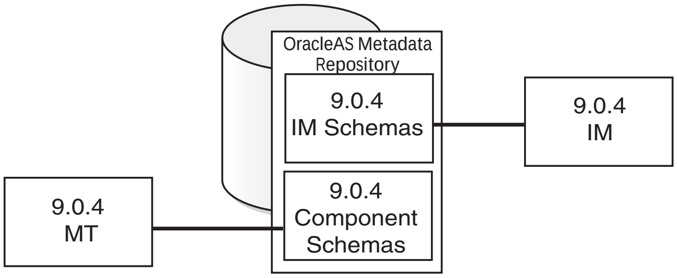
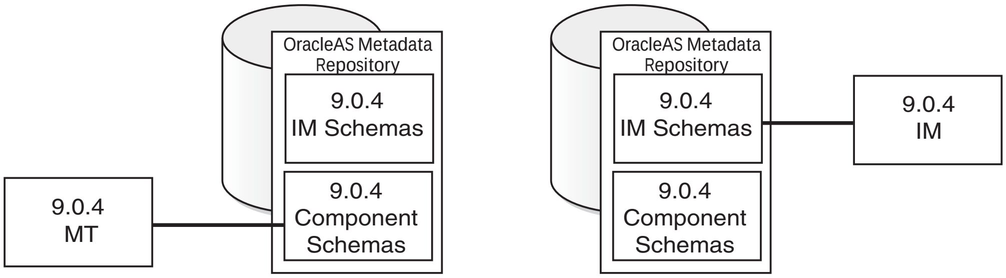


Figure 5–2 Example of 10g (9.0.4) Middle Tiers that Do Not Use the Same OracleAS Metadata Repository as Oracle Identity Management



5.2 Task 2: Locate Instructions for Upgrading Middle Tiers to 10*g* Release 2 (10.1.2)

To upgrade your 10*g* (9.0.4) middle tiers to 10*g* Release 2 (10.1.2):

1. Obtain the appropriate licenses and download the Oracle Application Server 10*g* Release 2 (10.1.2) software from the Oracle Technology Network (OTN):

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

2. Refer to the *Oracle Application Server Upgrade and Compatibility Guide* in the Oracle Application Server 10*g* Release 2 (10.1.2) documentation library, which is available on the Oracle Technology Network (OTN):

   ```
   http://www.oracle.com/technology/documentation/appserver101202.html
   ```

6

Upgrading the Database That Hosts the OracleAS Metadata Repository

Depending on the topology of your Oracle Application Server environment, you might have to upgrade the database that hosts the OracleAS Metadata Repository before you can upgrade to Oracle Identity Management 10*g* (10.1.4.0.1).

The following sections describe in detail the process of upgrading your OracleAS Metadata Repository database:

- Task 1: Review the OracleAS Metadata Repository Database Requirements
- Task 2: Determine Your Database Version and Upgrade Path
- Task 3: Upgrade the Database
- Task 4: Relocate the Database Datafiles, Control Files, and Log Files
- Task 5: Configure Oracle Enterprise Manager 10g Database Control

6.1 Task 1: Review the OracleAS Metadata Repository Database Requirements

The following sections contain information about supported database versions for Oracle Application Server 10*g* (10.1.4.0.1):

- Summary of the Database Versions Supported by Oracle Identity Management 10g (10.1.4.0.1)
- Using OracleMetaLink to Obtain the Latest Oracle Application Server Software Requirements

6.1.1 Summary of the Database Versions Supported by Oracle Identity Management 10*g* (10.1.4.0.1)

The database that hosts the OracleAS Metadata Repository must be one of the following supported versions:

Table 6–1 Supported Databases for the 10g (10.1.4.0.1) OracleAS Metadata Repository

Version	Description
Oracle Database 10*g* (10.1.0.5)	This is the version of the database that Oracle Universal Installer creates and configures when you install a new 10*g* (10.1.4.0.1) OracleAS Metadata Repository. This is also the database version that results when you use Oracle Universal Installer to upgrade a seed database in a colocated Infrastructure or non-colocated Infrastructure Oracle home. If you used the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS RepCA to install the OracleAS Metadata Repository in an existing Oracle 10*g* (10.1.0.x) database, then you must upgrade your database to this version.
Oracle9*i* Release 2 (9.2.0.7)	If you used the OracleAS RepCA to install the OracleAS Metadata Repository in an existing Oracle9*i* Database (9.1.0.x or 9.2.0.x), then you must upgrade your Oracle9*i* Database to this version.
Oracle Database 10*g* (10.2)	If you used the 10*g* Release 2 (10.1.2) OracleAS RepCA to install the OracleAS Metadata Repository in an existing Oracle Database 10*g* (10.2) database, then no database upgrade is necessary.

6.1.2 Using Oracle*MetaLink* to Obtain the Latest Oracle Application Server Software Requirements

The Oracle Application Server 10*g* (10.1.4.0.1) software requirements included in this guide were accurate at the time this manual was published. For the most up-to-date information about software requirements, including the database versions required for Oracle Identity Management 10*g* (10.1.4.0.1), refer to Oracle*MetaLink*:

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

After logging into Oracle*MetaLink*, click **Certify and Availability**. From the resulting Web page, you can view the latest certifications by product, platform, and product availability.

6.2 Task 2: Determine Your Database Version and Upgrade Path

Use the following sections to determine your version of your Oracle Identity Management database and to determine your database upgrade path:

- Determining Your Current Database Version
- Seed Database Versus OracleAS Metadata Repository Database
- Flow Chart of the OracleAS Metadata Repository Database Upgrade Process

6.2.1 Determining Your Current Database Version

To determine the version of your Oracle database, query the `PRODUCT_COMPONENT_VERSION` view, as follows:

```
prompt> sqlplus "sys/password as sysdba"
SQL> SELECT version FROM v$instance;
```

In this example, replace *password* with the password for the SYS database user.

6.2.2 Seed Database Versus OracleAS Metadata Repository Database

The upgrade path you choose for your OracleAS Metadata Repository database depends upon whether your OracleAS Metadata Repository database is a seed database or an OracleAS RepCA database.

> **See Also:** Section 2.1.4, "Determining Whether Your Database is a Seed Database or OracleAS RepCA Database"

After you determine whether your database is a seed database or an OracleAS RepCA database, you can begin to determine an upgrade path:

- If your database is a seed database, then you can use Oracle Universal Installer and the standard Oracle Identity Management 10*g* (10.1.4.0.1) installation procedure to upgrade your database automatically. Oracle Universal Installer upgrades your database to Oracle Database 10*g* (10.1.0.5).

  Refer to Section 6.3.1, "Upgrading a Seed Database with Oracle Universal Installer" for detailed instructions.

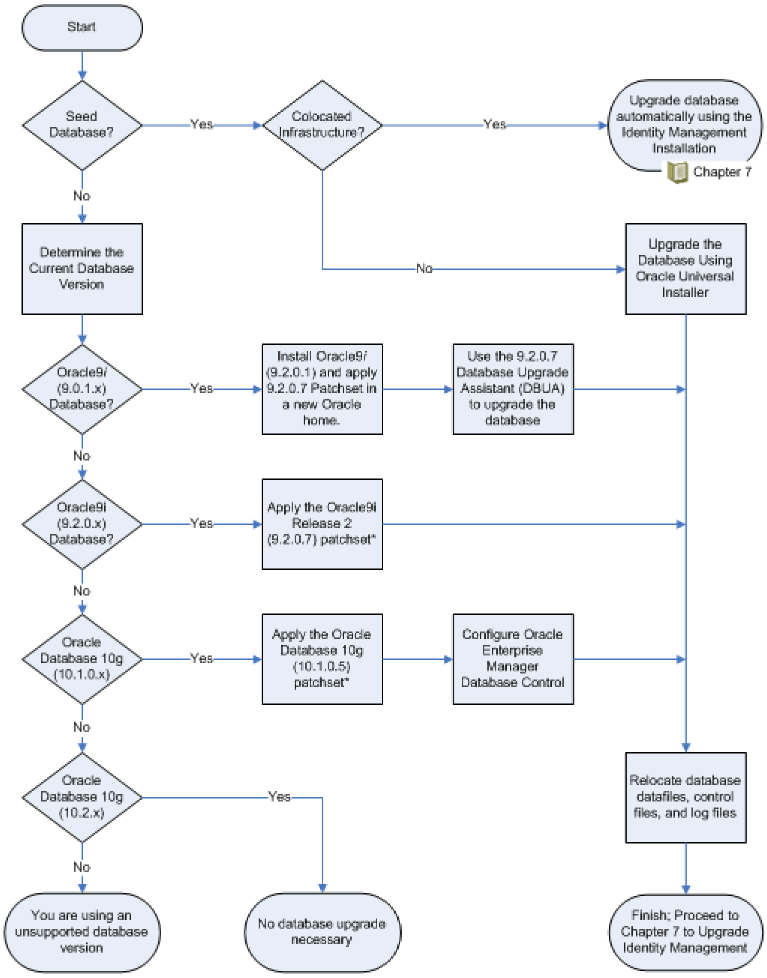
- If your database is an OracleAS RepCA database, you must first determine the current version of the database and upgrade the database, if necessary.

  Refer to Section 6.3.2, "Upgrading an OracleAS RepCA Database" for details about determining your OracleAS RepCA database upgrade path.

6.2.3 Flow Chart of the OracleAS Metadata Repository Database Upgrade Process

Figure 6–1 provides a flow chart that summarizes the procedure for upgrading your seed database or OracleAS RepCA database.

Figure 6–1 Summary of Determining Your Database Upgrade Path


Start
Seed Database?
Yes
Colocated Infrastructure?
Yes
Upgrade database automatically using the Identity Management Installation
Chapter 7
No
Determine the Current Database Version
No
Upgrade the Database Using Oracle Universal Installer
Oracle9*i* (9.0.1.x) Database?
Yes
Install Oracle9*i* (9.2.0.1) and apply 9.2.0.7 Patchset in a new Oracle home.
Use the 9.2.0.7 Database Upgrade Assistant (DBUA) to upgrade the database
No
Oracle9i (9.2.0.x) Database?
Yes
Apply the Oracle9i Release 2 (9.2.0.7) patchset*
No
Oracle Database 10g (10.1.0.x)
Yes
Apply the Oracle Database 10g (10.1.0.5) patchset*
Configure Oracle Enterprise Manager Database Control
No
Oracle Database 10g (10.2.x)
Yes
Relocate database datafiles, control files, and log files
No
You are using an unsupported database version
No database upgrade necessary
Finish; Proceed to Chapter 7 to Upgrade Identity Management

6.2.4 Table Describing the Steps in the Database Upgrade Path Flow Chart

Table 6–2 describes the upgrade process steps shown in Figure 6–1.

Table 6–2 Description of Steps in the Database Upgrade Path Flow Chart

Step	Description	More Information
Seed Database?	Determine whether or not the database you are upgrading is a seed database. If the database is a seed database, you can use Oracle Universal Installer to upgrade the database automatically. Otherwise, you must determine the current version of the database and then upgrade the database manually.	Section 2.1.4, "Determining Whether Your Database is a Seed Database or OracleAS RepCA Database"
Colocated Database?	Determine whether or not the seed database is part of a colocated Infrastructure. If the seed database is part of a colocated Infrastructure, you can upgrade the database automatically as part of the OracleAS Identity Management upgrade described in Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management" Otherwise, you can use Oracle Universal Installer and the procedure in Section 6.3.1, "Upgrading a Seed Database with Oracle Universal Installer" to upgrade the database.	Section 2.1.3, "Reviewing Your Current OracleAS Infrastructure Configuration"
Determine the Current Database Version	If the database is not a seed database, then you must determine the version of the database and use one of the remaining steps in this table to upgrade the database manually, depending upon the version.	Section 6.2.1, "Determining Your Current Database Version"
Oracle9*i* (9.0.1.x) database?	If your database is an Oracle9*i* Database, then you must upgrade the database to Oracle9*i* Release 2 (9.2.0.1) and apply the Oracle9*i* Release 2 (9.2.0.7) patchset.	Section 6.3.2.1, "If You Installed the OracleAS Metadata Repository in an Oracle9i Database" Section 6.3.2.2, "Special Instructions When Applying the Oracle9i Release 2 (9.2.0.7) Database Patchset"
Oracle Database 10*g* (10.1.x)?	If your database is an Oracle Database 10*g* (10.1.x) database, then you must apply the Oracle Database 10*g* (10.1.0.5) patchset.	Section 6.3.2.3, "If You Installed the OracleAS Metadata Repository in an Oracle 10g Database"
Oracle Database 10*g* (10.2.x)?	If your database is an Oracle Database 10*g* (10.2.x) database, then no database upgrade is necessary.	Section 6.3.2.3, "If You Installed the OracleAS Metadata Repository in an Oracle 10g Database"

6.3 Task 3: Upgrade the Database

The following sections describe how to upgrade your database, depending upon the database upgrade path for your Oracle Identity Management environment:

- Upgrading a Seed Database with Oracle Universal Installer
- Upgrading an OracleAS RepCA Database

6.3.1 Upgrading a Seed Database with Oracle Universal Installer

If the OracleAS Metadata Repository resides in a seed database, which was created using the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) application server installation procedure, you can use the Oracle Universal Installer and the Oracle Identity Management 10*g*

(10.1.4.0.1) installation procedure to upgrade your OracleAS Metadata Repository database.

This method of upgrading your database is the easiest method, since Oracle Universal Installer does the database upgrade for you.

> **Note:** When you use Oracle Universal Installer to upgrade your OracleAS Metadata Repository database, the installer invokes the Database Upgrade Assistant (DBUA).
>
> DBUA can take a significant amount of time to upgrade the database. For more information on how long it takes to upgrade your database, see Section 4.2, "Planning for System Downtime" and plan accordingly.

Refer to the following sections for more information on using Oracle Universal Installer to upgrade your OracleAS Metadata Repository database:

- Overview of Using Oracle Universal Installer to Upgrade a Seed Database
- Upgrading an OracleAS Metadata Repository Seed Database in a Non-Colocated Infrastructure
- Stopping the Database Listener When Prompted During the OracleAS Identity Management Upgrade

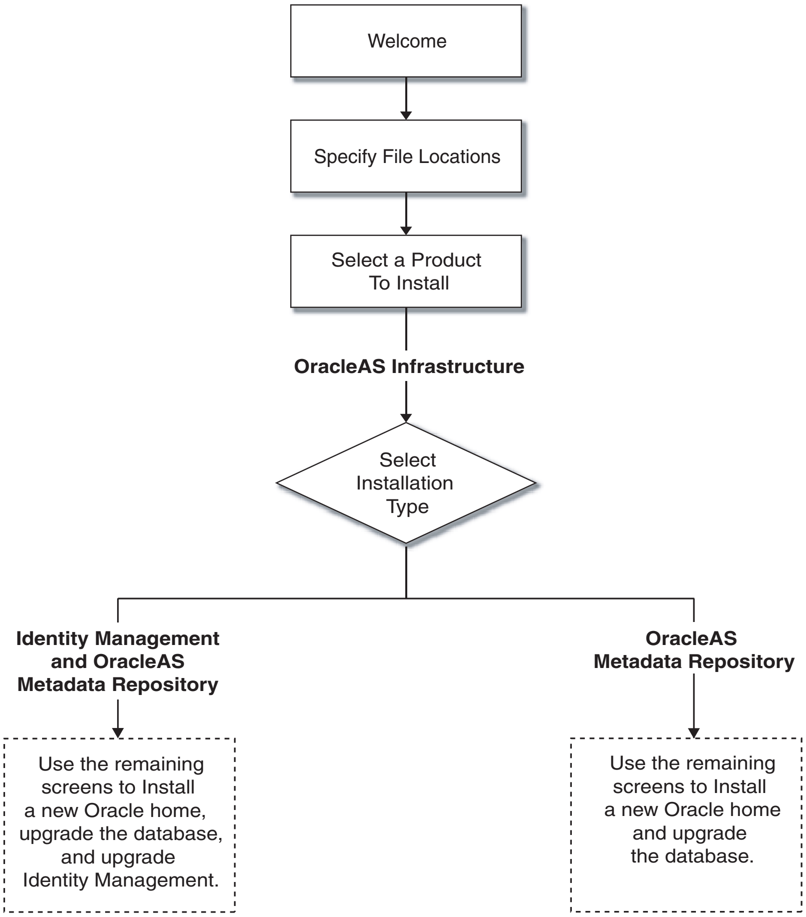
6.3.1.1 Overview of Using Oracle Universal Installer to Upgrade a Seed Database

Figure 6–2 provides a graphical representation of the first few screens of the 10*g* (10.1.4.0.1) installation procedure. It shows how you can select the appropriate Installation Type to install 10*g* (10.1.4.0.1) and upgrade your existing OracleAS Metadata Repository.

As shown in the illustration, if you are running OracleAS Identity Management in a colocated Infrastructure, then the database that hosts the OracleAS Metadata Repository will be upgraded automatically as part of the OracleAS Identity Management upgrade, as described in Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management".

On the other hand, if your OracleAS Metadata Repository resides in a non-colocated Infrastructure, refer to Section 6.3.1, "Upgrading a Seed Database with Oracle Universal Installer" for more information.

Figure 6–2 Using Oracle Universal Installer to Upgrade the OracleAS Metadata Repository Database


Welcome
Specify File Locations
Select a Product To Install
OracleAS Infrastructure
Select Installation Type
Identity Management and OracleAS Metadata Repository
OracleAS Metadata Repository
Use the remaining screens to Install a new Oracle home, upgrade the database, and upgrade Identity Management.
Use the remaining screens to Install a new Oracle home and upgrade the database.

6.3.1.2 Upgrading an OracleAS Metadata Repository Seed Database in a Non-Colocated Infrastructure

When you use the 10*g* (10.1.4.0.1) installation procedure to upgrade your OracleAS Metadata Repository database in a non-colocated Infrastructure, you perform the following tasks using the standard Oracle Universal Installer installation screens.

If your OracleAS Metadata Repository resides in a colocated Infrastructure, the database is upgraded automatically during the OracleAS Identity Management upgrade by Oracle Universal Installer.

1. Stop all the middle tiers that are using the services of the OracleAS Identity Management installation.
2. Make sure that the OracleAS Metadata Repository database and database listener are up and running.
3. Log in to the computer on which source instance is installed, as the same operating system user that performed the 10*g* (9.0.4) installation.

> **Note:** You must be logged in as a member of the `dba` operating system group.

4. Make sure the Oracle Internet Directory server is up and running.

To verify that Oracle Internet Directory is running, enter one of the following commands.

Note: You may have to temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the `ldapbind` command.

After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 10*g* (10.1.4.0.1) installer, as directed in Step 6.

If you are running Oracle Internet Directory on a non-secure port:

```
SOURCE_ORACLE_HOME/bin/ldapbind -p Non-SSL_port
```

If you are running Oracle Internet Directory on a secure port:

```
SOURCE_ORACLE_HOME/bin/ldapbind -p SSL_port -U 1
```

These commands should return a "bind successful" message.

5. Set the required environment variables, as defined in the section "Environment Variables" in the "Requirements" chapter of the *Oracle Application Server Installation Guide*.

   In particular, be sure to set following variables so they do not reference any Oracle home directories:

   - PATH
   - CLASSPATH
   - LD_LIBRARY_PATH
   - SHLIB_PATH

   In addition, be sure the following environment variables are not set:

   - TNS_ADMIN
   - ORACLE_HOME
   - ORACLE_SID

6. Mount the CD-ROM and start the installer.

   See Also: *Oracle Application Server Installation Guide* for detailed instructions about starting Oracle Universal Installer on your platform

7. Refer to Table 6–3 for information on the options you should select on each screen.

8. After the End of Installation screen appears, exit Oracle Universal Installer and then verify that Oracle Internet Directory and Oracle Application Server Single Sign-On are functioning and accessible in the new 10*g* (10.1.4.0.1) Oracle home.

   See Also: *Oracle Application Server Administrator's Guide*, Chapter 1, "Accessing the Single Sign-On Server"

Note that this procedure upgrades only the database version. After you upgrade the database, you must then run the Metadata Repository Upgrade Assistant (MRUA) to upgrade the OracleAS Metadata Repository component schemas, and you must run

Oracle Universal Installer to upgrade the OracleAS Identity Management schemas after the database is upgraded to a supported database version.

> **See Also:** Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository"
>
> Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management"

Table 6–3 Summary of the Oracle Universal Installer Screens During the OracleAS Metadata Repository Upgrade in a Non-Colocated Oracle Home

Screen	Description and Recommended Options to Select
Welcome	Welcomes you to Oracle Universal Installer and the Oracle Application Server 10*g* (10.1.4.0.1) installation procedure.
Specify File Locations	Enter a name and path for the new Oracle home. This new Oracle home will be the destination Oracle home for your Oracle Application Server 10*g* (10.1.4.0.1) upgrade.
Select a Product to Install	Select **OracleAS Infrastructure 10g**. If multiple languages are used in the OracleAS Infrastructure you are upgrading, then click **Product Languages**.
Language Selection	The screen appears only if you clicked **Product Languages** on the Select a Product to Install screen. If multiple languages are used in the OracleAS Infrastructure you are upgrading, select those languages. If you are not sure which languages were installed, but want languages other than English, click the double arrow button (>>) to select all languages.
Select Installation Type	Select **Metadata Repository**. **Note:** It is very important that you select the same installation type that is used in the Oracle home you are upgrading.
Upgrade Existing Infrastructure	This screen appears when Oracle Universal Installer detects an existing Oracle Application Server installation of the same type as the one you selected on the Select Installation Type screen. Select the option to upgrade an existing OracleAS Infrastructure, and then select the Oracle home you want to upgrade from the drop-down list. (If there is only one Infrastructure of the selected type on the computer, then the drop-down list is inactive.) Note that Oracle Universal Installer detects only the Oracle homes that match the installation type you selected on the Select Installation Type screen.
Specify Infrastructure Database Connection	Enter `SYS` in the **Username** field and the `SYS` user's password in the **Password** field.

Table 6–3 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Metadata Repository Upgrade in a Non-Colocated Oracle Home

Screen	Description and Recommended Options to Select
Warning dialog box	This dialog box warns you that all the clients of the OracleAS Metadata Repository database must now be stopped. Oracle Universal Installer will stop any clients within the current Oracle home automatically[1]. However, you must manually stop any database or OracleAS Metadata Repository clients that reside in another Oracle home. Clients of the OracleAS Metadata Repository include: ■ OracleAS Identity Management components that use this OracleAS Metadata Repository. ■ Middle tier instances that use this OracleAS Metadata Repository Within each middle tier that uses this OracleAS Metadata Repository, you must be sure to stop all components, including Oracle HTTP Server and OracleAS Web Cache. For more information, see the chapter "Starting and Stopping " in the *Oracle Application Server Administrator's Guide*.
Database Listener Warning Dialog Box	If a database listener is running on the host, a warning dialog box displays. Review the dialog box determine whether or not you need to stop the listener manually. For more information, see Section 6.3.1.3, "Stopping the Database Listener When Prompted During the OracleAS Identity Management Upgrade".
Summary	Use this screen to confirm the choices you've made. Click **Install** to begin upgrading to the new 10*g* (10.1.4.0.1) Oracle home. On UNIX systems, a dialog box appears when the copying is complete. This dialog box prompts you to run a configuration script as the root user. Follow the instructions in the dialog box and click **OK** when the script is finished.
The Configuration Assistants	After the initial software is installed, a set of configuration assistants automatically set up the components in the new 10*g* (10.1.4.0.1) Oracle home. Use this screen to follow the progress of each assistant and to identify any problems during this phase of the installation. **Notes:** ■ The Database Upgrade Assistant (DBUA) can take a significant amount of time to upgrade the database. For more information how long it takes to upgrade your database, see Section 4.2, "Planning for System Downtime". ■ While Database Upgrade Assistant is running, do not use the **Stop** button to interrupt the execution of Database Upgrade Assistant. If you press **Stop**, the underlying processes for Database Upgrade Assistant will continue to run. Also, Oracle Universal Installer will wait until those processes complete before returning control to the user.
End of Installation	When the installation and upgrade is complete, this screen provides important details about the 10*g* (10.1.4.0.1) Oracle home, such as the URL for the Application Server Control Console and the location of the `setupinfo.txt` file. After you review the information on this screen, you can exit Oracle Universal Installer and proceed to the post-upgrade tasks.

[1] You can access a log of the automated shutdown procedure executed by Oracle Universal Installer in the `shutdownprocesses.log` file, which is located in the `cfgtoollogs` directory in the destination Oracle home.

6.3.1.3 Stopping the Database Listener When Prompted During the OracleAS Identity Management Upgrade

Depending upon the OracleAS Identity Management configuration you are upgrading, you might be prompted to stop the database listener during the OracleAS Identity Management upgrade. Specifically, you should receive this prompt if you are upgrading a colocated Infrastructure, where the OracleAS Metadata Repository and OracleAS Identity Management are installed in the same Oracle home.

You should not stop the listener until you are prompted to do so. However, when such a prompt appears, use the `lsnrctl` utility to stop the database listener as follows:

1. Set the `ORACLE_HOME` environment variable to the Oracle home of the listener you want to stop.
2. Verify the version of the listener you are about to stop by entering the following command:

   ```
   $ORACLE_HOME/bin/lsnrctl version
   ```

   The `lsnrctl` utility displays information about the current database listener. Review the information to verify that you are stopping the correct listener.
3. Stop the listener by entering the following command:

   ```
   $ORACLE_HOME/bin/lsnrctl stop
   ```

6.3.2 Upgrading an OracleAS RepCA Database

If you used OracleAS RepCA to install the OracleAS Metadata Repository, you must verify the version of the database that hosts the repository.

As shown in Figure 6–1, your goal is to upgrade your database to a version that can support 10*g* (10.1.4.0.1).

> **See Also:** Section 6.1.2, "Using OracleMetaLink to Obtain the Latest Oracle Application Server Software Requirements" for information about obtaining the very latest information on the OracleAS Metadata Repository database requirements

Refer to the following sections for more information:

- If You Installed the OracleAS Metadata Repository in an Oracle9i Database
- Special Instructions When Applying the Oracle9i Release 2 (9.2.0.7) Database Patchset
- If You Installed the OracleAS Metadata Repository in an Oracle 10g Database

6.3.2.1 If You Installed the OracleAS Metadata Repository in an Oracle9*i* Database

If you installed your OracleAS Metadata Repository in an Oracle9*i* Database, you must be sure your database is Oracle9*i* Release 2 (9.2.0.7) or higher. Refer to the following sections for more information.

If You Installed the OracleAS Metadata Repository in an Oracle9*i* (9.0.1.x) Database

1. Install Oracle9*i* Release 2 (9.2.0.1) into a new Oracle home
2. Apply the Oracle9*i* Release 2 (9.2.0.7) patchset to the Oracle9*i* Release 2 (9.2.0.1) Oracle home; be sure to carefully follow the instructions in the Oracle9*i* Release 2 (9.2.0.7) patchset notes.

   You can download the patchset from Oracle*MetaLink* (`http://metalink.oracle.com`). Download patchset number 4163445.
3. Use the Database Upgrade Assistant (DBUA) in the Oracle9*i* Release 2 (9.2.0.7) Oracle home.

   > **See Also:** *Oracle9i Database Migration* in the Oracle9*i* Database documentation library for information about using DBUA and upgrading specific database components to Oracle9*i* Release 2 (9.2.0.7)

   > **Note:** The Database Upgrade Assistant (DBUA) can take a significant amount of time to upgrade the database. For more information how long it takes to upgrade your database, see Section 4.2, "Planning for System Downtime".

If you installed the OracleAS Metadata Repository in an Oracle9*i* Release 2 (9.2.0.x) database

1. Apply the Oracle9*i* Release 2 (9.2.0.7) patchset to the Oracle9*i* Release 2 (9.2.0.x) Oracle home; be sure to carefully follow the instructions in the Oracle9*i* Release 2 (9.2.0.7) patchset notes.

   You can download the patch set from Oracle*MetaLink* (`http://metalink.oracle.com`). Download patchset number 4163445.
2. See the section Section 6.3.2.2, "Special Instructions When Applying the Oracle9i Release 2 (9.2.0.7) Database Patchset" for more information before upgrading the OracleAS Metadata Repository.

6.3.2.2 Special Instructions When Applying the Oracle9*i* Release 2 (9.2.0.7) Database Patchset

When you upgrade your database to Oracle9*i* Release 2 (9.2.0.7), make sure that you carefully follow the instructions in the Oracle9*i* Release 2 (9.2.0.7) *Patch Set Notes*.

In particular, be sure to perform the following tasks after you run the apply the patch:

- Run the `catpatch.sql` script.
- Run `utlrp.sql`.

  To check that you have run the `catpatch.sql` script, you can run the following command in SQL*Plus:

  ```
  C:\> sqlplus "sys/password as sysdba"
  SQL> select comp_name, version, status from dba_registry
       where comp_id = 'CATPROC';
  ```

  You should get the following results:

  ```
  COMP_NAME                     VERSION     STATUS
  ----------------------------- ----------- --------
  Oracle9i Packages and Types   9.2.0.7.0   Valid
  ```

> **Note:** Be sure that the `catpatch.sql` script has been run against your database. Even if you have patched your database Oracle home to Oracle9*i* Release 2 (9.2.0.7), when you create a new database using the Database Configuration Assistant (DBCA), the new database might require the `catpatch.sql` script.

6.3.2.3 If You Installed the OracleAS Metadata Repository in an Oracle 10*g* Database

If you used the OracleAS RepCA to install the OracleAS Metadata Repository in an Oracle Database 10*g* database, then one of the following scenarios apply:

- If the database is an Oracle Database 10*g* (10.1.x) database, you must apply the Oracle Database 10*g* (10.1.0.5) patchset before you can use Metadata Repository Upgrade Assistant (MRUA) to upgrade the component schemas in the OracleAS Metadata Repository.
- If the database is an Oracle Database 10*g* (10.2.x) database, then no database upgrade is necessary.

6.4 Task 4: Relocate the Database Datafiles, Control Files, and Log Files

By default, after you upgrade your database, the datafiles, control files, and log files associated with the database remain in their original location. For example, if you used Oracle Universal Installer to upgrade a OracleAS Metadata Repository seed database, the datafiles for the OracleAS Metadata Repository database remain in the source Oracle home.

As a result, Oracle recommends that you relocate these files as a safeguard against inadvertently deleting them (for example, by deleting or decommissioning the entire source Oracle home directory tree). In addition, there may be performance benefits to moving the database files outside of the source Oracle home.

> **See Also:** "Renaming and Relocating Datafiles" and "Creating Additional Copies, Renaming, and Relocating Control Files" in the *Oracle Database Administrator's Guide*

6.5 Task 5: Configure Oracle Enterprise Manager 10*g* Database Control

The Oracle Enterprise Manager 10*g* Database Control provides a Web-based console you can use to manage Oracle Database 10*g*. When your OracleAS Metadata Repository is installed in an Oracle Database 10*g* instance, you can use the Database Control to manage your OracleAS Metadata Repository database.

> **See Also:** "Managing the OracleAS Metadata Repository Database with Database Control" in the *Oracle Application Server Administrator's Guide*

However, after you use Oracle Universal Installer to upgrade your OracleAS Metadata Repository database to Oracle Database 10*g*, the Database Control is not configured automatically. Instead, if you want to use the Database Control to manage your upgraded OracleAS Metadata Repository database, you must configure the Database Control manually using the Enterprise Manager Configuration Assistant (EMCA).

See Also: "Configuring the Database Control with EMCA" in *Oracle Enterprise Manager Advanced Configuration*

7 Using Oracle Universal Installer to Upgrade Oracle Identity Management

This chapter contains the following sections:

7.1 Overview of the OracleAS Identity Management Components

OracleAS Identity Management is part of the Oracle Application Server Infrastructure. It consists of:

- OracleAS Single Sign-On
- Oracle Internet Directory
- Oracle Delegated Administration Services
- Oracle Directory Integration and Provisioning
- Oracle Application Server Certificate Authority

> **See Also:** *Oracle Application Server Concepts* for an overview of the OracleAS Infrastructure
>
> *Oracle Application Server Installation Guide* for information about installing OracleAS Identity Management

> **Note:** If you are upgrading an OracleAS Identity Management replication environment, a high availability environment, or if you are interested in the data migration method upgrading OracleAS Identity Management, then refer to the appropriate appendix:
>
> - Appendix A, "Performing an Oracle Identity Management Multimaster and Fan-Out Replication Upgrade"
> - Appendix B, "Upgrading High Availability Configurations"
> - Appendix C, "Using the Data Migration Method of Upgrading OracleAS Identity Management"

7.2 Task 1: Review Your OracleAS Identity Management Configuration

Before you upgrade OracleAS Identity Management, you should be familiar with the various configurations that you may have implemented at your site.

Oracle Application Server provides three OracleAS Infrastructure installation types. These installation types allow you to install:

- Identity Management and OracleAS Metadata Repository
- Identity Management
- OracleAS Metadata Repository

Selecting the **Identity Management and OracleAS Metadata Repository** installation type results in a colocated Infrastructure, where both the OracleAS Metadata Repository and OracleAS Identity Management are in the same Oracle home.

If you install only **OracleAS Identity Management**, you must provide connection details and logon credentials for a valid OracleAS Metadata Repository.

The option you choose when you install the OracleAS Infrastructure determines whether or not you are installing a colocated Infrastructure or a non-colocated Infrastructure.

> **See Also:** Section 2.1, "Reviewing Your Current Oracle Application Server Installations" for more information about colocated Infrastructure and non-colocated Infrastructure installations

In addition, your OracleAS Identity Management configuration can be distributed or non-distributed. Consider the following examples of distributed OracleAS Identity Management installations:

- Figure 7–1 shows how the OracleAS Single Sign-On component of OracleAS Identity Management can be installed in a separate 10*g* (9.0.4) Oracle home from the Oracle Internet Directory, but share the same OracleAS Metadata Repository.
- Figure 7–2 shows an extension of the previous example. It introduces a third host, which is used to host an Oracle Application Server Certificate Authority (OCA) installation. The OCA installation uses the same Oracle Internet Directory as OracleAS Single Sign-On, but it has its own OracleAS Metadata Repository to store the OCA schema.

Figure 7–1 Distributed Identity Management - Example 1

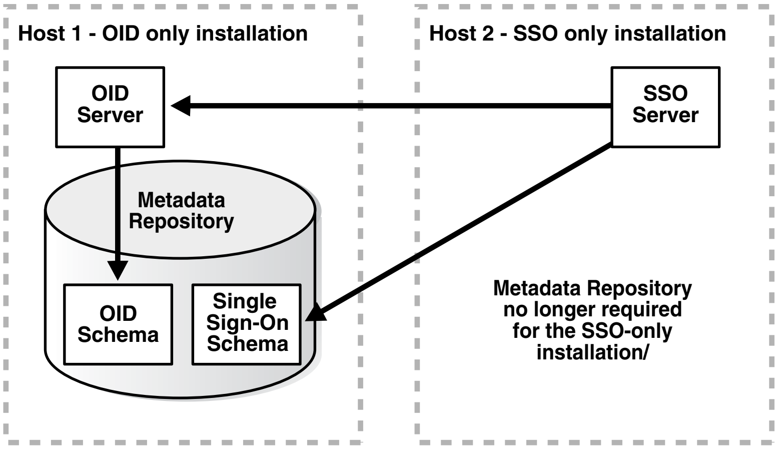
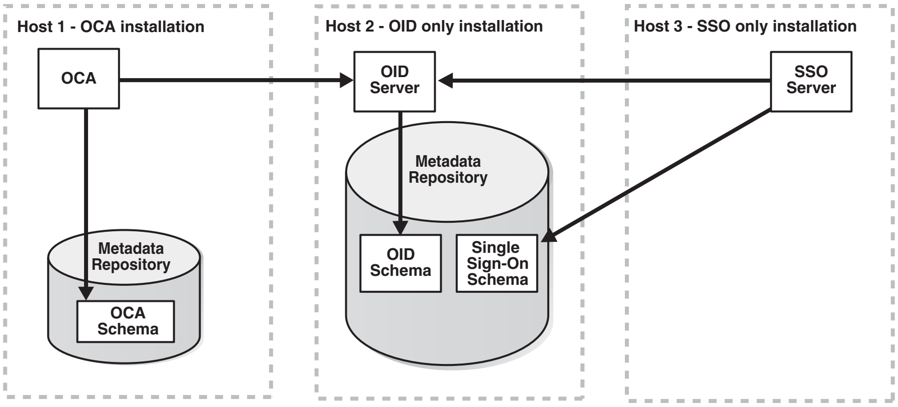

Host 1 - OID only installation
Host 2 - SSO only installation
OID Server
SSO Server
Metadata Repository
OID Schema
Single Sign-On Schema
Metadata Repository no longer required for the SSO-only installation/

Figure 7–2 Distributed Identity Management - Example 2



7.3 Task 2: Understand the OracleAS Identity Management Database Requirements

Regardless of the OracleAS Identity Management configuration, all OracleAS Identity Management installations require access to an OracleAS Metadata Repository. The OracleAS Metadata Repository is required because OracleAS Identity Management depends upon specific schemas that are created in the OracleAS Metadata Repository during the OracleAS Metadata Repository installation.

When you upgrade OracleAS Identity Management, the upgrade procedure upgrades the OracleAS Identity Management schemas in the OracleAS Metadata Repository. However, it can only do so if the database that hosts the OracleAS Metadata Repository is upgraded to a database version supported by Oracle Application Server 10*g* (10.1.4.0.1).

> **See Also:** Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository" for complete information and instructions for upgrading the OracleAS Metadata Repository database

7.4 Task 3: Back Up the OracleAS Identity Management Installation

Before you begin upgrading your OracleAS Identity Management installation, perform a backup of the OracleAS Identity Management Oracle home, and make sure that you have performed a backup of the database that hosts the OracleAS Identity Management schemas.

> **See Also:** Section 4.1, "Backup Strategies Before Upgrade"

7.5 Task 4: Perform the OracleAS Identity Management Upgrade

The following sections describe how to perform the OracleAS Identity Management upgrade for the typical OracleAS Identity Management configurations.

- Upgrading OracleAS Identity Management in a Colocated Infrastructure
- Upgrading OracleAS Identity Management in a Non-Colocated Infrastructure
- Upgrading Distributed OracleAS Identity Management Configurations

> **See Also:** Appendices A through C for information about upgrading more advanced OracleAS Identity Management configurations

7.5.1 Upgrading OracleAS Identity Management in a Colocated Infrastructure

If OracleAS Identity Management is installed as part of a colocated Infrastructure, you can use Oracle Universal Installer to do all of the following as part of the Oracle Application Server 10*g* (10.1.4.0.1) installation procedure:

- Upgrade the OracleAS Metadata Repository database.
- Upgrade the OracleAS Identity Management program, configuration, and data files.
- Upgrade the OracleAS Identity Management schemas in the OracleAS Metadata Repository.

To upgrade OracleAS Identity Management in a colocated Infrastructure Oracle home:

1. Stop all the middle tiers that are using the services of the OracleAS Identity Management installation.
2. Log in to the computer on which 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) instance is installed, as the same operating system user that performed the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) installation.

   > **Note:** You must be logged in as a member of the `dba` operating system group.

3. Make sure that the OracleAS Metadata Repository database and database listener are up and running.
4. Make sure the Oracle Internet Directory server is up and running.

   To verify that Oracle Internet Directory is running, you can use the Application Server Control Console, or you can use a command-line tool.

   To use the Application Server Control, enter the Application Server Control URL in your browser and navigate to the Application Server Home page for the OracleAS Infrastructure installation. Check the status of the **Internet Directory** component in the System Components table.

   To use the command line to check the status of the Oracle Internet Directory, use the following commands:

   If you are running Oracle Internet Directory on a non-secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p Non-SSL_port
   ```

   If you are running Oracle Internet Directory on a secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p SSL_port -U 1
   ```

   These commands should return a "bind successful" message.

Note: If you receive an "unable to locate message file" error, temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the `ldapbind` command.

After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 10*g* (10.1.4.0.1) installer, as directed in Step 5.

See Also: "Syntax for LDIF and Command-Line Tools" in the *Oracle Internet Directory Administrator's Guide* for more information about the `ldapbind` utility

Note: Oracle Internet Directory 10*g* (9.0.4) allows you to start and stop the directory service using OPMN or the `oidctl` utility.

Before upgrading a 10*g* (9.0.4) OracleAS Identity Management Oracle home that contains Oracle Internet Directory, start the Oracle Internet Directory instance using the `opmnctl` utility or the Application Server Control Console. Do not use the `oidctl` utility to start and stop Oracle Universal Installer in a 10*g* (9.0.4) Oracle home; otherwise, Oracle Universal Installer will not be able to start and stop Oracle Internet Directory automatically during the upgrade process.

The correct use of `opmnctl` and `oidctl` is described in the Chapter "Oracle Internet Directory Process Control–Best Practices" in the *Oracle Internet Directory Administrator's Guide*.

5. Set the required environment variables, as defined in the section "Environment Variables" in the "Requirements" chapter of the *Oracle Application Server Installation Guide*.

   In particular, be sure to set following variables so they do not reference any Oracle home directories:

   - PATH
   - CLASSPATH
   - LD_LIBRARY_PATH
   - SHLIB_PATH

   In addition, be sure the following environment variables are not set:

   - TNS_ADMIN
   - ORACLE_HOME
   - ORACLE_SID

6. Mount the media and start the installer.

   See Also: *Oracle Application Server Installation Guide* for detailed instructions about starting Oracle Universal Installer on your platform

7. Refer to Table 7–1 for information on the options you should select on each screen.

8. After the End of Installation screen appears, exit Oracle Universal Installer and then verify that Oracle Internet Directory and Oracle Application Server Single Sign-On are functioning and accessible in the new 10*g* (10.1.4.0.1) Oracle home.

   See Also: *Oracle Application Server Administrator's Guide*, Chapter 1, "Accessing the Single Sign-On Server"

Table 7–1 Summary of the Oracle Universal Installer Screens During the OracleAS Identity Management Upgrade in a Colocated infrastructure

Screen	Description and Recommended Options to Select
Welcome	Welcomes you to Oracle Universal Installer and the Oracle Identity Management 10*g* (10.1.4.0.1) installation procedure.
Specify File Locations	Enter a name and path for the new Oracle home. This new Oracle home is called the destination Oracle home for your Oracle Identity Management 10*g* (10.1.4.0.1) upgrade.
Select a Product to Install	Select **Oracle Application Server Infrastructure 10g**. If multiple languages are used in the OracleAS Infrastructure you are upgrading, then click **Product Languages**.
Language Selection	The screen appears only if you clicked **Product Languages** on the Select a Product to Install screen. If multiple languages are used in the OracleAS Infrastructure you are upgrading, select those languages. If you are not sure which languages were installed, but want languages other than English, click the double arrow button (>>) to select all languages.
Select Installation Type	Select **Identity Management and Metadata Repository**. **Note:** It is very important that you select the same installation type that is used in the Oracle home you are upgrading.
Product-Specific Prerequisite Checks	This screen lists the prerequisites that are checked automatically for you by Oracle Universal Installer. If any of the prerequisites are not met, then you can choose to stop the installation and update your system as suggested by the information on this screen. Otherwise, if the screen warns you about a specific prerequisite, you can select the appropriate check box to acknowledge the prerequisite and then continue with the installation.
Upgrade Existing Infrastructure	This screen appears when Oracle Universal Installer detects an existing Oracle Application Server installation of the same type as the one you selected on the Select Installation Type screen. Select the option to upgrade an existing OracleAS Infrastructure, and then select the Oracle home you want to upgrade from the drop-down list. (If there is only one Infrastructure of the selected type on the computer, then the drop-down list is inactive.)

Table 7–1 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Identity Management Upgrade in a Colocated infrastructure

Screen	Description and Recommended Options to Select
Confirm Pre-Installation Requirements	This screen prompts you to verify that you have performed the recommended pre-installation tasks and that you have met specific pre-installation requirements. In particular, use this screen to verify that you have backed up the necessary files in the Oracle home that you are about to upgrade, and--if you are on a UNIX system--verify that you have root privileges on the selected host. Select the pre-installation requirements that you have met. If you have not met the pre-installation requirements, you can cancel the installation, perform the required tasks, and then start the installation again later.
Specify Oracle Internet Directory Login	In the **Username** field, enter the superuser distinguished name (DN) for the Oracle Internet Directory you are about to upgrade. The superuser DN `cn=orcladmin` is the default for this field; change this value only if the Oracle Internet Directory superuser DN is not `cn=orcladmin`. In the **Password** field, enter the password for the superuser DN.
Specify Infrastructure Database Connection Information	Enter `SYS` in the **Username** field and the `SYS` user's password in the **Password** field.
Warning dialog box	This dialog box warns you that all the clients of the OracleAS Metadata Repository database must now be stopped. Oracle Universal Installer will automatically stop any clients within the source Oracle home.[1] However, you must manually stop any database clients and OracleAS Metadata Repository clients that reside in another Oracle home. Clients of the OracleAS Metadata Repository include: ■ OracleAS Identity Management components that use this OracleAS Metadata Repository. ■ Middle tier instances that use this OracleAS Metadata Repository Within each middle tier that uses this OracleAS Metadata Repository, you must be sure to stop all components, including Oracle HTTP Server and OracleAS Web Cache. For more information, see the chapter "Starting and Stopping " in the *Oracle Application Server Administrator's Guide*.
Database Listener Warning Dialog Box	Review the dialog box determine whether or not you need to stop the listener manually. For more information, see Section 6.3.1.3, "Stopping the Database Listener When Prompted During the OracleAS Identity Management Upgrade".

Table 7–1 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Identity Management Upgrade in a Colocated infrastructure

Screen	Description and Recommended Options to Select
Specify Instance Name and ias_admin Password	Enter a name for the new Oracle Application Server 10*g* (10.1.4.0.1) instance and a password for the `ias_admin` Administrator account. You use the `ias_admin` password to log on to Application Server Control Console to manage upgraded Oracle Application Server. In general, the minimum length of the `ias_admin` password is five alphanumeric characters. At least one of the characters must be a number and the password cannot start with a number. For more information, see the section "The ias_admin User and Restrictions on its Password" in the *Oracle Application Server Installation Guide*.
Summary	Use this screen to confirm the choices you've made. Click **Install** to begin upgrading to the new 10*g* (10.1.4.0.1) Oracle home. A dialog box appears when the copying is complete. This dialog box prompts you to run a configuration script as the root user. Follow the instructions in the dialog box and click **OK** when the script is finished.
The Configuration Assistants	After the initial software is installed, a set of configuration assistants automatically set up the components in the new 10*g* (10.1.4.0.1) Oracle home. Use this screen to follow the progress of each assistant and to identify any problems during this phase of the installation. **Notes:** ■ The Database Upgrade Assistant (DBUA) can take a significant amount of time to upgrade the database. For more information how long it takes to upgrade your database, see Section 4.2, "Planning for System Downtime". ■ While Database Upgrade Assistant is running, do not use the **Stop** button to interrupt the execution of Database Upgrade Assistant. If you press **Stop**, the underlying processes for Database Upgrade Assistant will continue to run. Also, Oracle Universal Installer will wait until those processes complete before returning control to the user.
End of Installation	When the installation and upgrade is complete, this screen provides important details about the 10*g* (10.1.4.0.1) Oracle home, such as the URL for the Application Server Control Console and the location of the `setupinfo.txt` file. After you review the information on this screen, you can exit Oracle Universal Installer and proceed to the post-upgrade tasks.

[1] You can access a log of the automated shutdown procedure executed by Oracle Universal Installer in the `shutdownprocesses.log` file, which is located in the `cfgtoollogs` directory in the destination Oracle home.

7.5.2 Upgrading OracleAS Identity Management in a Non-Colocated Infrastructure

To upgrade OracleAS Identity Management in a non-colocated Infrastructure, you use Oracle Universal Installer just as you do when OracleAS Identity Management is in a colocated Infrastructure.

To upgrade OracleAS Identity Management in a non-colocated Infrastructure:

1. Verify that the version of the database that hosts the OracleAS Identity Management schemas is a supported version for 10*g* (10.1.4.0.1) OracleAS Identity Management.

   If necessary, upgrade the database by using the instructions in Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository".

2. Make sure that the OracleAS Metadata Repository database and database listener are up and running.

3. Log in to the computer on which the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) instance is installed, as the same operating system user that performed the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) installation.

   > **Note:** You must be logged in as a member of the `dba` operating system group.

4. Make sure the Oracle Internet Directory server is up and running.

   To verify that Oracle Internet Directory is running, enter one of the following commands.

   > **Note:** You may have to temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the `ldapbind` command.
   >
   > After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 10*g* (10.1.4.0.1) installer, as directed in Step 5.

   If you are running Oracle Internet Directory on a non-secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p Non-SSL_port
   ```

   If you are running Oracle Internet Directory on a secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p SSL_port -U 1
   ```

   These commands should return a "bind successful" message.

   > **See Also:** "Syntax for LDIF and Command-Line Tools" in the *Oracle Internet Directory Administrator's Guide* for more information about the `ldapbind` utility

Note: Oracle Internet Directory 10*g* (9.0.4) allows you to start and stop the directory service using OPMN or the `oidctl` utility.

Before upgrading an OracleAS Identity Management Oracle home that contains Oracle Internet Directory, start the Oracle Internet Directory instance using the `opmnctl` utility or the Application Server Control Console. Do not use the `oidctl` utility; otherwise, Oracle Universal Installer will not be able to start and stop Oracle Internet Directory automatically during the upgrade process.

The correct use of `opmnctl` and `oidctl` is described in the Chapter "Oracle Internet Directory Process Control–Best Practices" in the *Oracle Internet Directory Administrator's Guide*.

5. Be sure to set the environment variables, as defined in the section "Environment Variables" in the "Requirements" chapter of the *Oracle Application Server Installation Guide*.

   In particular, be sure to set following variables so they do not reference any Oracle home directories:

   - PATH
   - CLASSPATH
   - LD_LIBRARY_PATH
   - SHLIB_PATH

   In addition, be sure the following environment variables are not set:

   - TNS_ADMIN
   - ORACLE_HOME
   - ORACLE_SID

6. Mount the Oracle Application Server 10*g* (10.1.4.0.1) CD–ROM and start the installer.

   See Also: *Oracle Application Server Installation Guide* for detailed instructions about starting Oracle Universal Installer on your platform

7. Refer to Table 7–2 for information on the options you should select on each screen.

8. After the End of Installation screen appears, exit Oracle Universal Installer and then verify that Oracle Internet Directory and Oracle Application Server Single Sign-On are functioning and accessible in the new 10*g* (10.1.4.0.1) Oracle home.

   See Also: *Oracle Application Server Administrator's Guide*, Chapter 1, "Accessing the Single Sign-On Server"

Table 7–2 Summary of the Oracle Universal Installer Screens During the OracleAS Identity Management Upgrade in a 10g (9.0.4) Non-Colocated infrastructure

Screen	Description and Recommended Options to Select
Welcome	Welcomes you to Oracle Universal Installer and the Oracle Identity Management 10*g* (10.1.4.0.1) installation procedure.

Table 7–2 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Identity Management Upgrade in a 10g (9.0.4) Non-Colocated infrastructure

Screen	Description and Recommended Options to Select
Specify File Locations	Enter a name and path for the new Oracle home. This new Oracle home will be the destination Oracle home for your Oracle Identity Management 10*g* (10.1.4.0.1) upgrade.
Select a Product to Install	Select **OracleAS Infrastructure 10g**. If multiple languages are used in the OracleAS Infrastructure you are upgrading, then click **Product Languages**.
Language Selection	The screen appears only if you clicked **Product Languages** on the Select a Product to Install screen. If multiple languages are used in the OracleAS Infrastructure you are upgrading, select those languages. If you are not sure which languages were installed, but want languages other than English, click the double arrow button (>>) to select all languages.
Select Installation Type	Select **Identity Management**. **Note:** It is very important that you select the same installation type that is used in the Oracle home you are upgrading.
Upgrade Existing Infrastructure	This screen appears when Oracle Universal Installer detects an existing Oracle Application Server installation of the same type as the one you selected on the Select Installation Type screen. Select the option to upgrade an existing OracleAS Infrastructure, and then select the Oracle home you want to upgrade from the drop-down list. (If there is only one Infrastructure of the selected time on the computer, then the drop-down list is inactive.)
Specify OID Login	Enter the Oracle Internet Directory superuser distinguished name (DN) in the **Username** field. The superuser DN `cn=orcladmin` is the default for this field; change this value if the Oracle Internet Directory superuser DN is not `cn=orcladmin`. Enter the password for the superuser DN in the **Password** field.
Specify Infrastructure Database Connection Information	Enter `SYS` in the **Username** field and the `SYS` user's password in the **Password** field.
Warning dialog box	This dialog box warns you that all the clients of the OracleAS Identity Management installation must now be stopped. Oracle Universal Installer will automatically stop any clients within the source Oracle home automatically.[1] However, you must manually stop any OracleAS Identity Management clients that reside in another Oracle home Clients of an OracleAS Identity Management instance include: ■ OracleAS Identity Management components that are distributed and installed in another Oracle home ■ Middle tier instances that use this OracleAS Identity Management instance for authentication or identity services Within each middle tier that uses this OracleAS Identity Management instance, you must be sure to stop all components, including Oracle HTTP Server and OracleAS Web Cache. For more information, see the chapter "Starting and Stopping " in the *Oracle Application Server Administrator's Guide*.

Table 7–2 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Identity Management Upgrade in a 10g (9.0.4) Non-Colocated infrastructure

Screen	Description and Recommended Options to Select
Database Listener Warning Dialog Box	If a database listener is running on the host, a warning dialog box displays. Review the dialog box determine whether or not you need to stop the listener manually. For more information, see Section 6.3.1.3, "Stopping the Database Listener When Prompted During the OracleAS Identity Management Upgrade".
Specify Instance Name and ias_admin Password	Enter a name for the new Oracle Identity Management 10*g* (10.1.4.0.1) instance and a password for the `ias_admin` Administrator account. You use the `ias_admin` password to log on to the Application Server Control Console to manage the Oracle Application Server instance. In general, the minimum length of the `ias_admin` password is five alphanumeric characters. At least one of the characters must be a number and the password cannot start with a number. For more information, see the section "The ias_admin User and Restrictions on its Password" in the *Oracle Application Server Installation Guide*.
Summary	Use this screen to confirm the choices you've made. Click **Install** to begin upgrading to the new 10*g* (10.1.4.0.1) Oracle home. The install screen shows you the progress of the installation as it copies files to your local disk. On UNIX systems, a dialog box appears when the copying is complete. This dialog box prompts you to run a configuration script as the root user. Follow the instructions in the dialog box and click **OK** when the script is finished.
The Configuration Assistants	After the initial software is installed, a set of configuration assistants automatically set up the components in the new 10*g* (10.1.4.0.1) Oracle home. Use this screen to follow the progress of each assistant and to identify any problems during this phase of the installation.
End of Installation	When the installation and upgrade is complete, this screen provides important details about the 10*g* (10.1.4.0.1) Oracle home, such as the URL for the Application Server Control Console and the location of the `setupinfo.txt` file. After you review the information on this screen, you can exit Oracle Universal Installer and proceed to the post-upgrade tasks.

[1] You can access a log of the automated shutdown procedure executed by Oracle Universal Installer in the `shutdownprocesses.log` file, which is located in the `cfgtoollogs` directory in the destination Oracle home.

7.5.3 Upgrading Distributed OracleAS Identity Management Configurations

The following sections describe how to upgrade a distributed OracleAS Identity Management configuration:

- Upgrading a Distributed OracleAS Identity Management Configuration
- Verifying Whether OracleAS Identity Management Components are Enabled or Disabled

7.5.3.1 Upgrading a Distributed OracleAS Identity Management Configuration

A distributed OracleAS Identity Management configuration consists of multiple Oracle homes. One of the Oracle homes contains the Oracle Internet Directory.

In a distributed OracleAS Identity Management installation, the other Oracle homes contain additional OracleAS Identity Management components, such as OracleAS Single Sign-On, Delegated Administration Services, Oracle Directory Integration and Provisioning, and OracleAS Certificate Authority.

To upgrade a distributed OracleAS Identity Management configuration (as shown in Figure 7–1), do the following:

1. Review Section 7.5.3.2, "Verifying Whether OracleAS Identity Management Components are Enabled or Disabled" to determine exactly which OracleAS Identity Management components will be upgraded.

2. Synchronize the system clocks on all nodes where the OracleAS Identity Management components reside so they are running within 250 seconds of each other.

   When synchronizing the system clocks, make sure the clocks are set to the same time zone.

3. Upgrade the Oracle home that includes the Oracle Internet Directory used by the other OracleAS Identity Management components.

   You must upgrade the Oracle Internet Directory first before upgrading the other distributed OracleAS Identity Management components.

   To upgrade the Oracle Internet Directory Oracle home, use one of the following procedures, depending upon the type of installation used for the Oracle Internet Directory Oracle home:

   - If the Oracle Internet Directory Oracle home includes its OracleAS Metadata Repository, then use the procedure in Section 7.5.1, "Upgrading OracleAS Identity Management in a Colocated Infrastructure"
   - If the Oracle Internet Directory is in its own Oracle home, and the its OracleAS Metadata Repository resides in a different Oracle home, use the procedure in Section 7.5.2, "Upgrading OracleAS Identity Management in a Non-Colocated Infrastructure"

   > **Note:** If you are running only Oracle Internet Directory from the Oracle home, check to be sure the other OracleAS Identity Management components are disabled so they will not be upgraded or started in the destination 10*g* (10.1.4.0.1) Oracle home.
   >
   > For more information, see Section 7.5.3.2, "Verifying Whether OracleAS Identity Management Components are Enabled or Disabled".

4. Make sure that the OracleAS Metadata Repository database and database listener used by the distributed components are up and running.

5. Log in to the computer on which the distributed OracleAS Identity Management components are installed, as the same operating system user that performed the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) installation.

Note: You must be logged in as a member of the `dba` operating system group.

6. Make sure the Oracle Internet Directory server is upgraded to 10*g* (10.1.4.0.1) and that it is up and running.

   To verify that Oracle Internet Directory is running, enter one of the following commands.

   Note: You may have to temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the `ldapbind` command.

   After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 10*g* (10.1.4.0.1) installer, as directed in Step 5.

   If you are running Oracle Internet Directory on a non-secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p Non-SSL_port
   ```

   If you are running Oracle Internet Directory on a secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p SSL_port -U 1
   ```

   These commands should return a "bind successful" message.

7. Be sure to set the environment variables, as defined in the section "Environment Variables" in the "Requirements" chapter of the *Oracle Application Server Installation Guide*.

   In particular, be sure to set following variables so they do not reference any Oracle home directories:

   - PATH
   - CLASSPATH
   - LD_LIBRARY_PATH
   - SHLIB_PATH

   In addition, be sure the following environment variables are not set:

   - TNS_ADMIN
   - ORACLE_HOME
   - ORACLE_SID

8. Mount the Oracle Application Server 10*g* (10.1.4.0.1) CD–ROM and start the installer.

   See Also: *Oracle Application Server Installation Guide* for detailed instructions about starting Oracle Universal Installer on your platform

9. Refer to Table 7–3 for information on the options you should select on each screen.

10. After the End of Installation screen appears, exit Oracle Universal Installer and then verify that Oracle Internet Directory and Oracle Application Server Single Sign-On are functioning and accessible.

> **See Also:** *"Accessing the Single Sign-On Server" in the Oracle Application Server Single Sign-On Administrator's Guide*

Table 7–3 Summary of the Oracle Universal Installer Screens During a 10g (9.0.4) Distributed OracleAS Identity Management Upgrade

Screen	Description and Recommended Options to Select
Welcome	Welcomes you to Oracle Universal Installer and the Oracle Identity Management 10*g* (10.1.4.0.1) installation procedure.
Specify File Locations	Enter a name and path for the new Oracle home. This new Oracle home will be the destination Oracle home for your Oracle Identity Management 10*g* (10.1.4.0.1) upgrade.
Select a Product to Install	Select **Oracle Application Server Infrastructure 10g**. If multiple languages are used in the OracleAS Infrastructure you are upgrading, then click **Product Languages**.
Language Selection	The screen appears only if you clicked **Product Languages** on the Select a Product to Install screen. If multiple languages are used in the OracleAS Infrastructure you are upgrading, select those languages. If you are not sure which languages were installed, but want languages other than English, click the double arrow button (>>) to select all languages.
Select Installation Type	Select **Identity Management** or **Identity Management and Metadata Repository**, depending upon the installation type you selected when you installed the distributed OracleAS Identity Management components. **Note:** It is very important that you select the same installation type that is used in the Oracle home you are upgrading. In this case, you are upgrading a non-colocated OracleAS Identity Management installation, so you must select **Identity Management**.
Upgrade Existing Infrastructure	This screen appears when Oracle Universal Installer detects an existing Oracle Application Server installation of the same type as the one you selected on the Select Installation Type screen. Select the option to upgrade an existing OracleAS Infrastructure, and then select the Oracle home you want to upgrade from the drop-down list. (If there is only one Infrastructure of the selected time on the computer, then the drop-down list is inactive.)
Specify OID Login	Enter the Oracle Internet Directory superuser distinguished name (DN) in the **Username** field. The superuser DN `cn=orcladmin` is the default for this field; change this value if the Oracle Internet Directory superuser DN is not `cn=orcladmin`. Enter the password for the superuser DN in the **Password** field.
Specify Infrastructure Database Connection Information	Enter `SYS` in the **Username** field and the `SYS` user's password in the **Password** field.

Table 7–3 (Cont.) Summary of the Oracle Universal Installer Screens During a 10g (9.0.4) Distributed OracleAS Identity Management Upgrade

Screen	Description and Recommended Options to Select
Warning dialog box	This dialog box warns you that all the clients of the OracleAS Identity Management installation must now be stopped. Oracle Universal Installer will automatically stop any clients within the source Oracle home automatically.[1] However, you must manually stop any OracleAS Identity Management clients that reside in another Oracle home Clients of an OracleAS Identity Management instance include: ■ OracleAS Identity Management components that are distributed and installed in another Oracle home ■ Middle tier instances that use this OracleAS Identity Management instance for authentication or identity services Within each middle tier that uses this OracleAS Identity Management instance, you must be sure to stop all components, including Oracle HTTP Server and OracleAS Web Cache. For more information, see the chapter "Starting and Stopping " in the *Oracle Application Server Administrator's Guide*.
Database Listener Warning Dialog Box	If a database listener is running on the host, a warning dialog box displays. Review the dialog box determine whether or not you need to stop the listener manually. For more information, see Section 6.3.1.3, "Stopping the Database Listener When Prompted During the OracleAS Identity Management Upgrade".
Specify Instance Name and ias_admin Password	Enter a name for the new Oracle Application Server 10*g* (10.1.4.0.1) instance and a password for the `ias_admin` Administrator account. You use the `ias_admin` password to log on to Application Server Control Console to manage Oracle Application Server. In general, the minimum length of the `ias_admin` password is five alphanumeric characters. At least one of the characters must be a number and the password cannot start with a number. For more information, see the section "The ias_admin User and Restrictions on its Password" in the *Oracle Application Server Installation Guide*.
Summary	Use this screen to confirm the choices you've made. Click **Install** to begin upgrading to the new 10*g* (10.1.4.0.1) Oracle home. On UNIX systems, a dialog box appears when the copying is complete. This dialog box prompts you to run a configuration script as the root user. Follow the instructions in the dialog box and click **OK** when script is finished.

Table 7–3 (Cont.) Summary of the Oracle Universal Installer Screens During a 10g (9.0.4) Distributed OracleAS Identity Management Upgrade

Screen	Description and Recommended Options to Select
The Configuration Assistants	After the initial software is installed, a set of configuration assistants automatically set up the components in the new 10*g* (10.1.4.0.1) Oracle home. Use this screen to follow the progress of each assistant and to identify any problems during this phase of the installation. **Notes:** ■ The Database Upgrade Assistant (DBUA) can take a significant amount of time to upgrade the database. For more information how long it takes to upgrade your database, see Section 4.2, "Planning for System Downtime". ■ While Database Upgrade Assistant is running, do not use the **Stop** button to interrupt the execution of Database Upgrade Assistant. If you press **Stop**, the underlying processes for Database Upgrade Assistant will continue to run. Also, Oracle Universal Installer will wait until those processes complete before returning control to the user.
End of Installation	When the installation and upgrade is complete, this screen provides important details about the 10*g* (10.1.4.0.1) Oracle home, such as the URL for the Application Server Control Console and the location of the `setupinfo.txt` file. After you review the information on this screen, you can exit Oracle Universal Installer and proceed to the post-upgrade tasks.

[1] You can access a log of the automated shutdown procedure executed by Oracle Universal Installer in the `shutdownprocesses.log` file, which is located in the `cfgtoollogs` directory in the destination Oracle home.

7.5.3.2 Verifying Whether OracleAS Identity Management Components are Enabled or Disabled

When you upgrade a distributed OracleAS Identity Management configuration, the 10*g* (10.1.4.0.1) installer will upgrade any OracleAS Identity Management components that are enabled in the source Oracle home.

An OracleAS Identity Management component is considered enabled when it is marked as such in the following configuration file in the source Oracle home:

```
SOURCE_ORACLE_HOME/config/ias.properties
```

Before you upgrade your Oracle Internet Directory installation in a distributed OracleAS Identity Management configuration, you can check the contents of this file to verify which components are enabled. If necessary, modify the entries to reflect exactly which components you have enabled, and as a result, which components will be upgraded.

If you are running only Oracle Internet Directory in the Oracle home, the ias.properties file should contain the following entries:

```
SSO.LaunchSuccess=False
OID.LaunchSuccess=True
DAS.LaunchSuccess=False
DIP.LaunchSuccess=False
OCA.LaunchSuccess=False
```

On the other hand, if you are running OracleAS Single Sign-On, Oracle Delegated Administration Services, and Oracle Directory Integration and Provisioning in one

Oracle home, but using Oracle Internet Directory in another Oracle home, the entries would appear as follows:

```
SSO.LaunchSuccess=True
OID.LaunchSuccess=False
DAS.LaunchSuccess=True
DIP.LaunchSuccess=True
OCA.LaunchSuccess=False
```

8

Using MRUA to Upgrade the OracleAS Metadata Repository

The OracleAS Identity Management schemas are upgraded as part of the Oracle Identity Management 10*g* (10.1.4.0.1) upgrade in Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management". This chapter describes how to upgrade the component schemas using the Metadata Repository Upgrade Assistant (MRUA).

The following sections provide more information:

- Task 1: Understand and Prepare for the OracleAS Metadata Repository Upgrade
- Task 2: Run MRUA and Upgrade the OracleAS Metadata Repository Schemas
- Task 3: Verify the Success of the OracleAS Metadata Repository Upgrade

8.1 Task 1: Understand and Prepare for the OracleAS Metadata Repository Upgrade

Use the following sections to understand why you must upgrade the OracleAS Metadata Repository and to prepare for the OracleAS Metadata Repository upgrade:

- Why Upgrade the OracleAS Metadata Repository?
- Preparing to Upgrade the OracleAS Metadata Repository

8.1.1 Why Upgrade the OracleAS Metadata Repository?

Whenever you upgrade to a new version of Oracle Application Server, Oracle recommends that you upgrade all your Oracle Application Server components to the latest version. This ensures that you have the latest bug fixes and feature improvements. It also facilitates troubleshooting of any compatibility and configuration issues.

As a result, Oracle recommends that you use the Metadata Repository Upgrade Assistant (MRUA) to upgrade the component schemas in the OracleAS Metadata Repository to the latest version.

In fact, if you are already running Oracle Application Server 10*g* Release 2 (10.1.2.0.2), or if you have upgraded your 10*g* Release 2 (10.1.2) environment to OracleAS Portal 10*g* Release 2 (10.1.4), many of the component schemas will already be at the latest version. In those cases, MRUA alerts you in the MRUA output and in the MRUA log file if any of the component schemas were upgraded previously.

Note: The following Oracle Application Server component schemas are no longer part of the Metadata Repository upgrade for 10*g* (10.1.4.0.1), and are not upgrade by MRUA:

- Oracle Workflow
- Oracle Ultra Search
- Oracle Application Server Certificate Authority (OCA)
- Oracle BPEL Process Manager (BPEL)

Running MRUA also verifies that the proper component schemas are installed and valid; it also verifies that the database that hosts the OracleAS Metadata Repository has been upgraded to a supported version.

See Also: Section 8.3.2, "About Component Schema Version Numbers After Upgrading to 10g (10.1.4.0.1)"

8.1.2 Preparing to Upgrade the OracleAS Metadata Repository

Use the following procedure to prepare your Oracle Application Server environment for the OracleAS Metadata Repository upgrade:

1. Be sure that you have created a recent backup of the OracleAS Metadata Repository database.

   See Also: Section 4.1, "Backup Strategies Before Upgrade"

2. Verify that the database that hosts the OracleAS Metadata Repository has been upgraded to a supported version for this release.

   See Also: Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository"

3. If you are running any 10*g* (9.0.4) middle tiers that use the OracleAS Metadata Repository, be sure to upgrade those middle tiers to 10*g* Release 2 (10.1.2) before proceeding with the OracleAS Metadata Repository upgrade.

   See Also: Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)"

4. Verify that the Oracle Internet Directory and database processes are running

   Specifically, make sure that the following processes are up and running:

   - The database that hosts the OracleAS Metadata Repository
   - The database listener for the OracleAS Metadata Repository database
   - The Oracle Internet Directory instance where the OracleAS Metadata Repository database is registered

   Log in to the Application Server Control Console to verify that the necessary processes are running and that the required components are configured properly. For example, you can use the Application Server Control Console to verify that the Farm page displays correctly and that the Oracle Internet Directory and OracleAS Single Sign-On components are up and running.

From the Application Server Home page in the Application Server Control Console click **Ports** to view a list of the ports currently in use by the application server instance, and to verify that the components are configured properly.

> **See Also:** "Introduction to Administration Tools" in the *Oracle Application Server Administrator's Guide* for more information about using the Application Server Control Console

5. Stop Any Middle Tier Instances That Use the OracleAS Metadata Repository

   Before you use MRUA, you must stop all processes associated with each middle tier that uses the OracleAS Metadata Repository.

   Note that at this point in the upgrade process, as a prerequisite for running MRUA, all the middle tier instances should have been upgraded to 10*g* Release 2 (10.1.2).

   There are two ways to view all the Oracle Application Server instances that use the OracleAS Metadata Repository:

   - Display the Farm page in the Application Server Control Console.

     > **See Also:** "Introduction to Administration Tools" in the *Oracle Application Server Administrator's Guide* for more information about the Application Server Control Console Farm page

   - Use the following Distributed Configuration Management command in the Oracle home of any middle-tier or OracleAS Identity Management instance that belongs to the farm:

     ```
     ORACLE_HOME/dcm/bin/dcmctl listinstances
     ```

     > **See Also:** *Distributed Configuration Management Administrator's Guide* for more information about `dcmctl` commands

   To stop all processes in a 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) middle tier:

   a. Stop all the Oracle Process Manager and Notification Server (OPMN) processes in the Oracle home:

   ```
   ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

   b. Stop the Application Server Control:

   ```
   ORACLE_HOME/bin/emctl stop iasconsole
   ```

6. Check for Invalid Database Objects.

   Use the following procedure to make sure that none of the database objects that are required by Oracle Application Server are invalid:

   a. Connect to the OracleAS Metadata Repository database.

   For example:

   ```
   METADATA_REPOSITORY_ORACLE_HOME/bin/sqlplus "connect / as sysdba"
   ```

   b. When prompted, enter the SYS password.

   c. Issue the following SQL command:

   ```
   SELECT owner, object_type, object_name
      FROM all_objects
   ```

```
WHERE status='INVALID';
```

The query should not return any database objects that have an Oracle Application Server component schema (such as PORTAL, WIRELESS, and so on) in the 'owner' column.

If you find any invalid objects, run the `utlrp.sql` script from the SQL*Plus command line to recompile the invalid objects:

```
@?/rdbms/admin/utlrp.sql
```

8.2 Task 2: Run MRUA and Upgrade the OracleAS Metadata Repository Schemas

To run MRUA:

1. Log in to the computer where the OracleAS Metadata Repository is running; use the same user account that was used to install the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Metadata Repository.

   > **Note:** Be sure to log in to the computer where the OracleAS Metadata Repository is running as the same user who installed the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Metadata Repository. MRUA must be run on the computer that hosts the OracleAS Metadata Repository that you are about to upgrade.

2. Mount the Metadata Repository Upgrade Assistant and Utilities CD–ROM.

   The MRUA and Utilities CD–ROM is part of the Oracle Application Server CD–ROM Pack that you receive when you order the Oracle Application Server software.

3. Start MRUA by entering the following command, with the following required arguments, which are described in Table 8–1:

   ```
   MRUA_CD_ROOT_DIRECTORY/mrua/mrua.sh
   -oracle_home metadata_repository_oracle_home
   -oid_host Oracle_Internet_Directory_host
   -oid_ssl_port Oracle_Internet_Directory_SSL_port
   ```

Table 8–1 Summary of the Required MRUA Command Line Arguments

Argument	Description
-oracle_home	The destination 10*g* (10.1.4.0.1) OracleAS Metadata Repository home directory.
-oid_host	The name of the computer that hosts the Oracle Internet Directory where the OracleAS Metadata Repository is registered.
-oid_ssl_port	The secure port for the Oracle Internet Directory. For the purposes of upgrading the OracleAS Metadata Repository, you must use a secure connection to the Oracle Internet Directory.

> **Note:** The value of the `-oid_host` argument and `-oid_ssl_port` arguments must match the value of the corresponding properties defined in following configuration file in the Identity Management Oracle home:
>
> ```
> IDENTITY_MANAGEMENT_HOME/config/ias.properties
> ```
>
> For example:
>
> ```
> OIDhost=sys42.acme.com
> OIDsslport=636
> ```

4. When you are prompted, enter the password for the database SYS user account.

   MRUA needs the SYS password so it can access and modify the component schemas in the database.

5. When you are prompted, enter the Oracle Internet Directory `cn=orcladmin` administrator password.

   MRUA needs the Oracle Internet Directory password to connect to the Oracle Internet Directory in which the OracleAS Metadata Repository is registered.

   After you provide the required passwords, MRUA checks to be sure the Oracle Internet Directory is running and does one of the following:

   - If Oracle Internet Directory is down or unavailable, MRUA displays an error message and exits.
   - If Oracle Internet Directory is up and running, MRUA connects to the directory service and obtains additional information required to upgrade the component schemas.
   - If multiple instances of the OracleAS Metadata Repository are registered with the directory, MRUA prompts you to select the OracleAS Metadata Repository you want to upgrade.

     You can upgrade only one OracleAS Metadata Repository at a time. You must select the OracleAS Metadata Repository on your local machine that corresponds to the value of the `-oracle_home` parameter.

6. If you are prompted to select a OracleAS Metadata Repository, select the OracleAS Metadata Repository you want to upgrade.

   MRUA starts the upgrade process. As each step in the upgrade is executed, information messages appear on the screen to show the progress of the upgrade.

   Example 8–1 shows an example of a typical MRUA upgrade session.

   > **See Also:** Section 4.2.2, "Example Execution Times for the Metadata Repository Upgrade Assistant" for information on how long it takes to upgrade the OracleAS Metadata Repository schemas

7. Review the output of the MRUA command; if MRUA reports any errors, see Appendix E, "OracleAS Metadata Repository Upgrade Error Messages".

Note: In many cases, MRUA will report that the Oracle Application Server Certificate Authority (OCA) and Oracle Ultra Search component schemas have already been upgraded. This is to be expected because in some cases, the OCA schema is updated automatically by the OracleAS Identity Management and the Oracle Ultra Search schema is updated during the database upgrade.

Example 8–1 Sample Output from an MRUA Session

```
mrua.sh -oracle_home /dua1/oracle10g -oid_host dserv1.acme.com -oid_ssl_port 3130

Executing mrua.pl
Running on UNIX

OracleAS Metadata Repository Upgrade Assistant 10.1.4.0.1

Enter the password for SYS:
Enter the password for cn=orcladmin:

Upgrading the OracleAS Metadata Repository to release 10.1.4.0.1

Calling upgrade plugin for MRUA
Component upgraded successfully MRUA

Calling upgrade plugin for UDDI
Component upgraded successfully UDDI

Calling upgrade plugin for WCS
Component upgraded successfully WCS

Calling upgrade plugin for WIRELESS
Component upgraded successfully WIRELESS

Calling upgrade plugin for PORTAL
Component upgraded successfully PORTAL

Calling upgrade plugin for DISCOVERER
Component upgraded successfully DISCOVERER

Calling upgrade plugin for B2B
Component upgraded successfully B2B

Calling upgrade plugin for BAM
Component upgraded successfully BAM

Calling upgrade plugin for MRC
Component upgraded successfully MRC

SUCCESS: All OracleAS plug-ins report successful upgrade

Finished mrua.pl
```

8.3 Task 3: Verify the Success of the OracleAS Metadata Repository Upgrade

Besides the MRUA log files, you can optionally query the database to verify the success of the OracleAS Metadata Repository upgrade. You should also be aware of what component schema versions to expect in the OracleAS Metadata Repository after a successful upgrade.

For more information, refer to the following topics:

- Using SQL to Verify the Status of Each Component Schema After Running MRUA
- About Component Schema Version Numbers After Upgrading to 10g (10.1.4.0.1)

8.3.1 Using SQL to Verify the Status of Each Component Schema After Running MRUA

To use a SQL command to see the current status of each component schema in the repository that is upgraded by MRUA:

1. Connect to the OracleAS Metadata Repository database.

   For example:

   ```
   METADATA_REPOSITORY_ORACLE_HOME/bin/sqlplus "connect / as sysdba"
   ```

2. When prompted, enter the SYS password.
3. Enter the following SQL command to verify the status of the component schemas:

   ```
   SELECT comp_id,version,status FROM APP_REGISTRY;
   ```

   Refer to the following example and tables for an explanation of the output of the query:

   - Example 8–2 shows an example of the output displayed from the component schema SQL query.
   - Table 8–2 describes the possible values in the COMP_ID column of the SQL query results.
   - Table 8–3 describes the possible values in the STATUS column of the SQL query results.

Example 8–2   Sample Output of the Component Schema SQL Query

```
SQL> SELECT comp_id, version, status FROM app_registry;

COMP_ID                        VERSION                        STATUS
------------------------------ ------------------------------ -----------
WIRELESS                       10.1.2.0.2                     VALID
PORTAL                         10.1.2.0.2                     VALID
SSO                            10.1.4.0.1                     VALID
WCS                            10.1.2.0.2                     VALID
DISCOVERER                     10.1.2.0.2                     VALID
OID                            10.1.4.0.1                     VALID
MRUA                           10.1.4.0.1                     VALID
B2B                            10.1.2.0.2                     VALID
UDDI                           10.1.2.0.2                     VALID
BAM                            10.1.2.0.2                     VALID
MRC                            10.1.2.0.2                     VALID

11 rows selected.
```

Note: The versions shown in the VERSION column will vary somewhat, depending upon the starting point for the 10*g* (10.1.4.0.1) upgrade.

For more information, see Section 8.3.2, "About Component Schema Version Numbers After Upgrading to 10g (10.1.4.0.1)".

Table 8–2 Component IDs in the OracleAS Metadata Repository

Component ID	Description
WIRELESS	Oracle Application Server Wireless
PORTAL	Oracle Application Server Portal
WCS	Oracle Application Server Web Clipping
DISCOVERER	Oracle Application Server Business Intelligence Discoverer
MRUA	Oracle Application Server Metadata Repository Upgrade Assistant
B2B	Oracle Application Server Integration B2B
UDDI	Oracle Application Server UDDI Registry
MRC	Oracle Application Server Metadata Repository Container
BAM	Oracle BPEL Process Analytics

Table 8–3 Component Status Indicators in the OracleAS Metadata Repository

Status	Description
LOADING	MRUA has begun creating the component database objects, but not all the component objects are created and loaded into the database.
LOADED	MRUA has created all the component database objects and loaded them into the database. MRUA can now begin upgrading the component schemas.
UPGRADING	MRUA has begun upgrading the schemas for this component, but the upgrade is not complete.
UPGRADED	MRUA has finished upgrading the schemas for this component.
VALID	The component schemas have been upgraded and are valid. This is the expected status after a successful upgrade to Oracle Application Server 10*g* (10.1.4.0.1).
INVALID	The component schemas have been upgraded, but the database component schemas are invalid. This state can be caused by a non-recoverable error or invalid data. See Appendix E, "OracleAS Metadata Repository Upgrade Error Messages" for information.

8.3.2 About Component Schema Version Numbers After Upgrading to 10*g* (10.1.4.0.1)

The OracleAS Metadata Repository contains schemas for all the Oracle Application Server components. However, depending upon the starting point for your upgrade, only a subset of those component schemas must be updated by MRUA for Oracle Identity Management 10*g* (10.1.4.0.1).

Other schemas, such as the OracleAS Identity Management schemas, are upgraded during the OracleAS Identity Management upgrade procedure in Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management". Still others do not require any upgrade from previous versions, depending upon your upgrade starting point.

As a result, even after running MRUA, some schemas in the OracleAS Metadata Repository remain at 10.1.2.0.2 and others are upgraded to 10.1.4.0.0.

For example, if you previously upgraded your 10*g* Release 2 (10.1.2) environment to OracleAS Portal 10*g* Release 2 (10.1.4), then the PORTAL schema will already be listed as 10.1.4.0.0.

On the other hand, if you have not previously upgraded to OracleAS Portal 10*g* Release 2 (10.1.4), the PORTAL schema will remain at 10*g* Release 2 (10.1.2.0.2), unless you later upgrade to OracleAS Portal 10*g* Release 2 (10.1.4).

9 Component-Specific Post-Upgrade Procedures

This chapter details the component-specific post-upgrade procedures, which will complete the Infrastructure upgrade to 10*g* (10.1.4.0.1). It is organized into these sections:

- Task 1: Enable OracleAS SSL Support (SSL) for OracleAS Identity Management Components
- Task 2: Perform Oracle Internet Directory Post-Upgrade Steps
- Task 3: Perform OracleAS Single Sign-On Post-Upgrade Steps
- Task 4: Perform OracleAS Portal Post-Upgrade Steps
- Task 5: Perform OracleAS Wireless Post-Upgrade Steps

9.1 Task 1: Enable OracleAS SSL Support (SSL) for OracleAS Identity Management Components

If you are upgrading distributed OracleAS Identity Management components that were configured to use SSL, you must re-enable SSL for the OracleAS Single Sign-On and Oracle Delegated Administration Services after the upgrade. For more information, see the following sections:

- Enabling SSL for Oracle Internet Directory After Upgrade
- Enabling SSL for OracleAS Single Sign-On After Upgrade
- Enabling SSL for Oracle Delegated Administration Services After Upgrade

9.1.1 Enabling SSL for Oracle Internet Directory After Upgrade

There is no need to enable SSL for Oracle Internet Directory, since the upgrade procedure automatically re-enables SSL for Oracle Internet Directory in the destination Oracle home if you were using SSL with Oracle Internet Directory in the source Oracle home.

9.1.2 Enabling SSL for OracleAS Single Sign-On After Upgrade

To enable SSL for OracleAS Single Sign-On, use the procedure described in the section "Enabling SSL" chapter of the *Oracle Application Server Single Sign-On Administrator's Guide*.

In particular, you must perform the following steps as described in that section of the *Oracle Application Server Single Sign-On Administrator's Guide*:

1. Enable SSL on the Single Sign-On middle tier, which involves editing the `opmn.xml` configuration file to enable SSL.
2. Change Single Sign-On URLs by running the `ssocfg` utility.
3. Update `targets.xml` and configure Oracle Enterprise Manager Application Server Control to recognize the SSL certificate.

   For more detailed information about this step in the SSL configuration process, see Section 9.1.2.1, "Enabling Monitoring of OracleAS Single Sign-On and Oracle Delegated Administration Services in Application Server Control".
4. Protect Single Sign-On URLs.
5. Restart the Oracle HTTP Server and the Single Sign-On Middle Tier (the OC4J_Security OC4J instance).
6. Register `mod_osso` with the SSL virtual host as documented in the section "Configuring mod_osso with Virtual Hosts" in the *Oracle Application Server Single Sign-On Administrator's Guide*.

9.1.2.1 Enabling Monitoring of OracleAS Single Sign-On and Oracle Delegated Administration Services in Application Server Control

To be sure that Application Server Control can monitor the OracleAS Single Sign-On and Oracle Delegated Administration Services components over SSL, refer to the following sections:

- Updating targets.xml with the Correct Protocols and URLs
- Configuring Application Server Control to Recognize the SSL Certificate

9.1.2.1.1 Updating targets.xml with the Correct Protocols and URLs Modify the `targets.xml` Application Server Control configuration file to be sure that Application Server Control can connect to the required OracleAS Single Sign-On and Oracle Delegated Administration Services URLs:

1. Locate and open the `targets.xml` file with a text editor.

   The file is located in the destination Oracle home:

   ```
   DESTINATION_ORACLE_HOME/sysman/emd/
   ```

2. In the `targets.xml` file, locate the Oracle Delegated Administration Services element:

   ```
   <Target TYPE="oracle_das_server" ... >
      ....
   </Target>
   ```

3. Within the `oracle_das_server` element, update the properties shown in Table 9–1 with the recommended values shown for each property.

Table 9–1 OracleAS Single Sign-On and Oracle Delegated Administration Services Properties to Modify in the targets.xml Configuration File

Property	Description and Required Value
HTTPProtocol	The protocol used by the Oracle HTTP Server. The value can be either HTTP or HTTPS (for secure SSL connections).
MonitorPort	The physical port used to monitor the Oracle Delegated Administration Services on the host. This is often the default Oracle HTTP Server port.

Table 9–1 (Cont.) OracleAS Single Sign-On and Oracle Delegated Administration Services Properties to Modify in the targets.xml Configuration File

Property	Description and Required Value
DasPort	The physical port used to monitor Oracle Delegated Administration Services on the host. This is often the default Oracle HTTP Server port.
DasURL	The complete Oracle Delegated Administration Services URL, including the protocol, physical host name, and port. In high availability environments, do not use the load balancer virtual host and port.
DasMonitorURL	The complete URL used by Application Server Control to monitor the Oracle Delegated Administration Services, including the protocol, physical host name, and port. In high availability environments, do not use the load balancer virtual host and port.

4. Locate the OracleAS Single Sign-On element within the targets.xml file:

```
<Target TYPE="oracle_sso_server" ... >
   ....
</Target>
```

5. Edit the values for the `HTTPPort` and `HTTPProtocol` properties within the `oracle_sso_server` element.

   Be sure to enter the port and protocol for the physical OracleAS Single Sign-On host; do not use the port and protocol used to connect to the load balancer.

6. Save your changes and close the `targets.xml` file.

9.1.2.1.2 Configuring Application Server Control to Recognize the SSL Certificate To be sure Application Server Control can monitor OracleAS Single Sign-On and Oracle Delegated Administration Services over the SSL connection, verify that Application Server Control has access to the proper security certificate.

If you do not perform this step, Application Server Control will indicate that OracleAS Single Sign-On and Oracle Delegated Administration Services are down or unavailable even though it is up and running.

To correct this problem you must allow the Application Server Control to recognize the Certificate Authority that was used 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 `sso_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 9–1.

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 `sso_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:

   ```
   DESTINATION_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/sso_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------
```

9.1.3 Enabling SSL for Oracle Delegated Administration Services After Upgrade

If you have also configured Oracle Delegated Administration Services in the upgraded Oracle home, you must reconfigure the Oracle Delegated Administration Services URL.

To reconfigure the Oracle Delegated Administration Services URL:

1. Start Oracle Directory Manager (`oidadmin)` and connect to the Oracle Internet Directory.

   The `oidadmin` tool is located in the following directory in the destination Oracle home:

   ```
   DESTINATION_ORACLE_HOME/bin/
   ```

   If you are connecting to the directory over SSL, make sure you select the **SSL Enabled** check box when connecting to the directory server.

2. In the System Objects Navigator, navigate to the `cn=OperationURLs` entry as follows:

   ```
   Entry Management ->
     cn=OracleContext ->
        cn=Products ->
           cn=DAS ->
              cn=OperationURLs
   ```

3. After you select the `cn=OperationURLs` entry, locate the orcldasurl attribute on the Properties tab in the right pane of the Oracle Directory Manager window.

4. Change the `orcldasurlbase` attribute so it references the SSL URL for the Oracle Delegated Administration Services:

   ```
   https://virtual_server_name:load_balancer_ssl_listen_port
   ```

> **See Also:** "Using Oracle Directory Manager" in the *Oracle Internet Directory Administrator's Guide*

9.2 Task 2: Perform Oracle Internet Directory Post-Upgrade Steps

To complete the Oracle Internet Directory Upgrade, you must perform the following tasks:

- Running the Certificate Upgrade Tool (upgradecert.pl)
- Modifying Access Policies After Oracle Internet Directory Upgrade
- Resetting the Replication Wallet Password
- Completing the Upgrade for the Oracle Directory Integration Platform
- Running the oidstats.sql Script After Upgrading Oracle Internet Directory from 10g (9.0.4)
- Modifying DSA Configuration Entries After Upgrade
- Recreating Oracle Internet Directory Indexes After Upgrade
- About the New Account Used for Accessing Server Manageability Information

9.2.1 Running the Certificate Upgrade Tool (upgradecert.pl)

Starting with release 10.1.2, a certificate hash value can be used to bind to Oracle Internet Directory. The introduction of this hash value requires that user certificates issued before release 10.1.2 be updated in the directory.

As a result, if you are upgrading from a release prior to 10*g* Release 2 (10.1.2), and if you if user certificates are provisioned in the directory, you must perform this additional post-upgrade step.

Note that this step is not required if you are upgrading from Oracle Internet Directory 10*g* Release 2 (10.1.2).

Complete instructions for running the Certificate Upgrade Tool (`upgradecert.pl`) to perform this task are available in Appendix A, "Syntax for LDIF and Command-Line Tools," in the *Oracle Internet Directory Administrator's Guide*.

9.2.2 Modifying Access Policies After Oracle Internet Directory Upgrade

During the Oracle Internet Directory upgrade, LDAP objects within the directory are modified or added to the Oracle Internet Directory. These updates often include access control information.

In a production environment, customized access control policies are often enforced in the directory. For this reason, the upgrade process leaves certain entries in the directory untouched intentionally to retain any customized behavior you may have implemented in the directory.

Further, in some cases, the default, out-of-the-box access control settings are required for Oracle components to function properly. As a result, after the Oracle Internet Directory upgrade, you should analyze the differences between the default, out-of-the-box access control policies and any custom policies you have implemented. The result of this task should be a new set of customized access control policies that will meet the requirements of Oracle components, as well as the access control polices of your organization.

Even if you have not implemented any customized access control polices, Oracle strongly recommends that you manually update the ACLs with the new default values after an upgrade.

The following example uses "dc=acme, dc=com" as a default realm DN. In this example, consider the following when analyzing the ACL policy for your directory:

- Realm DN (eg. dc=acme, dc=com)
- Parent of the Realm DN. This is also known as the Realm Search Base, for example, "dc=com".
- Realm User container. This is also known as the Realm User Search Base, for example, "cn=Users, dc=acme, dc=com". Depending on the deployment requirement, this can be customized.
- Realm Group container. This is also known as the Realm Group Search Base, for example, "cn=Groups, dc=acme, dc=com". Depending on the deployment requirement, this can be customized.

The out-of-the-box access control policies is available in the following files:

- Policies for the Parent of Realm DN can be found in the following file:

  ```
  $ORACLE_HOME/ldap/schema/oid/oidDefaultSubscriberConfig.sbs
  ```

- Policies for the Realm DN, Realm User container, and Realm Group container can be found in:

  ```
  $ORACLE_HOME/ldap/schema/oid/oidSubscriberCreateAuxDIT.sbs
  ```

The default ACL policy is described in the *Oracle Internet Directory Administrator's Guide*, in Chapter 17, in the section on "Default Privileges for Reading Common Group Attributes".

9.2.3 Resetting the Replication Wallet Password

If you upgrade a 9.0.x node to 10*g* (10.1.4.0.1) and then try to set up replication for this node, the replication server will fail to come up and the replication setup itself may fail. For information on changing and resetting the replication wallet password, see Section A.4.1, "Changing the Replication DN Password in the Oracle Internet Directory Wallet for Each Replica".

9.2.4 Completing the Upgrade for the Oracle Directory Integration Platform

If you had an older version (9.0.2 or 9.0.4) of the Directory Integration Platform operating in a different Oracle home, on a different computer, and using the Oracle Internet Directory you are currently upgrading, and you want to continue using the Oracle Directory Integration Platform, you must re-register the Oracle Directory Integration Platform server.

> **See Also:** *Oracle Identity Management Integration Guide* for instructions on registering the DIP server.

9.2.5 Running the oidstats.sql Script After Upgrading Oracle Internet Directory from 10*g* (9.0.4)

After you upgrade Oracle Internet Directory from 10*g* (9.0.4) to 10*g* (10.1.4.0.1), you could observe some degradation in the performance of some LDAP queries.

To remedy this issue, perform the following procedure, which updates some database statistics in the Oracle Database 10*g* database that hosts the Oracle Internet Directory server:

1. In the newly upgraded Oracle Internet Directory Oracle home, execute the following SQL script by connecting to the OID database as the ODS database user:

   ```
   sqlplus ods/<passwd> @$ORACLE_HOME/ldap/admin/oidstats.sql
   ```

2. Restart the Oracle Internet Directory server as follows:

   a. Run the following command to stop the Oracle Internet Directory server:

   ```
   opmnctl stopproc ias-component=OID
   ```

   b. Wait a few seconds for the Oracle Internet Directory server to shut down completely.

   c. Run the following command to start the Oracle Internet Directory server:

   ```
   opmnctl startproc ias-component=OID
   ```

Similarly, if you are running in an environment where the database that hosts the Oracle Internet Directory is upgraded before you upgrade the Oracle Internet Directory, you should gather the database statistics immediately after the database upgrade by running the following SQL command on the database:

```
exec dbms_stats.gather_schema_stats('ODS');
```

9.2.6 Modifying DSA Configuration Entries After Upgrade

When you upgrade Oracle Internet Directory from 10*g* (9.0.4) to 10*g* (10.1.4.0.1), all attributes in the DSA Configuration entry are reset to their default values. For example:

```
cn=dsaconfig,cn=configsets,cn=oracle internet directory
```

As a result, if any attributes in this entry were modified before the upgrade, you must reconfigure them to their values before the upgrade.

9.2.7 Recreating Oracle Internet Directory Indexes After Upgrade

When you upgrade Oracle Internet Directory from 10*g* (9.0.4) to 10*g* (10.1.4.0.1), some indexes are recreated automatically by the upgrade procedure. For example, the `EI_attrstore` index is recreated automatically during the upgrade.

As a result, if you recreated the `EI_attrstore` index before the upgrade, then the index will have to be recreated again after the upgrade. Note that recreating the `EI_attrstore` index is part of the performance recommendation for large group entry lookups described in section "21.8.1 Optimizing Searches for Large Group Entries" of the *Oracle Internet Directory Administrator's Guide*. If you performed this procedure prior to the upgrade to 10*g* (10.1.4.0.1), you will need to perform this task again after the upgrade.

9.2.8 About the New Account Used for Accessing Server Manageability Information

The Oracle Internet Directory database account ODSSM is used to access server manageability information from the database. During upgrade to 10*g* (10.1.4.0.1), this account is created and given a randomly-generated password.

The credentials for this account, including the randomized password are stored in the Oracle Internet Directory snippet in the Enterprise Manager file `targets.xml`.

The only way you can change this account's password is to use SQLPLUS. There is no support in the `oidpasswd` tool for changing this password. Also, its password is not stored in a wallet. After altering this password in the database, you must also change it in the file `targets.xml`. You do this either by setting the new values in the user and password fields or by running the tool `oidemdpasswd`.

9.3 Task 3: Perform OracleAS Single Sign-On Post-Upgrade Steps

To complete the OracleAS Single Sign-On upgrade, depending on the configuration upgraded, you may need to perform the tasks described in the following sections:

- Re-configuring the OracleAS Single Sign-On Middle Tier
- Configuring Third-party Authentication
- Installing Customized Pages in the Upgraded Server
- Setting Up OracleAS Single Sign-On Replication
- Upgrading the OracleAS Single Sign-On Server with a Customized Middle Tier
- Troubleshooting Wireless Voice Authentication
- Installing Languages in the OracleAS Single Sign-On Server

- Removing Obsolete OracleAS Single Sign-On Partner Applications

9.3.1 Re-configuring the OracleAS Single Sign-On Middle Tier

If the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) middle tier for the Single Sign-On server had custom configurations (for example, Oracle HTTP Server configured for SSL, or the Oracle Application Server Single Sign-On server Database Access Descriptor had any custom configuration), then you must re-configure the upgraded 10*g* (10.1.4.0.1) middle tier in a like manner.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide* for instructions on configuring the middle tier.

If you are using OracleAS Portal and you reconfigure the 10*g* Release 2 (10.1.2) middle tier for SSL, the URL used for Oracle Delegated Administration Services might not be up-to-date. To remedy this problem, force a refresh of the portal cache, which holds the relevant Oracle Internet Directory information:

1. Logon to OracleAS Portal as a user with administrator privileges.
2. Go to the Builder.
3. Click the **Administration** tab.
4. From the Portal tab, open Global Settings and navigate to the SSO/OID tab.
5. Scroll to the bottom of the page.
6. Check **Refresh Cache** for the Oracle Internet Directory parameters.
7. Click **Apply**.

   The page should refresh with the appropriate value in the DAS Host Name field.

> **See Also:** *Oracle Application Server Portal Configuration Guide*

9.3.2 Configuring Third-party Authentication

If the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) middle tier was configured to authenticate with a user certificate or third party authentication mechanism, then you must re-configure the 10*g* (10.1.4.0.1) OracleAS Single Sign-On server in a like manner.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide*, Chapter 13, for instructions on configuring the middle tier.

9.3.3 Installing Customized Pages in the Upgraded Server

If you have customized the login, password and the sign-off pages in the 10g (9.0.4) or 10*g* Release 2 (10.1.2) Single Sign-On server, then you must update those pages with 10*g* (10.1.4.0.1) specifications. This is also applicable if you have enabled support for Application Service Providers and updated the deployment login page to enable the company field.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide*, Chapter 12, for instructions on configuring the middle tier.

9.3.4 Setting Up OracleAS Single Sign-On Replication

If you are using Oracle Internet Directory replication and want to also use OracleAS Single Sign-On replication, add the upgraded 10*g* (10.1.4.0.1) tables in the replication group along with 9.0.4 Oracle Internet Directory. Follow the steps below to add OracleAS Single Sign-On tables for replication:

1. Stop the Oracle Internet Directory replication server on all replicas of the Directory Replication Group.
2. On the Master Directory replica, in `$ORACLE_HOME/ldap/admin`, issue the following command:

   ```
   sqlplus repadmin/password@<mds connect id> @oidrssou.sql
   ```

3. Start the Oracle Internet Directory replication server on all replicas of the Directory Replication Group.

   See Also: Oracle Internet Directory Administrator's Guide, Chapter 25, "Managing Directory Replication", for instructions.

9.3.5 Upgrading the OracleAS Single Sign-On Server with a Customized Middle Tier

If the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Single Sign-On server was using a middle tier other than the default mid-tier installation along with the OracleAS Single Sign-On server, then you must configure that middle tier to point to the upgraded OracleAS Single Sign-On server.

For example, if there was a reverse proxy configured in the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Single Sign-On server middle tier, then you must configure it on the 10*g* (10.1.4.0.1) OracleAS Single Sign-On server middle tier.

9.3.6 Troubleshooting Wireless Voice Authentication

If you want to use wireless voice authentication with the 10*g* (10.1.4.0.1) OracleAS Single Sign-On server, and it doesn't work, verify that the OracleAS Single Sign-On server entry is a member of the Verifier Services Group in Oracle Internet Directory (`cn=verifierServices,cn=Groups,cn=OracleContext`). This is a requirement for the wireless voice authentication feature. Follow the steps below to verify membership:

1. Issue the following command:

   ```
   ldapsearch -h host
       -p port
       -D "cn=orcladmin"
       -w password
       -b "cn=verifierServices, cn=Groups, cn=OracleContext" "objectclass=*"
   ```

   The OracleAS Single Sign-On server is a member of the Verifier Services Group if it is listed as a `uniquemember` in the entry, as shown in Example 9–2.

Example 9–2 OracleAS Single Sign-On Server uniquemember Listing

```
cn=verifierServices, cn=Groups,cn=OracleContext
.
.
.
uniquemember=orclApplication
CommonName=ORASSO_SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
.
.
.
```

9.3.7 Installing Languages in the OracleAS Single Sign-On Server

If you did not select any languages during the OracleAS Single Sign-On upgrade, or you want to install additional languages after the upgrade, you can install the necessary languages by following the steps below.

1. Copy the necessary language files from the Repository Creation Assistant CD-ROM to the OracleAS Single Sign-On server Oracle home:

   ```
   copy repCA_CD/portal/admin/plsql/nlsres/ctl/lang\*.* DESTINATION_ORACLE_
   HOME/sso/nlsres/ctl/lang
   ```

   In this example, `lang` is the language code. For example, the language code for Japanese is `ja`.

2. Load the languages into the server.

   > **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide*, Chapter 2, "Configuring Globalization Support" section, for instructions on loading the languages.

9.3.8 Removing Obsolete OracleAS Single Sign-On Partner Applications

After the upgrade, you will notice additional and obsolete partner applications on the OracleAS Single Sign-On Partner Application administration page.

For example, you will notice two Oracle Application Server Certificate Authority (OCA) partner applications and two OracleAS Wireless partner applications.

You can safely remove the 10*g* (9.0.4) OCA partner application that uses port 4400.

> **See Also:** Section 10.2, "Task 2: Decommission the OracleAS Identity Management Source Oracle Home" for specific instructions about removing source components from the list of partner applications

As for the OracleAS Wireless partner applications, the 10*g* Release 2 (10.1.2) Oracle HTTP Server configuration is changed after during the upgrade to use the 10*g* (9.0.4) HTTP Server port; this partner application is not valid and can be removed. The valid OracleAS Wirelesspartner application is the upgraded partner application, which existed in the 10*g* (9.0.4) environment.

Review the list of partner applications for any other obsolete or already upgraded components or applications.

> **See Also:** Section 10.2, "Task 2: Decommission the OracleAS Identity Management Source Oracle Home" for information about removing the partner applications that represent the OracleAS Identity Management installations you have upgraded

9.4 Task 4: Perform OracleAS Portal Post-Upgrade Steps

The following sections describe how to complete the upgrade of the OracleAS Portal schema.

Note: The procedures described in this section must be performed only if you run the 10*g* (10.1.4.0.1) Metadata Repository Upgrade Assistant (MRUA) and MRUA reports that the PORTAL schema was upgraded to 10*g* Release 2 (10.1.2.0.2).

If the MRUA output indicates that the PORTAL schema was already upgraded, then there is no need to perform the steps listed in this section.

- Moving the Portlet Repository to the New Format (Optional)
- Starting all Middle Tiers That Use The Upgraded Portal Instance
- Accessing the Upgraded OracleAS Portal
- Impact of Shutting Down the OracleAS Metadata Repository Database on OracleAS Portal Oracle Text Indexes
- Reconfiguring OracleAS Portal to Work with Delegated Administration Services
- Updating OracleAS Portal Performance Reporting

9.4.1 Starting all Middle Tiers That Use The Upgraded Portal Instance

After the script has executed successfully, start each middle tier that is using the upgraded Portal instance by performing these steps:

1. Start OPMN and processes managed by it with this command:

```
MIDDLE_TIER_ORACLE_HOME/opmn/bin/opmnctl startall
```

2. Start the Application Server Control using the following command:

```
MIDDLE_TIER_ORACLE_HOME/bin/emctl start iasconsole
```

9.4.2 Moving the Portlet Repository to the New Format (Optional)

By default, the portlet repository is upgraded in-place in the OracleAS Portal schema. The existing pages, templates, items, and so on, in the portlet repository are upgraded, and the new portlets are added into the repository. Since the old settings are preserved, the pages look very similar to the way they did before the upgrade was run.

Note: If your starting version is Oracle9*i*AS Portal 9.0.2 and you had rendered the Portlet Repository as grouped by Provider names, then after the upgrade, the folders in the repository will be grouped by category, because the Group by Provider Name option has been deprecated since OracleAS 10g (9.0.4).

To create a similar organization, assign the portlet names to categories representing the Provider names.

If you want the repository to have the appearance of a newly installed instance, a script is available to re-create the upgraded portlet repository. The script removes the existing portlet repository and re-creates it. Use the script only if you do not wish to preserve customizations, settings, styles, banners, and so on in the portlet repository.

To re-create the portlet repository, follow these steps after starting the middle tiers as described in Section 9.4.1, "Starting all Middle Tiers That Use The Upgraded Portal Instance":

1. Perform a backup of the database, since the script overwrites the repository and is not reversible.
2. Navigate to the following directory on the OracleAS Metadata Repository Upgrade Assistant and Utilities CD–ROM, which contains the `prrplc.sql` script:

   ```
   MRUA_CDROM_ROOT/portal/admin/plsql/upg/common
   ```

3. Log in to the OracleAS Metadata Repository database as Portal schema user from SQL*Plus.
4. Run the `prrplc.sql` script with no arguments.

9.4.3 Accessing the Upgraded OracleAS Portal

If there were no errors in the OracleAS Portal Repository upgrade, you can access your upgraded Portal. Open a browser and navigate to the following URL:

```
http://host.domain:port/pls/portal_DAD
```

For example:

```
http://portalhost42.acme.com:7777/pls/portal
```

9.4.4 Impact of Shutting Down the OracleAS Metadata Repository Database on OracleAS Portal Oracle Text Indexes

Missing Oracle Text indexes are created during the OracleAS Portal upgrade process, but they are not populated, as this can be very time consuming. The new indexes are populated once the upgrade is complete, when the next synchronization job is scheduled.

If you need to shut down the database after the upgrade (to back up) and the Oracle Text index synchronization job has started, consider the impact of the following shutdown commands on the synchronization process:

- Shutdown Immediate or Abort

  The indexing job stops immediately and is rolled back.

- Shutdown Normal

  Entire indexing job finishes before the database shuts down.

- Shutdown Transactional

  Synchronization of the current index is allowed to finish before the database shuts down. If one or more indexes still need to be synchronized, synchronization of the next index is not started.

9.4.5 Reconfiguring OracleAS Portal to Work with Delegated Administration Services

In releases of OracleAS Portal prior to 10*g* Release 2 (10.1.2), if the Infrastructure and Application Server middle tier were separated onto different hosts or protocols, the user and group Lists of Values (LOVs) required configuration to accommodate the JavaScript Origin Server Security policy. The resultant JavaScript errors were due to the OracleAS Portal and Delegated Administration Services (DAS) residing in different domains.

There were two options provided for resolution of this issue:

- Setting up of a common-domain by running the script secjsdom.sql
- Deploying DAS on the middle tier.

In OracleAS Portal 10*g* Release 2 (10.1.2), the implementation of the LOVs has been modified to support a callback method, removing the cross-domain issue and the need for the configuration steps above. However, this callback mechanism requires a corresponding patch to the DAS environment to support the use of LOVs across domains.

Support for the callback method has been included in DAS versions 9.0.4.1 and later. Conversely, if you are using DAS version 9.0.2.3 you can apply patch 3278638 to enable callback support.

If you have installed the appropriate DAS version in your environment, and have not previously implemented the configuration options mentioned above, then no subsequent configuration steps are required in OracleAS Portal to support the LOVs on a separate host. However, if you used the configuration options mentioned above, it is required to remove these steps. This can be done as follows:

1. If a common domain was defined, reset it by executing the secjsdom.sql script as follows:

   a. From your operating system command prompt, go to the following directory:

   ```
   DESTINATION_MIDTIER_ORACLE_HOME/portal/admin/plsql/wwc
   ```

   b. Using SQL*Plus, connect to the OracleAS Portal Repository as the schema owner and run the following commands:

   ```
   @secjsdom ''
   commit;
   ```

2. If OracleAS Portal has been configured to use a locally deployed DAS servlet, reconfigure it to point to the Infrastructure tier by running the secdaslc.sql script as follows:

   a. From the operating system prompt, go to the following directory:

   ```
   DESTINATION_MIDTIER_ORACLE_HOME/portal/admin/plsql/wwc
   ```

   b. Using SQL*Plus, connect to the OracleAS Portal Repository as the schema owner and run the following commands:

   ```
   @secdaslc N
   commit;
   ```

9.4.6 Updating Customized Login Portlets

If you have customized the login portlet, you must update it to work in this release. In prior releases, user credentials were posted to OracleAS Portal's `wwptl_login.login_url` procedure. In this release, the user credentials must be passed to OracleAS Single Sign-On's `wwsso_app_admin.ls_login` procedure instead. Follow the steps outlined in Oracle*MetaLink* note `290445.1` to update your customized login portlet to use `wwsso_app_admin.ls_login`.

Note: You do not have to perform any additional steps at this time if you followed the instructions provided in the patch documentation after applying Oracle Application Server 10g (9.0.4) Patch Set 1 (9.0.4.1), or any of the following one-off patches:

- 3273358 (Release 9.0.4)
- 3273354 (Release 9.0.2.6)
- 3273342 (Release 9.0.2.3)

9.4.7 Updating OracleAS Portal Performance Reporting

To generate performance reports for OracleAS Portal, you must use a set of SQL scripts. These scripts are used to load OracleAS Portal log files into a database table and create reports based on that information. The scripts are located in the following directory:

```
ORACLE_HOME/portal/admin/plsql/perf
```

If you are already using the performance reporting scripts, then after upgrading to OracleAS Portal 10.1.2.0.2, you must run the new copy of the following file:

```
ORACLE_HOME/portal/admin/plsql/perf/install/update.sql
```

This is to accommodate the new URL format for Repository requests and to enable collection of new data. If this is not done, then the scripts will not work.

For details about how you can use the scripts to monitor OracleAS Portal performance, refer to the following file in the scripts subdirectory:

```
ORACLE_HOME/portal/admin/plsql/perf/scripts/README.html
```

9.5 Task 5: Perform OracleAS Wireless Post-Upgrade Steps

The following sections describe the tasks you must perform in order to complete the Oracle Application Server Wireless upgrade:

- Adding Unique Constraint on the orclWirelessAccountNumber Attribute in Oracle Internet Directory
- Assigning Change Password Privilege to OracleAS Wireless
- Specifying URL Query Parameters for Wireless Services That Use the HTTP Adapter

9.5.1 Adding Unique Constraint on the orclWirelessAccountNumber Attribute in Oracle Internet Directory

In 10*g* (10.1.4.0.1), Oracle Internet Directory does not automatically set unique constraints on any user attributes. Wireless voice authentication will not function properly unless a unique constraint is set on the `orclWirelessAccountNumber` attribute of the `orclUserV2` object class.

Set the unique constraint by performing the steps below after the middle tier and infrastructure upgrades are complete.

1. Execute the script `addAccountNumberUniqueConstraint.sh`, which is located in the following directory:

```
DESTINATION_ORACLE_HOME/wireless/bin
```

The script takes one argument, the full path to the Oracle home. For example:

```
addAccountNumberUniqueConstraint.sh DESTINATION_ORACLE_HOME
```

2. Restart the Oracle Internet Directory server.

9.5.2 Assigning Change Password Privilege to OracleAS Wireless

In Oracle Application Server 10*g* (10.1.4.0.1), by default, the OracleAS Wireless application entity does not have the privileges to change the user password. Consequently, upon installation, users cannot change the password to the OracleAS Wireless server. However, you can enable functionality to change passwords by assigning the `UserSecurityAdmins` privilege to the OracleAS Wireless application entity.

To do this, execute the following script:

```
DESTINATION_ORACLE_HOME/wireless/bin/assignUserSecurityAdminsPrivilege.sh
```

The syntax is:

```
assignUserSecurityAdminsPrivilege.sh oid_super_user_dn user_password
```

In this example:

- *oid_super user_dn* is the Distinguished Name of the Oracle Internet Directory super user. This user should have privileges to grant UserSecurityAdmins privileges to application entities.
- *user_password* is the password of the Oracle Internet Directory super user.

For example:

```
assignUserSecurityAdminsPrivilege.sh "cn=orcladmin" welcome1
```

See Also: "Resetting the Password" in *Oracle Application Server Wireless Administrator's Guide*

9.5.3 Specifying URL Query Parameters for Wireless Services That Use the HTTP Adapter

When you use the HTTP adapter to build Wireless services, one of the service parameters that you must specify is the URL to a back-end application. In some cases, you may send some query parameters to the back-end application. There are two ways to do this from OracleAS Wireless, shown in Example 9–3 and Example 9–4. In Example 9–3, the parameter name is `fn` and the value is `Joe`.

Example 9–3 URL Using a Query Parameter

```
http://localhost:7777/myapp/home.jsp?fn=Joe
```

The query parameter is sent only in the request for the first page of that service. If there is a link from the first page to some other pages, then the parameter is not added to the request for those pages.

Example 9–4 URL Using an Extra Service Parameter

```
http://localhost:7777/myapp/home.jsp
```

Instead of modifying the URL, you add an extra service parameter with name `fn` and value `Joe`. The the parameter is sent to all pages, not just the first one. The parameter is also sent with all HTTP redirect requests. However, this method also sends extra URL parameters to the OracleAS Single Sign-On server, which causes the server to return an error.

The error occurs when the back-end application is protected by mod_osso. In that case, the request to that application is intercepted and redirected to the Oracle SSO server for user authentication. The OracleAS Single Sign-On server has restrictive rules concerning query parameters that can be sent to it. Consequently, for back-end applications protected by mod_osso, you must change the Wireless service and add the query parameter to the URL as shown in Example 9–3.

10

Verifying the Upgrade and Decommissioning the Source Oracle Homes

Use this chapter to verify that the upgrade to Oracle Identity Management 10*g* (10.1.4.0.1) was successful and to decommission the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) Oracle Identity Management Oracle home.

This chapter contains the following sections:

- Task 1: Verify the Oracle Identity Management Upgrade
- Task 2: Decommission the OracleAS Identity Management Source Oracle Home

10.1 Task 1: Verify the Oracle Identity Management Upgrade

Use the following procedure to verify that the upgrade was successful.

Step 1 Verify the Application Server Control Console Port

Verify that you can access the Application Server Control Console by entering the Application Server Control URL in your Web browser. Use the port number assigned during the 10*g* (10.1.4.0.1) installation.

Note: You can locate the URL for the 10*g* (10.1.4.0.1) Application Server Control Console by checking the contents of the following file in the 10*g* (10.1.4.0.1) Oracle home:

```
DESTINATION_ORACLE_HOME/install/readme.txt
```

Step 2 Verify the Administration Passwords

After you upgrade your Oracle Application Server instance, use the following passwords in the destination Oracle home:

- To log in to the Application Server Control Console, use the `ias_admin` password you defined during the installation of the destination Oracle home.
- To log in to the OracleAS Web Cache Manager, use the OracleAS Web Cache `Administrator` password you used in the OracleAS Web Cache source Oracle home.

Step 3 Test OracleAS Single Sign-On Connectivity

After the Identity Management upgrade is complete, log in to Oracle Application Server Single Sign-On as user ORCLADMIN. A successful login indicates that Oracle

Application Server Single Sign-On and Oracle Internet Directory are functioning after the Identity Management upgrade.

1. In a browser, access the Oracle Enterprise Manager 10*g* Application Server Control Console in the destination Infrastructure Oracle home by entering its URL. Ensure that you provide the correct host name and port number. For example:

   ```
   http://infrahost.mycompany.com:1812
   ```

   Oracle Enterprise Manager 10*g* displays the Farm page, with the Oracle Application Server 10*g* (10.1.4.0.1) Identity Management instance in the **Standalone Instances** section.

2. Click the link for the Identity Management instance.

   The **System Components** page appears.

3. Verify that the status of the Oracle HTTP Server, Oracle Internet Directory, and Oracle Application Server Single Sign-On components is **Up**.

4. In the browser, access the ORASSO page by entering its URL. Ensure that you enter the correct host name and port number for the upgraded Oracle HTTP Server. For example:

   ```
   http://infrahost.mycompany.com:7777/pls/orasso/ORASSO.home
   ```

   The ORASSO page appears.

5. Click the **Login** link (in the upper right corner of the page).

   A page appears with **User Name** and **Password** fields.

6. Enter ORCLADMIN in the User Name field, and the password you have selected for ORCLADMIN in the Password field.

7. Click **Login**.

   The Oracle Application Server Single Sign-On Server **Administration** page appears, thus validating the basic operation of the upgraded Identity Management components (Oracle Application Server Single Sign-On and Oracle Internet Directory).

Step 4 Test Oracle Application Server Certificate Authority

If you have upgraded Oracle Application Server Certificate Authority (OCA), you can verify that the upgrade completed successfully by accessing the OCA User page.

Open your Web browser and enter the following URL:

```
https://infrahost.mycompany.com:6600/oca/user
```

Check to be sure that you can log in as a regular user and view the user's existing certificates. This ensures that OCA is working with Oracle Internet Directory and OracleAS Single Sign-On.

Note: After the upgrade, you will notice two OCA partner applications in the OracleAS Single Sign-On Partner Application administration page. One is the partner application for the 10*g* (9.0.4) OCA installation and the other is the partner application for the upgraded 10*g* (10.1.4.0.1) OCA installation.

The original partner application can be removed. The upgraded OCA will be running on port 6600 after upgrade, instead of port 4400.

10.2 Task 2: Decommission the OracleAS Identity Management Source Oracle Home

After you upgrade your OracleAS Identity Management Oracle home, the source Oracle home can eventually be deinstalled. However, before you deinstall the source Oracle home, be sure to perform the following steps.

Step 1 If Necessary, Relocate the Database Datafiles, Control Files, and Log Files

If you upgraded OracleAS Identity Management as part of a colocated Infrastructure, then you also upgraded the OracleAS Metadata Repository database to a supported database version.

After you upgrade the OracleAS Metadata Repository database using the OracleAS Upgrade Assistant, the datafiles, control files, and log files for the database remain in the source Oracle home. Before you deinstall or remove the Oracle home, you must first relocate the database files.

> **See Also:** Section 6.4, "Task 4: Relocate the Database Datafiles, Control Files, and Log Files"

Step 2 Preserve Any Important Application Files and Log Files

If there are application files or log files in the source Oracle home that are being referenced or used by the destination Oracle home, you should move them to another location before you decommission the source Oracle home, and, in the destination Oracle home, change any references to the files to the new location.

Step 3 Remove the Source OracleAS Identity Management Instance from the partner application list

After you upgrade to Oracle Identity Management 10*g* (10.1.4.0.1), the source OracleAS Identity Management instance that you upgraded remains in the list of OracleAS Single Sign-On partner applications.

From the command line, set the ORACLE_HOME environment variable and then run the following command:

```
DESTINATION_ORACLE_HOME/bin/ssoreg.bat
  -oracle_home_path path_to_oracle_home
  -site_name name_of_sso_site
  -config_mod_osso TRUE
  -mod_osso_url partner_app_URL
  -update_mode DELETE
  -config_file path_to_osso_config_file
```

Note that the `-config_file` argument is necessary only when SSL is enabled.

> **See Also:** "Configuring and Administering Partner Applications" in the *Oracle Application Server Single Sign-On Administrator's Guide* for specific information on the syntax and available arguments to the `ssoreg.sh` utility

Step 4 Remove the Source OracleAS Identity Management Instance from the OracleAS Farm

After you upgrade to Oracle Identity Management 10*g* (10.1.4.0.1), the source OracleAS Identity Management instance that you upgraded remains in the list of instances on the Application Server Control Console Farm page.

To remove the source instance from the farm and from the Farm page, use the following command in the source Oracle home:

```
SOURCE_ORACLE_HOME/dcm/bin/dcmctl leavefarm
```

See Also: *Distributed Configuration Management Administrator's Guide* for more information about the `dcmctl leavefarm` command

"Introduction to Administration Tools" in the *Oracle Application Server Administrator's Guide* for more information about the Farm page in the Application Server Control Console

Step 5 Deinstall the OracleAS Identity Management Source Oracle Home

When you are certain that the upgrade was successful, you have all of the necessary backups, and have no plans to revert to the source Oracle home, you may elect to remove the files from the source Oracle home.

Use the Oracle Universal Installer to deinstall the instance.

Part III

Appendices for Specialized Environments and Troubleshooting

This part contains the following appendices:

A

Performing an Oracle Identity Management Multimaster and Fan-Out Replication Upgrade

This appendix describes how to upgrade to Oracle Identity Management 10*g* (10.1.4.0.1) in an Oracle Internet Directory replicated environment.

Refer to the following sections for more information:

- Task 1: Review the Terminology, Prerequisites, and Key Concepts For Upgrading a Replication Environment
- Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade
- Task 3: Perform the Oracle Internet Directory Replica Upgrade
- Task 4: Completing the Upgrade of Each Replica
- Task 5: Upgrading OracleAS Single Sign-On and Oracle Delegated Administration Services in a Replicated Environment

A.1 Task 1: Review the Terminology, Prerequisites, and Key Concepts For Upgrading a Replication Environment

Review the following prerequisites and requirements before proceeding with the upgrade procedures in this chapter:

- Terminology Conventions for This Chapter
- Valid Starting Points When Upgrading a Replication Environment
- Understanding the Proper Order of Upgrades in a Replication Environment
- Oracle Recommendations When Upgrading a Replication Environment

A.1.1 Terminology Conventions for This Chapter

In this chapter, the **destination replica** is the newly installed and upgraded 10*g* (10.1.4.0.1) replica; the **source replica** is the 10*g* Release 2 (10.1.2) replica you are upgrading.

A.1.2 Valid Starting Points When Upgrading a Replication Environment

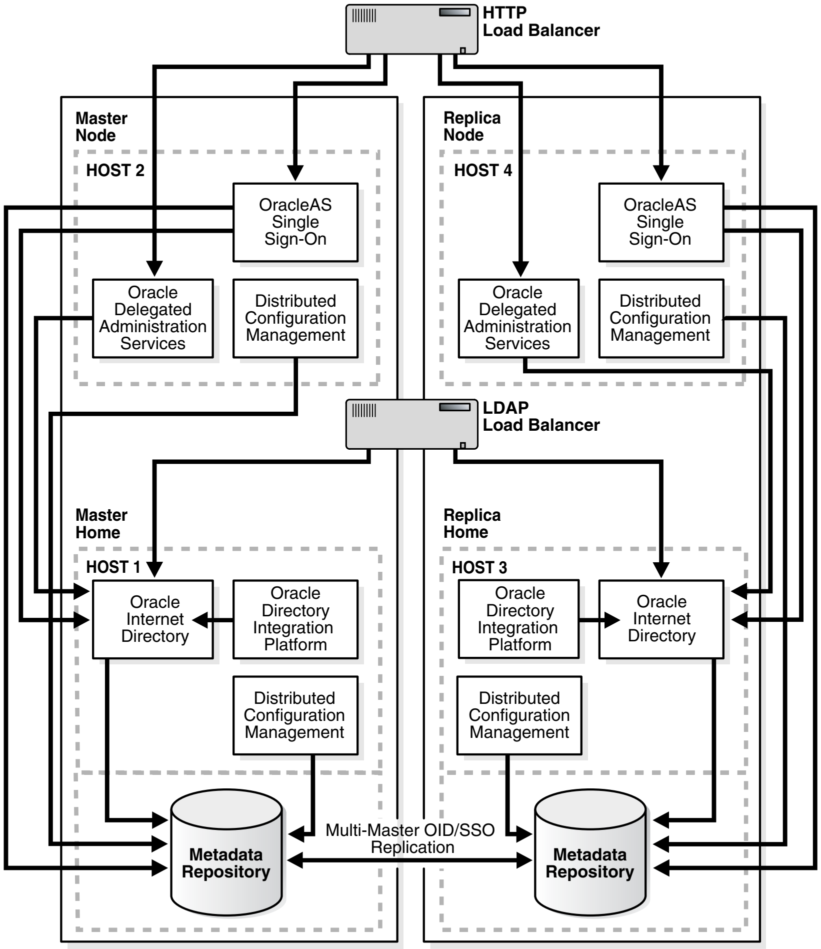
The upgrade procedures in this chapter are designed for administrators who have installed and configured an Oracle Internet Directory 10*g* (9.0.4), 10*g* Release 2

(10.1.2.0.2), or 10*g* Release 2 (10.1.2.1.0) multimaster or fan-out replication environment.

This chapter assumes that the Oracle Identity Management components in the replication environment are distributed. In other words, you have installed the Oracle Internet Directory (and optionally Oracle Directory Integration Platform) components in one or more Oracle homes, and you installed the Oracle Application Server Single Sign-On and Oracle Delegated Administration Services components in one or more additional Oracle homes.

Figure A–1 shows a typical Oracle Identity Management 10*g* Release 2 (10.1.2) multimaster replication environment, which is described in detail in "Deploying Identity Management with Multimaster Replication," in the 10*g* Release 2 (10.1.2) *Oracle Application Server High Availability Guide*.

Figure A–1 A Typical Oracle Identity Management 10g Release 2 (10.1.2) Multimaster Replication Environment


HTTP Load Balancer
Master Node
HOST 2
OracleAS Single Sign-On
Oracle Delegated Administration Services
Distributed Configuration Management
Replica Node
HOST 4
OracleAS Single Sign-On
Oracle Delegated Administration Services
Distributed Configuration Management
LDAP Load Balancer
Master Home
HOST 1
Oracle Internet Directory
Oracle Directory Integration Platform
Distributed Configuration Management
Replica Home
HOST 3
Oracle Directory Integration Platform
Oracle Internet Directory
Distributed Configuration Management
Metadata Repository
Multi-Master OID/SSO Replication
Metadata Repository

Information about deploying Oracle Identity Management with fan-out replication can be found in the Oracle Application Server 10*g* Release 2 (10.1.2) *Oracle Identity Management Concepts and Deployment Planning Guide*, which is available in the Oracle Application Server 10*g* Release 2 (10.1.2) documentation library.

A.1.3 Understanding the Proper Order of Upgrades in a Replication Environment

Oracle recommends that you first upgrade theOracle Internet Directory and Oracle Directory Integration Platform Oracle homes on all replicas to 10*g* (10.1.4.0.1). Then, after the Oracle Internet Directory installations are upgraded, upgrade the OracleAS Single Sign-On and Oracle Delegated Administration Services components of Oracle Identity Management.

A.1.4 Oracle Recommendations When Upgrading a Replication Environment

Oracle Corporation recommends the following during the upgrade procedure:

- After you upgrade the destination replica, disable replication between the destination replica and the source replica. The destination replica can receive and process changes from source replica, but the source replica cannot process changes originated and received from destination replica.
- The replication environment can be a Single Master (that is, only one replica is set to read and write, and all others are set to read only).

A.2 Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade

Before you begin upgrading Oracle Internet Directory in a replicated environment, you must perform the following steps for all replicas other than Master Definition Site (MDS) Replica or Primary supplier replica:

1. Locate the database registration entry of the database of replica to be upgraded.

```
SOURCE_ORACLE_HOME/bin/ldapsearch
     -h hostname_of_replica_being_upgraded
     -p port
     -D cn=orcladmin
     -w superuser_password
     -b "cn=oraclecontext"
     -s one "(objectclass=orcldbserver)" dn
```

   This will return a list of Distinguished Names (DNs) corresponding to all the Databases registered in Oracle Internet Directory in the following form:

```
cn=database_name,cn=oraclecontext
```

   From the returned list of entries, locate and make a note of the DN of the following entry, which corresponds to the replica upgraded:

```
cn=dbname_of_replica_to_be_upgraded,cn=oraclecontext
```

2. Identify the replica ID of the replica to be upgraded by issuing following command:

```
SOURCE_ORACLE_HOME/bin/ldapsearch
     -h hostname_of_replica_being_upgraded
     -p port
     -D cn=orcladmin
     -w superuser_password
     -b ""
     -s base "(objectclass=*)" orclreplicaid
```

3. Modify the `seeAlso` attribute of the replica subentry so that it points to the database you are about to upgrade.

The seeAlso attribute is a standard Oracle Internet Directory attribute. For more information, see the "Attribute Reference" in the *Oracle Identity Management User Reference*.

To modify the seeAlso attribute:

a. Create a file, for example mod.ldif, with following contents:

```
#File Name : mod.ldif
dn: orclreplicaid=replicaid_from_step_2,cn=replication configuration
changetype: modify
replace: seeAlso
#The DN used in seealso attribute is obtained in Step #1.
seeAlso: cn=dbname_of_replica_being_upgraded,cn=oraclecontext
```

b. Modify the replica subentry using ldapmodify command.

```
SOURCE_ORACLE_HOME/bin/ldapmodify
   -h hostname_of_replica_being_upgraded
   -p port
   -D superuser_DN
   -w superuser_password
   -v
   -f mod.ldif
```

4. Navigate to the following directory and locate ias.properties file:

```
SOURCE_ORACLE_HOME/config
```

5. Open the ias.properties file and verify that the properties shown in Table A–1 are correct and valid.

6. Make sure the Oracle Internet Directory server is up and running.

   To verify that Oracle Internet Directory is running, enter one of the following commands.

   > **Note:** You may have to temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the ldapbind command.
   >
   > After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 10*g* (10.1.4.0.1) installer to begin the upgrade procedure.

   If you are running Oracle Internet Directory on a non-secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p Non-SSL_port
   ```

   If you are running Oracle Internet Directory on a secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p SSL_port -U 1
   ```

   These commands should return a "bind successful" message.

7. If you are upgrading a 10*g* (9.0.4) replication environment, verify that the tnsnames.ora file contains only one alias for the local database.

   For example, the tnsnames.ora file might contain two entries for a database called ORCL03, as in the following example:

```
ORCL03 =
  (DESCRIPTION =
     (ADDRESS_LIST =
         (ADDRESS = (PROTOCOL = TCP)
                    (HOST = stakb03.acme.com)
                    (PORT = 1521)))
      (CONNECT_DATA =
          (SERVICE_NAME = orcl03.acme.com)))

ORCL03.US.ORACLE.COM =
  (DESCRIPTION =
      (ADDRESS_LIST =
           (ADDRESS = (PROTOCOL = TCP)
                      (HOST = stakb03.acme.com)
                      (PORT = 1521)))
       (CONNECT_DATA =
            (SERVICE_NAME = orcl03.us.oracle.com)))
```

In this example, remove the second, fully-qualified entry for the local database before you begin the upgrade procedure. After upgrade is complete, you can add the fully qualified database name alias to the `tnsnames.ora` file.

8. If you are upgrading from 10*g* (9.0.4), then perform the following steps to add required entries to the Oracle Internet Directory server:

   a. Create an LDIF file, for example `add.ldif`, with the contents shown in Example A–1.

   b. Start a second instance of the Oracle Internet Directory server with "change log generation disabled" as shown below.

   Note that this example assumes that the second instance is not in use and port 4444 is not used by any process.

   ```
   oidctl connect=connect_string_of_db
          server=oidldapd
          instance=2
          flags="-p 4444 -l false"
          start
   ```

   c. Add the entries defined in the `ldif` file you created in Step 8 by using `ldapadd` tool as shown below.To add these entries, you must use the port used for the LDAP server you started in Step b.

   This example assumes that the LDAP server you started in step 8 is listening at port 4444.

   ```
   ldapadd -p 4444
           -h hostname
           -D cn=orcladmin
           -w password
           -f ldif_filename
           -c
   ```

   For example:

   ```
   ldapadd -p 4444
           -h mgmt42.acme.com
           -D cn=orcladmin
           -w m03kslj
           -f add.ldif
           -c
   ```

9. Stop the second LDAP server as shown below.

   This example assumes that the instance number used for the second instance was 2.

   ```
   oidctl connect=<connect_string_of_db> server=oidldapd instance=2 stop
   ```

Table A–1   Properties to Verify in ias.properties Before Replication Upgrade

Property Name	Correct Value Before Replication Upgrade
OID.LaunchSuccess	True
OIDhost	*host name of replica*
OIDport	*port of replica*
OIDsslport	*SSL port for replica*

Example A–1   Contents of LDIF File Used to Prepare for Replication Upgrade

```
#File Name : add.ldif
################################
# Event Type Configuration
################################

dn: cn=ProvisioningEventTypeConfig,cn=odi,cn=oracle internet directory
changetype: add
cn: ProvisioningEventTypeConfig
orclaci: access to entry by group="cn=Provisioning Admins,
  cn=changelog subscriber,cn=oracle internet directory" (browse,add,delete)
orclaci: access to attr=(*) by group="cn=Provisioning Admins,
  cn=changelog subscriber,cn=oracle internet directory"
  (read,search,write,compare)
objectclass: orclContainer

dn: orclODIPProvEventObjectType=ENTRY,cn=ProvisioningEventTypeConfig,cn=odi,
  cn=oracle internet directory
changetype: add
orclODIPProvEventObjectType: ENTRY
orclODIPProvEventLDAPChangeType: Add
orclODIPProvEventLDAPChangeType: Modify
orclODIPProvEventLDAPChangeType: Delete
orclODIPProvEventCriteria: objectclass=*
objectclass: orclODIPProvEventTypeConfig

dn: orclODIPProvEventObjectType=USER,cn=ProvisioningEventTypeConfig,cn=odi,
  cn=oracle internet directory
changetype: add
orclODIPProvEventObjectType: USER
orclODIPProvEventLDAPChangeType: Add
orclODIPProvEventLDAPChangeType: Modify
orclODIPProvEventLDAPChangeType: Delete
orclODIPProvEventCriteria: objectclass=InetOrgPerson
orclODIPProvEventCriteria: objectclass=orclUserV2
objectclass: orclODIPProvEventTypeConfig

dn: orclODIPProvEventObjectType=IDENTITY,cn=ProvisioningEventTypeConfig,cn=odi,
  cn=oracle internet directory
changetype: add
orclODIPProvEventObjectType: IDENTITY
orclODIPProvEventLDAPChangeType: Add
```

```
orclODIPProvEventLDAPChangeType: Modify
orclODIPProvEventLDAPChangeType: Delete
orclODIPProvEventCriteria: objectclass=InetOrgPerson
orclODIPProvEventCriteria: objectclass=orclUserV2
objectclass: orclODIPProvEventTypeConfig

dn: orclODIPProvEventObjectType=GROUP,cn=ProvisioningEventTypeConfig,cn=odi,
    cn=oracle internet directory
changetype: add
orclODIPProvEventLDAPChangeType: Add
orclODIPProvEventLDAPChangeType: Modify
orclODIPProvEventLDAPChangeType: Delete
orclODIPProvEventCriteria: objectclass=orclGroup
orclODIPProvEventCriteria: objectclass=orclPrivilegeGroup
orclODIPProvEventCriteria: objectclass=groupOfUniqueNames
orclODIPProvEventCriteria: objectclass=groupofNames
objectclass: orclODIPProvEventTypeConfig

dn: orclODIPProvEventObjectType=SUBSCRIPTION,cn=ProvisioningEventTypeConfig,
  cn=odi,cn=oracle internet directory
changetype: add
orclODIPProvEventObjectType: SUBSCRIPTION
orclODIPProvEventLDAPChangeType: Add
orclODIPProvEventLDAPChangeType: Modify
orclODIPProvEventLDAPChangeType: Delete
orclODIPProvEventCriteria: objectclass=orclServiceSubscriptionDetail
objectclass: orclODIPProvEventTypeConfig

dn: orclODIPProvEventObjectType=SUBSCRIBER,cn=ProvisioningEventTypeConfig,
  cn=odi,cn=oracle internet directory
changetype: add
orclODIPProvEventObjectType: SUBSCRIBER
orclODIPProvEventLDAPChangeType: Add
orclODIPProvEventLDAPChangeType: Modify
orclODIPProvEventLDAPChangeType: Delete
orclODIPProvEventCriteria: objectclass=orclSubscriber
objectclass: orclODIPProvEventTypeConfig

######################################################################
# DIPADMIN Account
######################################################################

dn: cn=dipadmin,cn=odi,cn=oracle internet directory
changetype: add
cn: dipadmin
sn: dipadmin
description: DIP Administrator Idenitity in OID
objectclass: person

######################################################################
# DIPADMIN Group
######################################################################

dn: cn=dipadmingrp,cn=odi,cn=oracle internet directory
changetype: add
cn: dipadmin
owner: cn=dipadmin,cn=odi,cn=oracle internet directory
uniquemember: cn=orcladmin
uniquemember: cn=dipadmin,cn=odi,cn=oracle internet directory
description: DIP Administrator Group in OID
```

```
objectclass: groupOfUniqueNames
objectclass: orclprivilegegroup

######################################################################
# ODIPGROUP getting recreated here from 904 (Had been removed in 902*)
######################################################################

dn: cn=odipgroup,cn=odi,cn=oracle internet directory
changetype: add
cn: odipgroup
objectclass: top
objectclass: groupofUniquenames
objectclass: orclprivilegegroup
uniquemember: cn=orcladmin
orclaci: access to entry by group="cn=dipadmingrp,cn=odi,cn=oracle internet
  directory" (browse) by * (none)
orclaci: access to attr=(uniquemember) by  group="cn=dipadmingrp,cn=odi,
  cn=oracle internet directory" (search,read,write,compare) by * (none)

dn: cn=odisgroup,cn=odi,cn=oracle internet directory
changetype: add
cn: odisgroup
objectclass: top
objectclass: groupofUniquenames
objectclass: orclprivilegegroup
uniquemember: cn=orcladmin
orclaci: access to entry by * (none)
orclaci: access to attr=(*) by * (none)
```

A.3 Task 3: Perform the Oracle Internet Directory Replica Upgrade

You can upgrade one replica at a time, or all of the replicas simultaneously. Refer to the following sections for more information:

- Selecting a Replica Upgrade Method
- Upgrading One Replica at a Time
- Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously

A.3.1 Selecting a Replica Upgrade Method

Upgrading one computer at a time in a replicated environment ensures that Oracle Internet Directory is available during the upgrade for additions, modifications, and searching. When you use this method, only the replica you are upgrading is down. The other replicas continue to run and are available to your users.

Upgrading multiple replicas simultaneously ensures that the entire network is upgraded without a transient stage. The procedure is simpler than upgrading one replica at a time, but involves directory service downtime.

A.3.2 Upgrading One Replica at a Time

Follow these steps to upgrade one replica at a time:

1. Make sure you have completed the procedure in Section A.2, "Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade".
2. Identify the replica to be upgraded.

The replica can be an LDAP-based partial or fan-out replica, or it can be an Oracle Advanced Replication (ASR) based multimaster replica.

> **See Also:** "Directory Replication Concepts" in the *Oracle Internet Directory Administrator's Guide*

3. Stop the replication server on the replica to be upgraded.

```
SOURCE_ORACLE_HOME/oidctl
   connect=db_connect_string
   server=OIDREPLD
   instance=1
   flags="-p port_at_which_ldap_server_is_listening"
   stop
```

> **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Identity Management User Reference* for more information about the `oidctl` administration tool

4. Make sure that the Oracle Internet Directory server, the Oracle Internet Directory database, and the database listener are up and running.
5. If you are upgrading an ASR-based replica, then delete all ASR jobs on other replicas by issuing the following command:

```
SOURCE_ORACLE_HOME/ldap/admin/oidrdjob.sql
```

All ASR jobs on other master sites that transfer changes to this replica are deleted. This has the effect of taking the replica currently being upgraded out of the replication environment, so that no changes come to it, while other replicas continue to operate and replicate changes.

6. Upgrade the replica as described in Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management".
7. Verify that the database in the upgraded replica Oracle home is up and running.
8. Test the connectivity to the other replicas.

The Net Services Upgrade assistant might have modified `listener.ora` and `tnsnames.ora,` breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the corresponding files in the source Oracle home.

For example, copy the original entries from the following files in the source Oracle home to the corresponding files in the destination Oracle home:

```
SOURCE_ORACLE_HOME/network/admin/listener.ora
SOURCE_ORACLE_HOME/network/admin/sqlnet.ora
SOURCE_ORACLE_HOME/network/admin/tnsnames.ora
```

If you are upgrading from a 10*g* (9.0.4) replication environment, add the database alias you removed from the `tnsnames.ora` file in Step 7 of Section A.2.

9. If you are upgrading an Oracle Advanced Replication (ASR) based Replica, recreate the jobs on each replica, after it is upgraded, by issuing the following command:

```
DESTINATION_ORACLE_HOME/ldap/bin/remtool -asrrectify
```

The jobs that were deleted in Step 5 are re-created. They will begin transferring the existing changes and new changes from other replicas to the upgraded replicas.

10. Perform the Oracle Internet Directory post-upgrade procedures.

    See Also: Section 9.2, "Task 2: Perform Oracle Internet Directory Post-Upgrade Steps"

11. Perform the procedures described in Section A.4, "Task 4: Completing the Upgrade of Each Replica" for the newly upgraded replica.

12. Start the replication server on the newly upgrade replica, if it is not already running:

```
DESTINATION_ORACLE_HOME/oidctl
   connect=db_connect_string
   server=OIDREPLD
   instance=1
   flags="-p port_at_which_ldap_server_is_listening"
   start
```

    See Also: "Oracle Identity Management Server Administration Tools" in the *Oracle Identity Management User Reference* for more information about the `oidctl` administration tool

13. Upgrade the remaining replicas using the same procedures you used to upgrade the first replica.

A.3.3 Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously

Use the following procedure to upgrade all the replicas simultaneously:

1. In all replicas other than MDS replica or primary supplier replica, make sure you have completed the pre-upgrade steps provided in Section A.2, "Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade".

2. Stop the replication server on all replicas in the Directory Replication Group (DRG):

```
SOURCE_ORACLE_HOME/oidctl
   connect=db_connect_string
   server=OIDREPLD
   instance=1
   flags="-p port_at_which_ldap_server_is_listening"
   stop
```

    See Also: "Oracle Identity Management Server Administration Tools" in the *Oracle Identity Management User Reference* for more information about the `oidctl` administration tool

3. Use Oracle Universal Installer and the 10*g* (10.1.4.0.1) installation procedure to upgrade each of the Oracle Internet Directory replicas.

   Refer to Section 7.5.2, "Upgrading OracleAS Identity Management in a Non-Colocated Infrastructure" for information about starting Oracle Universal Installer and selecting the proper options on the installer screens.

4. Verify that the database on each upgraded replica is up and running.

5. Test the connectivity to the other replicas.

   The Net Services Upgrade assistant might have modified `listener.ora` and `tnsnames.ora,` breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the corresponding files in the source Oracle home.

For example, copy the original entries from the following files in the source Oracle home to the corresponding files in the destination Oracle home:

```
SOURCE_ORACLE_HOME/network/admin/listener.ora
SOURCE_ORACLE_HOME/network/admin/sqlnet.ora
SOURCE_ORACLE_HOME/network/admin/tnsnames.ora
```

If you are upgrading from a 10*g* (9.0.4) replication environment, add the database alias you removed from the `tnsnames.ora` file in Step 7 of Section A.2.

6. Perform the Oracle Internet Directory post-upgrade procedures.

   See Also: Chapter 9.2, "Task 2: Perform Oracle Internet Directory Post-Upgrade Steps"

7. For each upgraded replica, perform the steps in Section A.4, "Task 4: Completing the Upgrade of Each Replica".

8. Start the replication server on each of the upgraded replicas:

```
DESTINATION_ORACLE_HOME/oidctl
   connect=db_connect_string
   server=OIDREPLD
   instance=1
   flags="-p port_at_which_ldap_server_is_listening"
   start
```

   See Also: "Oracle Identity Management Server Administration Tools" in the *Oracle Identity Management User Reference* for more information about the `oidctl` administration tool

A.4 Task 4: Completing the Upgrade of Each Replica

The following sections describe tasks you must perform after you have completed the upgrade of a replica:

- Changing the Replication DN Password in the Oracle Internet Directory Wallet for Each Replica
- Setting the orclreplicationid Attribute in the Upgraded 10g (10.1.4.0.1) Directory

A.4.1 Changing the Replication DN Password in the Oracle Internet Directory Wallet for Each Replica

After you upgrade a replica, change the password for the replication distinguished name (DN). After you change or reset the password, you can then start `oidmon`, LDAP server, and replication server.

Refer to the following sections for more information:

- Changing the Replication DN Password
- Resetting the Replication DN Password

A.4.1.1 Changing the Replication DN Password

After you upgrade a replica, change the replication distinguished name (DN) password stored in the wallet using the Replication Environment Management Tool (`remtool`), as follows:

```
DESTINATION_ORACLE_HOME/ldap/bin/remtool -pchgwalpwd -v -bind host:port/repl_dn_
pwd
```

Note that you must provide the existing password on the `remtool` command line. If you do not know the replication DN password, see Section A.4.1.2, "Resetting the Replication DN Password".

> **See Also:** "remtool" in the *Oracle Identity Management User Reference* for details about the arguments you can use with the `remtool` command, including the `-pchgwalpwd` and `-presetpwd` arguments

A.4.1.2 Resetting the Replication DN Password

If you do not know replication DN password, reset the replication DN password using the following command:

```
DESTINATION_ORACLE_HOME/ldap/bin/remtool -presetpwd -v -bind host:port
```

If you are upgrading a fan-out replica, you must also reset the password of the replication DN at its supplier. To reset the password of replication DN at its supplier:

Create an LDIF file (for example, `modpwd.ldif`), with following contents:

```
dn: cn=replication dn,orclreplicad=consumer_replicaid,cn=replication configuration
changetype: modify
replace: userpassword
userpassword: new_password
```

Apply the change at supplier using ldapmodify tool as shown below:

```
ldapmodify  -h supplier_hostname
            -p supplier_port_number>
            -D cn=orcladmin
            -w super_user_password_of_supplier
            -f modpwd.ldif
```

A.4.2 Setting the orclreplicationid Attribute in the Upgraded 10*g* (10.1.4.0.1) Directory

If you are upgrading a replica in an environment with fan-out replication, you must set the `orclreplicationid` in the Oracle Internet Directory attribute to a valid value. This is a new attribute for Oracle Identity Management 10*g* (10.1.4.0.1).

Oracle recommends that you set the value of this attribute so it matches the value of the existing `orclagreementID` attribute. To perform this task:

1. Create an LDIF file called `id.ldif` with the following content:

   ```
   dn: orclagreementid=000002,orclreplicaid=replicaid,cn=replication configuration
   changetype: modify
   replace: orclreplicationid
   orclreplicationid: 2
   ```

   Note that in the above example, the first two lines should appear all in one line in the LDIF file.

2. Apply the LDIF file by using the following `ldapmodify` command:

```
ldapmodify -p port
           -h host
           -D DN
           -w password
           -f id.ldif
```

In this example, replace *port*, *host*, *DN*, and *password* with the appropriate values for your environment.

> **See Also:** "The Replication Agreement Entry" in the chapter, "Oracle Internet Directory Replication Concepts" in the *Oracle Internet Directory Administrator's Guide* for information about the `orclreplicationid` attribute
>
> "Oracle Internet Directory Data Management Tools" in the *Oracle Identity Management User Reference* for more information about using the `ldapmodify` command

A.5 Task 5: Upgrading OracleAS Single Sign-On and Oracle Delegated Administration Services in a Replicated Environment

After you have upgraded the Oracle Internet Directory Oracle homes, you can then upgrade the OracleAS Single Sign-On and Oracle Delegated Administration Services Oracle homes.

To upgrade the OracleAS Single Sign-On and Oracle Delegated Administration Services Oracle homes, use Oracle Universal Installer and the 10*g* (10.1.4.0.1) installation procedure.

Refer to Section 7.5.3, "Upgrading Distributed OracleAS Identity Management Configurations" for instructions on starting Oracle Universal Installer and selecting the proper options on the installer screens.

B

Upgrading High Availability Configurations

This chapter describes considerations, restrictions, and recommended procedures for upgrading an Oracle Application Server environment that has been configured for high availability.

This chapter contains the following sections:

- Summary of High Availability Upgrade Options, Restrictions, and Prerequisites
- Upgrading an OracleAS Cold Failover Cluster Infrastructure
- Transforming 10g (9.0.4) Rack-Mounted Identity Management
- Transforming a Distributed 10g (9.0.4) Rack-Mounted Identity Management Environment
- Upgrading an OracleAS Cluster (Identity Management) 10g Release 2 (10.1.2) Colocated Configuration
- Upgrading an OracleAS Cluster (Identity Management) 10g Release 2 (10.1.2) Distributed Configuration

B.1 Summary of High Availability Upgrade Options, Restrictions, and Prerequisites

Oracle Application Server 10*g* (9.0.4) introduced high availability configurations that you could install as part of the Oracle Application Server installation procedure. These configurations were also available as part of 10*g* Release 2 (10.1.2.0.0), 10*g* Release 2 (10.1.2.1.0), and 10*g* Release 2 (10.1.2.0.2).

Table B–1 shows the upgrade paths supported for the high availability configurations.

Table B–1 Summary of the High Availability Upgrade Options

Existing Configuration	Upgrade Path	More Information
Oracle Application Server Cold Failover Clusters	Upgrade to Oracle Application Server Cold Failover Clusters for 10*g* (10.1.4.0.1).	Section B.2, "Upgrading an OracleAS Cold Failover Cluster Infrastructure"
10*g* (9.0.4) Rack-Mounted Identity Management	Transform the environment into a 10*g* (10.1.4.0.1) OracleAS Cluster (Identity Management) environment.	Section B.3, "Transforming 10g (9.0.4) Rack-Mounted Identity Management"

Table B–1 (Cont.) Summary of the High Availability Upgrade Options

Existing Configuration	Upgrade Path	More Information
10*g* Release 2 (10.1.2) colocated OracleAS Cluster (Identity Management)	Upgrade the cluster to OracleAS Cluster (Identity Management) 10*g* (10.1.4.0.1)	Section B.5, "Upgrading an OracleAS Cluster (Identity Management) 10g Release 2 (10.1.2) Colocated Configuration"
10*g* Release 2 (10.1.2) Distributed OracleAS Cluster (Identity Management)	Upgrade the distributed Oracle homes to OracleAS Cluster (Identity Management) 10*g* (10.1.4.0.1)	Section B.6, "Upgrading an OracleAS Cluster (Identity Management) 10g Release 2 (10.1.2) Distributed Configuration"
Disaster Recovery	Upgrade the production site and the standby site separately.	"Oracle Application Server Disaster Recovery" in the *Oracle Application Server High Availability Guide*

The procedures provided in this chapter assume that you used the Oracle Application Server 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) installation guide (depending upon the upgrade options you select) to install and configure your high availability configuration and that you have met all of the prerequisites described in the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) installation guide.

For example, these procedures assume you have already installed and configured clusterware such as Sun Cluster, VERITAS Cluster Server, or Fujitsu-Siemens PrimeCluster. For the official list of certified clusterware, visit the Certify section of Oracle*MetaLink*:

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

To check that the clusterware is running, use the command appropriate for your clusterware. For example, if you are running Sun Cluster, use the `scstat` command to get the status of the nodes in the cluster.

These procedures also assume you are using the seed database that was installed automatically with the 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) installation procedure or with the OracleAS RepCA.

> **See Also:** The Oracle Application Server 10*g* (9.0.4) installation guide for your platform, which is available as part of the platform-specific documentation library on the Oracle Technology Network:
>
> ```
> http://www.oracle.com/technology/documentation/appserver10g.html
> ```
>
> The Oracle Application Server 10*g* Release 2 (10.1.2) installation guide for your platform, which is available as part of the platform-specific documentation library on the Oracle Technology Network:
>
> ```
> http://www.oracle.com/technology/documentation/appserver101402.html
> ```

B.2 Upgrading an OracleAS Cold Failover Cluster Infrastructure

To upgrade a 10*g* (9.0.4) OracleAS Cold Failover Cluster Infrastructure installation:

1. If vendor clusterware agents or packages are being utilized to automatically monitor and manage the OracleAS Cold Failover Cluster environment, these should be stopped before you perform the 10*g* (10.1.4.0.1) upgrade.

   In addition, to re-enable vendor cluster agents or packages after the upgrade has been completed, verify that certification has been provided by the appropriate vendor for the 10*g* (10.1.4.0.1) OracleAS Cold Failover Cluster environment.

2. Make sure that the OracleAS Metadata Repository database and database listener are up and running.

3. Log in to the computer on which the 10*g* (9.0.4) OracleAS Cold Failover Cluster is installed, as the same operating system user that performed the 10*g* (9.0.4) installation.

   > **Note:** You must be logged in as a member of the `dba` operating system group.

4. Make sure the Oracle Internet Directory server is up and running.

   To verify that Oracle Internet Directory is running, enter one of the following commands.

   > **Note:** You may have to temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the `ldapbind` command.
   >
   > After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 10*g* (10.1.4.0.1) installer, as directed in Step 5.

   If you are running Oracle Internet Directory on a non-secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p Non-SSL_port
   ```

   If you are running Oracle Internet Directory on a secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p SSL_port -U 1
   ```

   These commands should return a "bind successful" message.

   > **See Also:** "Syntax for LDIF and Command-Line Tools" in the *Oracle Internet Directory Administrator's Guide* for more information about the `ldapbind` utility

Note: Oracle Internet Directory 10*g* (9.0.4) allows you to start and stop the directory service using OPMN or the `oidctl` utility.

Before upgrading an OracleAS Identity Management Oracle home that contains Oracle Internet Directory, start the Oracle Internet Directory instance using the `opmnctl` utility or the Application Server Control Console. Do not use the `oidctl` utility; otherwise, Oracle Universal Installer will not be able to start and stop Oracle Internet Directory automatically during the upgrade process.

The correct use of `opmnctl` and `oidctl` is described in the Chapter "Oracle Internet Directory Process Control–Best Practices" in the *Oracle Internet Directory Administrator's Guide*.

5. Be sure to set the environment variables, as defined in the section "Environment Variables" in the "Requirements" chapter of the *Oracle Application Server Installation Guide*.

   In particular, be sure to set following variables so they do not reference any Oracle home directories:

   - PATH
   - CLASSPATH
   - LD_LIBRARY_PATH

   In addition, be sure the following environment variables are not set:

   - TNS_ADMIN
   - ORACLE_HOME
   - ORACLE_SID

6. Mount the Oracle Application Server 10*g* (10.1.4.0.1) CD–ROM and start the installer.

   See Also: *Oracle Application Server Installation Guide* for detailed instructions about starting Oracle Universal Installer on your platform

7. Refer to Table B–2 for information on the options you should select on each screen.
8. After the End of Installation screen appears, exit Oracle Universal Installer and then verify that Oracle Internet Directory and Oracle Application Server Single Sign-On are functioning and accessible in the new 10*g* (10.1.4.0.1) Oracle home.

   See Also: *Oracle Application Server Administrator's Guide*, Chapter 1, "Accessing the Single Sign-On Server"

9. Review Chapter 9, "Component-Specific Post-Upgrade Procedures" and perform any post-upgrade tasks that are required for your configuration.
10. The following step is required only if you meet **both** of these requirements:

    - You plan to use the Automatic Storage Management (ASM) feature of Oracle Database 10*g* for the OracleAS Metadata Repository.
    - Your computer does not have an existing Oracle Database 10*g*.

If you meet these requirements, you need to configure the CSS daemon on the other node. The CSS daemon synchronizes ASM instances with the database instances that use the ASM instances for database file storage.

To configure the CSS daemon:

1. Stop all the processes in the Oracle Application Server Cold Failover Clusters (Infrastructure) home.
2. Stop the CSS daemon. You can do this by running the following command as root.

   ```
   # /etc/init.d/init.cssd stop
   ```

3. Fail over the IP and the disk to the other node.
4. On the other node, run the following command as root:

   ```
   # $ORACLE_HOME/root.sh
   ```

   ORACLE_HOME is where you installed the Oracle Application Server Cold Failover Clusters (Infrastructure).

11. After you upgrade OracleAS Identity Management in a colocated Infrastructure, refer to the following sections for information about post-upgrade tasks you should consider performing to help you manage and maintain the upgraded database:

    - Section 6.4, "Task 4: Relocate the Database Datafiles, Control Files, and Log Files"
    - Section 6.5, "Task 5: Configure Oracle Enterprise Manager 10g Database Control"

12. If you have installed or upgraded any 10*g* Release 2 (10.1.2) middle tiers that use the OracleAS Metadata Repository for components such as OracleAS Portal, OracleAS Wireless, or Oracle Application Server Certificate Authority, then run the Metadata Repository Upgrade Assistant (MRUA) to upgrade the component schemas in the OracleAS Metadata Repository.

    For instructions on running MRUA, see Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository".

13. Complete the Oracle Application Server Cold Failover Clusters Post-Installation instructions described in "Post-Installation Steps for OracleAS Cold Failover Cluster" in the *Oracle Application Server Installation Guide*.

Table B–2 Summary of the Oracle Universal Installer Screens During the OracleAS Cold Failover Cluster Infrastructure Upgrade

Screen	Description and Recommended Options to Select
Welcome	Welcomes you to Oracle Universal Installer and the Oracle Application Server installation procedure.

Table B–2 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Cold Failover Cluster Infrastructure Upgrade

Screen	Description and Recommended Options to Select
Specify File Locations	Enter a name and path for the new Oracle home. This new Oracle home will be the destination Oracle home for your Oracle Application Server 10*g* (10.1.4.0.1) upgrade. **Notes:** ■ You must enter a directory in the file system that can be mounted from either node in the OracleAS Cold Failover Cluster configuration. ■ You must enter a new Oracle home name and directory. Do not select an existing Oracle home from the drop down list. If you select an existing Oracle home, the installer will not display the next screen, Specify Hardware Cluster Installation Mode. Example: `/mnt/app/oracle/OraInfra_10_1_2`
Specify Hardware Cluster Installation Mode	This screen appears only if you have Oracle Cluster Ready Services installed. It is okay if you do not see this screen; Oracle Cluster Ready Services is not required for OracleAS Cold Failover Cluster. Select **Local Installation** because you are installing OracleAS Infrastructure on the shared storage. Click Next.
Select a Product to Install	Select **OracleAS Infrastructure 10g**. If multiple languages are used in the OracleAS Infrastructure you are upgrading, then click **Product Languages**.
Language Selection	The screen appears only if you clicked **Product Languages** on the Select a Product to Install screen. If multiple languages are used in the OracleAS Infrastructure you are upgrading, select those languages. If you are not sure which languages were installed, but want languages other than English, click the double arrow button (>>) to select all languages.
Select Installation Type	Select **Identity Management and OracleAS Metadata Repository**. **Note:** It is very important that you select the same installation type that is used in the Oracle home you are upgrading.
Upgrade Existing Infrastructure	This screen appears when Oracle Universal Installer detects an existing Oracle Application Server installation of the same type as the one you selected on the Select Installation Type screen. Select the option to upgrade an existing OracleAS Infrastructure, and then select the Oracle home you want to upgrade from the drop-down list. (If there is only one Infrastructure of the selected time on the computer, then the drop-down list is inactive.)
Specify Login for Oracle Internet Directory	Enter the Oracle Internet Directory superuser distinguished name (DN) in the **Username** field. The superuser DN `cn=orcladmin` is the default for this field; change this value if the Oracle Internet Directory superuser DN is not `cn=orcladmin`. Enter the password for the superuser DN in the **Password** field.
Specify Infrastructure Database Connection	Enter `SYS` in the **Username** field and the `SYS` user's password in the **Password** field.

Table B–2 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Cold Failover Cluster Infrastructure Upgrade

Screen	Description and Recommended Options to Select
Warning dialog box	This dialog box warns you that all the clients of the OracleAS Metadata Repository database must now be stopped. Oracle Universal Installer will automatically stop any clients within the current Oracle home.[1] However, you must manually stop any database clients and OracleAS Metadata Repository clients that reside in another Oracle home. Clients of the OracleAS Metadata Repository include: ■ OracleAS Identity Management components that use this OracleAS Metadata Repository. ■ Middle tier instances that use this OracleAS Metadata Repository Within each middle tier that uses this OracleAS Metadata Repository, you must be sure to stop all components, including Oracle HTTP Server and OracleAS Web Cache. For more information, see the chapter "Starting and Stopping " in the *Oracle Application Server Administrator's Guide*.
Database Listener Warning Dialog Box	If a database listener is running on the host, a warning dialog box displays. Review the dialog box determine whether or not you need to stop the listener manually. For more information, see Section 6.3.1.3, "Stopping the Database Listener When Prompted During the OracleAS Identity Management Upgrade".
Specify Instance Name and ias_admin Password	Enter a name for the new Oracle Application Server 10*g* (10.1.4.0.1) instance and a password for the `ias_admin` Administrator account. You use the `ias_admin` password to log on to the Application Server Control Console to manage the Oracle Application Server instance. In general, the minimum length of the `ias_admin` password is five alphanumeric characters. At least one of the characters must be a number and the password cannot start with a number. For more information, see the section "The ias_admin User and Restrictions on its Password" in the *Oracle Application Server Installation Guide*.
Summary	Use this screen to confirm the choices you've made. Click **Install** to begin upgrading to the new 10*g* (10.1.4.0.1) Oracle home. A dialog box appears when the copying is complete. This dialog box prompts you to run a configuration script as the root user. Follow the instructions in the dialog box and click **OK** when script is finished.

Table B–2 (Cont.) Summary of the Oracle Universal Installer Screens During the OracleAS Cold Failover Cluster Infrastructure Upgrade

Screen	Description and Recommended Options to Select
The Configuration Assistants	After the initial software is installed, a set of configuration assistants automatically set up the components in the new 10*g* (10.1.4.0.1) Oracle home. Use this screen to follow the progress of each assistant and to identify any problems during this phase of the installation. **Notes:** ■ The Database Upgrade Assistant (DBUA) can take a significant amount of time to upgrade the database. For more information how long it takes to upgrade your database, see Section 4.2, "Planning for System Downtime". ■ While Database Upgrade Assistant is running, do not use the **Stop** button to interrupt the execution of Database Upgrade Assistant. If you press **Stop**, the underlying processes for Database Upgrade Assistant will continue to run. Also, Oracle Universal Installer will wait until those processes complete before returning control to the user.
End of Installation	When the installation and upgrade is complete, this screen provides important details about the 10*g* (10.1.4.0.1) Oracle home, such as the URL for the Application Server Control Console and the location of the `setupinfo.txt` file. After you review the information on this screen, you can exit Oracle Universal Installer and proceed to the post-upgrade tasks.

[1] You can access a log of the automated shutdown procedure executed by Oracle Universal Installer in the following directory: `ORACLE_HOME/cfgtoollogs/shutdownprocesses.log`

B.3 Transforming 10*g* (9.0.4) Rack-Mounted Identity Management

The following sections describe how to transform a 10*g* (9.0.4) Rack-Mounted Identity Management environment to OracleAS Cluster (Identity Management):

- About Rack-Mounted Identity Management and OracleAS Cluster (Identity Management)
- Task 1: Review the Requirements for Transforming the 10g (9.0.4) Rackmounted Identity Management
- Task 2: Upgrade the Database That Hosts the OracleAS Metadata Repository
- Task 3: If Necessary, Upgrade Any Middle Tiers That Use the OracleAS Metadata Repository
- Task 4: Upgrade the First OracleAS Identity Management Instance
- Task 5: Use the Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository
- Task 6: Install Subsequent OracleAS Cluster (Identity Management) Instances
- Task 7: Verify the Upgrade and Decommission the 10g (9.0.4) Oracle Homes

B.3.1 About Rack-Mounted Identity Management and OracleAS Cluster (Identity Management)

Following the release of Oracle Application Server 10*g* (9.0.4), a procedure was released for deploying multiple Identity Management instances against one

Infrastructure Metadata Repository. This procedure was released in the form of a whitepaper titled *Highly Available Identity Management example - Rack Mounted Identity Management* and it was made available to customers on the Oracle Technology Network (OTN) at:

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

Note that the link to the whitepaper on OTN might actually be shown as *Highly Available Identity Management Deployment Example - Multi-box Identity Management*.

Starting with the release of Oracle Application Server 10*g* Release 2 (10.1.2), an "out-of-the-box" Multiple Identity Management solution is now available. This configuration is known as OracleAS Cluster (Identity Management).

> **See Also:** "Installing in High Availability Environments: OracleAS Cluster (Identity Management)" in the *Oracle Application Server Installation Guide*

The following sections provide step-by-step instructions for customers who wish to upgrade their 10*g* (9.0.4) Multiple Identity Management deployment to an OracleAS Clusters (Identity Management) 10*g* (10.1.4.0.1) deployment.

The testing and steps provided in this document are based upon an OracleAS Identity Management implementation deployed on RedHat Linux 3.0. The steps provided in this document, however, apply to any Unix platform.

B.3.2 Task 1: Review the Requirements for Transforming the 10*g* (9.0.4) Rackmounted Identity Management

The following sections describe the requirements you must meet in order to transform your highly available environment from 10*g* (9.0.4) Rack-Mounted Identity Management to OracleAS Cluster (Identity Management):

- OracleAS Identity Management Configuration Requirements
- Requirements for Colocated Versus Distributed OracleAS Identity Management
- OracleAS Metadata Repository Storage Requirements
- OracleAS Cluster (Identity Management) Backup Requirements

B.3.2.1 OracleAS Identity Management Configuration Requirements

Before you use this procedure, you must consider the following configuration requirements:

- You must have followed the exact set of steps outlined in the paper *Highly Available Identity Management example - Rack Mounted Identity Management*
- The Identity Management instances you are upgrading must be 10*g* (9.0.4) intances; previous releases of OracleAS are not supported for this configuration.
- The Metadata Repository must have been created in an Oracle9*i* Release 2 (9.2.0.1) or greater database, using the 10*g* (9.0.4) OracleAS RepCA (MRCA).

B.3.2.2 Requirements for Colocated Versus Distributed OracleAS Identity Management

OracleAS Identity Management consists of components that can also be installed separately:

- Oracle Internet Directory (OID)
- OracleAS Single Sign-On (SSO)
- Oracle Delegated Administration Services (DAS)
- Oracle Directory Integration Platform (DIP)

This procedure does not include support for Oracle Application Server Certificate Authority (OCA).

In this procedure, the primary focus is on installations where all Identity management components are installed in one Oracle home. This is known as a **colocated** OracleAS Infrastructure, which includes Oracle Internet Directory, Oracle Delegated Administration Services, and OracleAS Single Sign-On, all installed within the same Oracle home.

To upgrade a distributed OracleAS Identity Management configuration where the Identity Management components are separated into two tiers, see Section B.4, "Transforming a Distributed 10g (9.0.4) Rack-Mounted Identity Management Environment". Such a configuration might be required, for example, where an organization needs the OracleAS Single Sign-On and Oracle Delegated Administration Services components running in a the DMZ and the Oracle Internet Directory running on the internal network inside the firewall.

B.3.2.3 OracleAS Metadata Repository Storage Requirements

This procedure assumes the database that hosts the OracleAS Metadata Repository is an Oracle Real Application Clusters (RAC) Database. Specifically, the procedure described in this section was tested on a two-node RAC environment. However, it is assumed that this procedure also applies to:

- A single-instance database
- A Real Application Clusters database consisting of more than two nodes

The requirement for Real Application Clusters is a shared-storage configuration. The implementation of the shared volume is vendor-specific. The procedures in this section should be applicable to all Operating systems and clusters but were developed and tested in a Linux environment. Specifically, the following shared storage options are supported:

- Raw devices
- Cluster filesystem (for example, OCFS on Linux)
- Network filesystem (for example, supported NAS devices)

Although cluster and volume management software is vendor-specific, the steps and considerations provided in this section apply specifically to customers wishing to optionally implement Oracle's Automated Storage Management (ASM).

B.3.2.4 OracleAS Cluster (Identity Management) Backup Requirements

Before you begin this transformation procedure, take a complete, full software backup of everything in the Oracle Home and related directories for the OracleAS Metadata Repository and the OracleAS Identity Management instances.

In addition, shut down all processes and perform a full cold database backup of the middle tiers and Infrastructure Oracle homes.

B.3.3 Task 2: Upgrade the Database That Hosts the OracleAS Metadata Repository

Before you can upgrade to OracleAS Cluster (Identity Management), you must upgrade the database that hosts the OracleAS Metadata Repository to a supported database.

For detailed instructions on upgrading the database that hosts the OracleAS Metadata Repository, see Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository".

> **Note:** When applying database patchsets, be sure to carefully review the patchset README for your specific platform. The instructions for installing patchsets can vary significantly from platform to platform. For example, some platforms, such as Linux, might require you to install a specific version of Oracle Universal Installer before proceeding with the patchset installation.

B.3.4 Task 3: If Necessary, Upgrade Any Middle Tiers That Use the OracleAS Metadata Repository

There are certain upgrade scenarios where you might have to upgrade any 10*g* (9.0.4) middle tiers in your Oracle Application Server environment to 10*g* Release 2 (10.1.2).

For more information, refer to Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)".

B.3.5 Task 4: Upgrade the First OracleAS Identity Management Instance

After the database that hosts the OracleAS Metadata Repository has been upgraded to a supported version, and after any middle tiers have been upgraded to 10*g* Release 2 (10.1.2), you can now upgrade the first OracleAS Identity Management Oracle home in the Rack-Mounted Identity Management configuration.

When you upgrade the first OracleAS Identity Management Oracle home, you also upgrade the OracleAS Identity Management schemas in the OracleAS Metadata Repository.

Note that in an OracleAS Cluster (Identity Management), the Identity Management instances are clustered together in a Distributed Configuration Management (DCM) Cluster. This ensures synchronization between the configurations of the different Identity Management components on all of the Identity Management instances.

To upgrade the first OracleAS Identity Management Oracle home, use the following steps.

1. Make sure that the other OracleAS Identity Management Instances in the Rack-Mounted Identity Management environment are down.

   Only the OracleAS Identity Management instance that you are upgrading first should be up and running. If necessary, shut down the other OracleAS Identity Management instances.

2. Configure the Load Balancer to direct traffic only to the OracleAS Identity Management instance you are about to upgrade

   All Requests should be directed only to the OracleAS Identity Management instance you are about to upgrade. The other OracleAS Identity Management instances in the Rack-Mounted Identity Management environment should be shut down.

3. Use the Oracle Application Server 10*g* (10.1.4.0.1) installation procedure to upgrade the OracleAS Identity Management instance.

   Refer to Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management" for complete instructions on upgrading the first OracleAS Identity Management Oracle home.

4. Perform any post-upgrade procedures that apply to your OracleAS Identity Management environment.

   Refer to Chapter 9, "Component-Specific Post-Upgrade Procedures" for more information.

5. Perform the steps described in Section B.5.4.3.3, "Configuration Steps When Oracle HTTP Server and the Load Balancer are Not Using SSL".

6. Create a Distributed Configuration Management (DCM) cluster that the other OracleAS Identity Management instances can join:

   a. Enter the DCM command-line shell:

   ```
   ORACLE_HOME/dcm/bin/dcmctl shell
   ```

   b. Create a new Cluster:

   ```
   DCM> createcluster -cl IMcluster
   ```

   In this example, *IMCluster* is the name you assign to the cluster.

   c. Join the DCM cluster as the first instance:

   ```
   DCM> joincluster -cl IMcluster
   ```

   At this point the instance will be stopped.

   d. Restart the instance:

   ```
   opmnctl startall
   ```

   A new cluster has now been created with the upgraded IM instance as its sole member.

7. Perform the steps described in Section B.5.4.4, "Task 4d: Finish the Upgrade of the First OracleAS Identity Management Instance".

B.3.6 Task 5: Use the Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository

1. Make sure that the OracleAS Identity Management instance (including Oracle Internet Directory) that you upgraded in Section B.3.5, "Task 4: Upgrade the First OracleAS Identity Management Instance" is up and running.

   If it is not running, start the Identity Management instance (including Oracle Internet Directory) as follows:

   ```
   ORACLE_HOME/opmn/bin/opmnctl startall
   ```

2. Upgrade the Metadata Repository in the newly upgraded database as described in Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository", with the following exception:

   On the MRUA command line, enter the address of the load balancer in place of the `oid_host` and `oid_ssl_port` arguments.

Note that the values you enter for the `-oid_host` argument and `-oid_ssl_port` arguments must match the value of the corresponding properties defined in following configuration file in the Identity Management Oracle home:

```
IDENTITY_MANAGEMENT_HOME/config/ias.properties
```

For example:

```
OIDhost=sys42.acme.com
OIDsslport=636
```

3. When MRUA finishes processing, verify that the schemas have been upgraded, as described in Section 8.3, "Task 3: Verify the Success of the OracleAS Metadata Repository Upgrade".
4. Complete the OracleAS Metadata Repository upgrade using the instructions in the section, Section 9.4, "Task 4: Perform OracleAS Portal Post-Upgrade Steps".

B.3.7 Task 6: Install Subsequent OracleAS Cluster (Identity Management) Instances

After you upgrade the first OracleAS Identity Management instance in the cluster, and after you upgrade the OracleAS Metadata Repository, you can then install the additional OracleAS Identity Management instances in the OracleAS Cluster (Identity Management):

1. Make sure that the Oracle Internet Directory is up and running on the first OracleAS Identity Management instance.
2. Make sure that the OracleAS Metadata Repository database and listener are up and running.
3. Make sure that the Load Balancer is configured to direct traffic only to the first Identity Management instance.
4. Install the new 10*g* (10.1.4.0.1) OracleAS Identity Management Oracle home by following the instructions in the section "Installing OracleAS Cluster (Identity Management) on Subsequent Nodes," in the *Oracle Application Server Installation Guide*.
5. Reconfigure Load Balancer and test the installation.

   After a successful installation of the subsequent OracleAS Identity Management Oracle home, configure the Load Balancer to route requests to the new instance.
6. Repeat this procedure for any additional and subsequent OracleAS Identity Management installations that will be part of the cluster.

B.3.8 Task 7: Verify the Upgrade and Decommission the 10*g* (9.0.4) Oracle Homes

After you have upgraded the first Oracle Identity Management instance in the cluster and you have added the remaining cluster members, you can then verify that the upgrade was successful and then decommission the 10*g* (9.0.4) Oracle homes.

For more information, refer to Chapter 10, "Verifying the Upgrade and Decommissioning the Source Oracle Homes".

B.4 Transforming a Distributed 10*g* (9.0.4) Rack-Mounted Identity Management Environment

In a distributed Rack-Mounted Identity Management environment, the Oracle Internet Directory is installed in a separate Oracle home from the other OracleAS Identity Management components.

The procedure for transforming distributed Rack-Mounted Identity Management components is the same as that for transforming a colocated Rack-Mounted Identity Management installation, except for the following exceptions. The following steps summarize the distributed transformation procedure:

Table B–3 Summary of the Steps for Transforming a Distributed Rack-Mounted Identity Management Environment to OracleAS Cluster (Identity Management)

Task No.	Description	More Information
1	Review the requirements for transforming Rack-Mounted Identity Management.	Section B.3.2, "Task 1: Review the Requirements for Transforming the 10g (9.0.4) Rackmounted Identity Management"
2	Upgrade the database that hosts the OracleAS Metadata Repository.	Section B.3.3, "Task 2: Upgrade the Database That Hosts the OracleAS Metadata Repository"
3	If necessary, upgrade any 10*g* (9.0.4) middle tiers.	Section B.3.4, "Task 3: If Necessary, Upgrade Any Middle Tiers That Use the OracleAS Metadata Repository"
4	Upgrade the first Oracle Internet Directory Oracle home.	Steps 1 through 4 of Section B.3.5, "Task 4: Upgrade the First OracleAS Identity Management Instance"
5	Upgrade the first OracleAS Single Sign-On Oracle home.	Steps 1 through 4 of Section B.6.5, "Task 5: Upgrade the First OracleAS Single Sign-On Oracle Home"
6	Create a Distributed Configuration Management (DCM) cluster for the OracleAS Single Sign-On instances.	Step 6 of Section B.3.5, "Task 4: Upgrade the First OracleAS Identity Management Instance".
7	Configure Oracle HTTP Server and OracleAS Single Sign-On in the OracleAS Single Sign-On Oracle home.	Section B.5.4.3.3, "Configuration Steps When Oracle HTTP Server and the Load Balancer are Not Using SSL"
8	Finish the upgrade of the first OracleAS Single Sign-On instance.	Section B.5.4.4, "Task 4d: Finish the Upgrade of the First OracleAS Identity Management Instance"
9	Use the Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository	Section B.3.6, "Task 5: Use the Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository"
10	Install Subsequent OracleAS Cluster (Identity Management) Instances	Section B.3.7, "Task 6: Install Subsequent OracleAS Cluster (Identity Management) Instances"
11	Verify the Upgrade and Decommission the 10g (9.0.4) Oracle Homes	Section B.3.8, "Task 7: Verify the Upgrade and Decommission the 10g (9.0.4) Oracle Homes"

B.5 Upgrading an OracleAS Cluster (Identity Management) 10*g* Release 2 (10.1.2) Colocated Configuration

A colocated OracleAS Identity Management installation includes all the OracleAS Identity Management components in each Oracle home. Compare the procedures in this section with those in Section B.6, "Upgrading an OracleAS Cluster (Identity Management) 10g Release 2 (10.1.2) Distributed Configuration".

The following sections describe how to upgrade a colocated 10*g* Release 2 (10.1.2) OracleAS Cluster (Identity Management) environment to 10*g* (10.1.4.0.1).

- Task 1: Review the OracleAS Cluster (Identity Management) Upgrade Requirements
- Task 2: Upgrade the Database That Hosts the OracleAS Metadata Repository
- Task 3: If Necessary, Upgrade any 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2.0.2)
- Task 4: Upgrade the First OracleAS Identity Management Instance
- Task 5: Using Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository
- Task 6: Installing Subsequent OracleAS Cluster (Identity Management) Instances
- Task 7: Verify the Upgrade and Decommission the 10g Release 2 (10.1.2) Oracle Homes

B.5.1 Task 1: Review the OracleAS Cluster (Identity Management) Upgrade Requirements

The following sections describe the requirements you must meet in order to upgrade your 10*g* Release 2 (10.1.2) colocated OracleAS Cluster (Identity Management) configuration to OracleAS Cluster (Identity Management) 10*g* (10.1.4.0.1):

- OracleAS Identity Management Configuration Requirements
- Requirements for Colocated Versus Distributed OracleAS Identity Management
- OracleAS Metadata Repository Storage Requirements
- OracleAS Cluster (Identity Management) Backup Requirements

B.5.1.1 OracleAS Identity Management Configuration Requirements

Before you use this procedure, note that the Identity Management instances you are upgrading must be 10*g* Release 2 (10.1.2) intances that were installed using the procedures documented in "Installing in High Availability Environments: OracleAS Cluster (Identity Management)" in the 10*g* Release 2 (10.1.2) *Oracle Application Server Installation Guide*.

B.5.1.2 Requirements for Upgrading a Colocated OracleAS Cluster (Identity Management) Configuration

OracleAS Identity Management consists of components that can also be installed separately:

- Oracle Internet Directory (OID)
- OracleAS Single Sign-On (SSO)
- Oracle Delegated Administration Services (DAS)

- Oracle Directory Integration Platform (DIP)

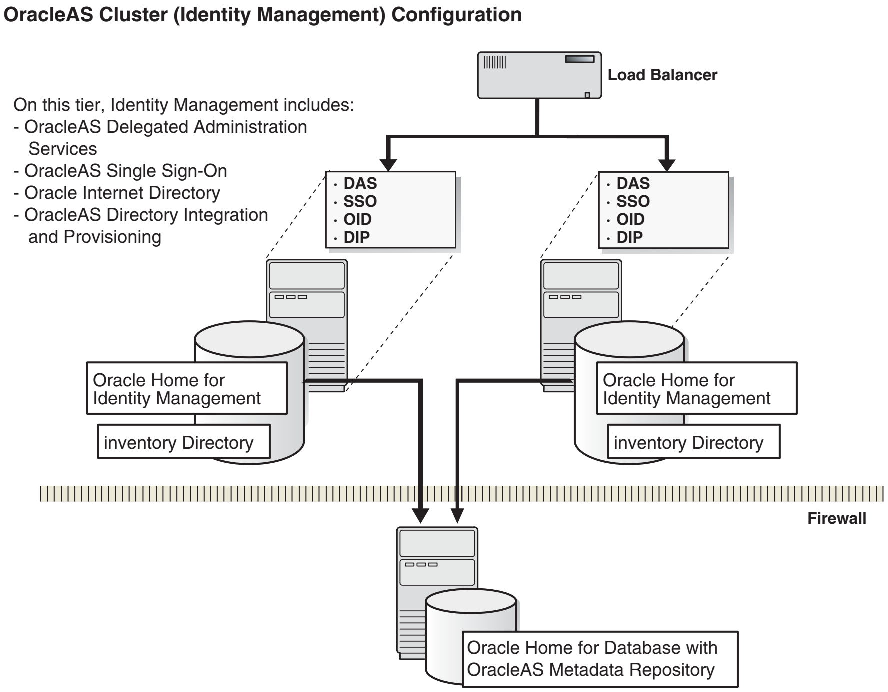
This procedure does not include support for Oracle Application Server Certificate Authority (OCA).

This procedure describes how to upgrade installations where all Identity management components are installed in each Oracle home. This is known as a **colocated** OracleAS Infrastructure, where Oracle Internet Directory, Oracle Delegated Administration Services, Oracle Directory Integration Platform, and OracleAS Single Sign-On are installed within the same Oracle home.

> **See Also:** Section B.6, "Upgrading an OracleAS Cluster (Identity Management) 10g Release 2 (10.1.2) Distributed Configuration" for information about upgrading a **distributed** OracleAS Identity Management configuration.

Figure B–1 shows a typical colocated OracleAS Cluster (Identity Management) 10*g* Release 2 (10.1.2) environment.

Figure B–1 10g Release 2 (10.1.2) Colocated OracleAS Cluster (Identity Management) Upgrade Starting Point


OracleAS Cluster (Identity Management) Configuration
Load Balancer
On this tier, Identity Management includes:
- OracleAS Delegated Administration Services
- OracleAS Single Sign-On
- Oracle Internet Directory
- OracleAS Directory Integration and Provisioning
· DAS
· SSO
· OID
· DIP
· DAS
· SSO
· OID
· DIP
Oracle Home for Identity Management
inventory Directory
Oracle Home for Identity Management
inventory Directory
Firewall
Oracle Home for Database with OracleAS Metadata Repository

B.5.1.3 OracleAS Cluster (Identity Management) Backup Requirements

Before you begin this procedure, perform a complete, full software backup of everything in the Oracle Home and related directories for the OracleAS Metadata Repository and the OracleAS Identity Management instances.

In addition, shut down all processes and perform a full cold database backup of the middle tiers and Infrastructure Oracle homes.

B.5.2 Task 2: Upgrade the Database That Hosts the OracleAS Metadata Repository

Before you can upgrade to OracleAS Cluster (Identity Management), you must upgrade the database that hosts the OracleAS Metadata Repository to a supported database.

For detailed instructions on upgrading the database that hosts the OracleAS Metadata Repository, see Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository".

> **Note:** When applying database patchsets, be sure to carefully review the patchset README for your specific platform. The instructions for installing patchsets can vary significantly from platform to platform. For example, some platforms, such as Linux, might require you to install a specific version of Oracle Universal Installer before proceeding with the patschset installation.

B.5.3 Task 3: If Necessary, Upgrade any 10*g* (9.0.4) Middle Tiers to 10*g* Release 2 (10.1.2.0.2)

There are certain upgrade scenarios where you might have to upgrade any 10*g* (9.0.4) middle tiers in your Oracle Application Server environment to 10*g* Release 2 (10.1.2).

For more information, refer to Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)".

B.5.4 Task 4: Upgrade the First OracleAS Identity Management Instance

After the database that hosts the OracleAS Metadata Repository has been upgraded to a supported version, and after any middle tiers have been upgraded to 10*g* Release 2 (10.1.2), you can now upgrade the first OracleAS Identity Management Oracle home in the OracleAS Cluster (Identity Management) configuration.

When you upgrade the first OracleAS Identity Management Oracle home, you also upgrade the OracleAS Identity Management schemas in the OracleAS Metadata Repository.

Note that in a colocated OracleAS Cluster (Identity Management), all the OracleAS Identity Management instances are clustered in a Distributed Configuration Management (DCM) Cluster. This ensures synchronization between the configurations of the different Identity Management components on all of the Identity Management instances.

To upgrade the first OracleAS Identity Management Oracle home, refer to the following sections:

- Task 4a: Prepare For and Perform the Upgrade
- Task 4b: Reconfigure the DCM Cluster
- Task 4c: Configure Oracle HTTP Server and OracleAS Single Sign-On
- Task 4d: Finish the Upgrade of the First OracleAS Identity Management Instance

B.5.4.1 Task 4a: Prepare For and Perform the Upgrade

Use the following steps to upgrade the first OracleAS Identity Management instance in the OracleAS Cluster (Identity Management) environment:

1. Make sure that the other OracleAS Identity Management Instances in the environment are down.

   Only the OracleAS Identity Management instance that you are upgrading first should be up and running. If necessary, shut down the other OracleAS Identity Management instances.

2. Configure the Load Balancer to direct traffic only to the OracleAS Identity Management instance you are about to upgrade.

   All Requests should be directed only to the OracleAS Identity Management instance you are about to upgrade. The other OracleAS Identity Management instances in the environment should be shut down.

3. Use the Oracle Universal Installer and the Oracle Application Server 10*g* (10.1.4.0.1) installation procedure to upgrade the OracleAS Identity Management instance.

   Refer to Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management" for complete instructions on upgrading the first OracleAS Identity Management instance.

4. Perform any post-upgrade procedures that apply to the Oracle Internet Directory Oracle home.

   Refer to Section 9.2, "Task 2: Perform Oracle Internet Directory Post-Upgrade Steps" for more information.

B.5.4.2 Task 4b: Reconfigure the DCM Cluster

Use the following steps to reconfigure the cluster and to prepare for installing the remaining OracleAS Identity Management instances:

1. Remove the OracleAS Identity Management 10*g* Release 2 (10.1.2) instances from the cluster:

   a. Start the Distributed Configuration Management (DCM) shell:

   ```
   DESTINATION_ORACLE_HOME/dcm/bin/dcmctl shell
   ```

   b. Display a list of the currently defined clusters:

   ```
   DCM> listclusters
   ```

   c. Note the name of the OracleAS Cluster (Identity Management) and then list the OracleAS Identity Management instances that are members of the cluster:

   ```
   DCM> listInstances -cl name_of_Identity_Management_cluster
   ```

   d. For each OracleAS Identity Management instance in the cluster, enter the following command:

   ```
   DCM> leavecluster -i 1012_instance_name
   ```

2. Add the newly upgraded Oracle Identity Management 10*g* (10.1.4.0.1) instance to the cluster:

   a. Join the cluster using the following command:

   ```
   DCM> joincluster -cl name_of_Identity_Management_cluster
   ```

   Note that the `joincluster` command stops the 10*g* (10.1.4.0.1) instance and all of its processes.

   b. Start the Oracle Identity Management 10*g* (10.1.4.0.1) instance:

   ```
   DESTINATION_ORACLE_HOME/opmn/bin/opmnctl stopall
   DESTINATION_ORACLE_HOME/opmn/bin/opmnctl startall
   ```

B.5.4.3 Task 4c: Configure Oracle HTTP Server and OracleAS Single Sign-On

Use the following steps to configure Oracle HTTP Server, OracleAS Single Sign-On, and OPMN after you have upgraded the first OracleAS Identity Management instance.

The steps you follow to configure these components vary, depending upon whether or not you have configured Oracle HTTP Server or your load balancer to accept HTTPS requests.

Refer to the following sections for more information:

- Configuration Steps When Both Oracle HTTP Server and the Load Balancer Are Configured for SSL
- Configuration Steps When Only the Load Balancer Is Configured for SSL
- Configuration Steps When Oracle HTTP Server and the Load Balancer are Not Using SSL

B.5.4.3.1 Configuration Steps When Both Oracle HTTP Server and the Load Balancer Are Configured for SSL The following steps apply if both the Oracle HTTP Server and the load balancer are configured to listen for the HTTPS protocol;

1. Configure the Oracle HTTP Server listener as follows:

   a. Edit the following Oracle HTTP Server configuration file:

   ```
   DESTINATION_ORACLE_HOME/Apache/Apache/conf/ssl.conf
   ```

   b. Make sure that the `ServerName` directive is set to the virtual host (for example, `imhost.domain.com`) and not to the physical host.

   c. Save and close the ssl.conf configuration file.

   d. Update DCM to recognize the changes made to the Oracle HTTP Server component using the following command:

   ```
   DESTINATION_ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct ohs -d -v
   ```

2. Configure OracleAS Single Sign-On to accept authentication requests on the SSL port over the HTTPS protocol by using the following command:

   ```
   ORACLE_HOME/sso/bin/ssocfg.sh https imhost.domain.com 4444
   ```

   In this example:

   - *imhost.domain.com* is the address configured at the load balancer for HTTPS requests.
   - The default HTTPS Listener port is `4444`, but this port may differ for your specific installation. You can obtain the correct value for your installation by examining the assigned to the "port" variable in the `ssl.conf` configuration file.

3. Edit the OPMN configuration file to enable SSL for the Oracle HTTP Server:

   a. Locate and open the following OPMN configuration file with a text editor:

   ```
   DESTINATION_ORACLE_HOME/opmn/conf/opmn.xml
   ```

b. Locate the following entry for the `HTTP_Server` component:

```
<ias-component id="HTTP_Server">
   <process-type id="HTTP_Server" module-id="OHS">
      <module-data>
         <category id="start-parameters">
             <data id="start-mode" value="ssl-disabled"/>
         </category>
      </module-data>
      <process-set id="HTTP_Server" numprocs="1"/>
   </process-type>
</ias-component>
```

c. Change the value of the `start-mode` entry to `ssl-enabled`.

The resulting entry in the opmn.xml file should appear as follows:

```
<ias-component id="HTTP_Server">
   <process-type id="HTTP_Server" module-id="OHS">
      <module-data>
         <category id="start-parameters">
             <data id="start-mode" value="ssl-enabled"/>
         </category>
      </module-data>
      <process-set id="HTTP_Server" numprocs="1"/>
   </process-type>
</ias-component>
```

4. Re-register the instance with OracleAS Single Sign-On:

Run the following command to re-register the instance with OracleAS Single Sign-On:

```
ORACLE_HOME/sso/bin/ssoreg.sh
    -oracle_home_path orcl_home_path
    -site_name instance_name_you_specified_during_upgrade
    -config_mod_osso TRUE
    -mod_osso_url effective_URL_of_the_partner_application
    -u userid
```

In this example:

- The *effective_URL_of_the_partner_application* is in this URL format:

  ```
  http://virtual_servername:ssl_port
  ```

- Replace *userid* with the Oracle owner.

Note that at this point in the procedure, the upgraded OracleAS Identity Management Oracle home should be a fully working 10*g* (10.1.4.0.1) OracleAS Identity Management instance running against the OracleAS Metadata Repository database. The load balancer is still pointing to only this new, upgraded instance.

5. Change the Oracle Delegated Administration Services `orcldasurlbase` attribute in the directory server, using the following steps:

a. Start Oracle Directory Manager (`oidadmin)` and connect to the Oracle Internet Directory.

The `oidadmin` tool is located in the following directory in the destination Oracle home:

```
DESTINATION_ORACLE_HOME/bin/
```

Make sure you select the **SSL Enabled** check box when connecting to the directory server.

b. In the System Objects Navigator, navigate to the `cn=OperationURLs` entry as follows:

```
Entry Management ->
  cn=OracleContext ->
     cn=Products ->
        cn=DAS ->
           cn=OperationURLs
```

c. After you select the `cn=OperationURLs` entry, locate the orcldasurl attribute on the Properties tab in the right pane of the Oracle Directory Manager window.

d. Change the `orcldasurlbase` attribute so it references the SSL URL for the Oracle Delegated Administration Services:

```
https://virtual_server_name:load_balancer_ssl_listen_port
```

B.5.4.3.2 Configuration Steps When Only the Load Balancer Is Configured for SSL The following steps apply if both the Oracle HTTP Server and the load balancer are configured to listen for the HTTPS protocol:

1. Configure the Oracle HTTP Server listener as follows:

   a. Use a text editor to locate and open the following Oracle HTTP Server configuration file:

   ```
   DESTINATION_ORACLE_HOME/Apache/Apache/conf/httpd.conf
   ```

   b. Make sure that the `ServerName` directive is set to the virtual host (for example, `imhost.domain.com`) and not to the physical host.

   c. Save and close the `httpd.conf` configuration file.

   d. Update DCM to recognize the changes made to the Oracle HTTP Server component using the following command:

   ```
   DESTINATION_ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct ohs -d -v
   ```

2. Configure OracleAS Single Sign-On to accept authentication requests on the SSL port over the HTTPS protocol by using the following command:

   ```
   ORACLE_HOME/sso/bin/ssocfg.sh https imhost.domain.com 4444
   ```

   In this example:

   - *imhost.domain.com* is the virtual host address configured at the load balancer for HTTPS requests.
   - The default HTTPS Listener port is `4444`, but this port may differ for your specific installation. You can obtain the correct value for your installation by examining the assigned to the "port" variable in the `ssl.conf` configuration file.

3. Re-register the instance with OracleAS Single Sign-On:

   Run the following command to re-register the instance with OracleAS Single Sign-On:

   ```
   ORACLE_HOME/sso/bin/ssoreg.sh
       -oracle_home_path orcl_home_path
       -site_name instance_name_you_specified_during_upgrade
   ```

```
-config_mod_osso TRUE
-mod_osso_url effective_URL_of_the_partner_application
-u userid
```

In this example:

- The *effective_URL_of_the_partner_application* is in this URL format:

  ```
  http://virtual_servername:load_blancer_ssl_port
  ```

- Replace *userid* with the Oracle owner.

Note that at this point in the procedure, the upgraded OracleAS Identity Management Oracle home should be a fully working 10*g* (10.1.4.0.1) OracleAS Identity Management instance running against the OracleAS Metadata Repository database. The load balancer is still pointing to only this new, upgraded instance.

4. Change the Oracle Delegated Administration Services `orcldasurlbase` attribute in the directory server, using the following steps:

   a. Start Oracle Directory Manager (`oidadmin)` and connect to the Oracle Internet Directory.

      The `oidadmin` tool is located in the following directory in the destination Oracle home:

      ```
      DESTINATION_ORACLE_HOME/bin/
      ```

      Make sure you select the **SSL Enabled** check box when connecting to the directory server.

   b. In the System Objects Navigator, navigate to the `cn=OperationURLs` entry as follows:

      ```
      Entry Management ->
        cn=OracleContext ->
           cn=Products ->
              cn=DAS ->
                 cn=OperationURLs
      ```

   c. After you select the `cn=OperationURLs` entry, locate the orcldasurl attribute on the Properties tab in the right pane of the Oracle Directory Manager window.

   d. Change the `orcldasurlbase` attribute so it references the SSL URL for the Oracle Delegated Administration Services:

      ```
      https://virtual_server_name:load_balancer_ssl_listen_port
      ```

B.5.4.3.3 Configuration Steps When Oracle HTTP Server and the Load Balancer are Not Using SSL The following steps apply if both the Oracle HTTP Server and the load balancer are configured to listen for the HTTPS protocol;

1. Configure the Oracle HTTP Server listener as follows:

   a. Use a text editor to locate and open the following Oracle HTTP Server configuration file:

      ```
      DESTINATION_ORACLE_HOME/Apache/Apache/conf/httpd.conf
      ```

   b. Make sure that the `ServerName` directive is set to the virtual host (for example, `imhost.domain.com`) and not to the physical host.

   c. Save and close the `httpd.conf` configuration file.

d. Update DCM to recognize the changes made to the Oracle HTTP Server component using the following command:

```
DESTINATION_ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct ohs -d -v
```

2. Configure OracleAS Single Sign-On to accept authentication requests on the SSL port over the HTTPS protocol by using the following command:

```
ORACLE_HOME/sso/bin/ssocfg.sh http imhost.domain.com 7777
```

In this example:

- *imhost.domain.com* is the address configured at the load balancer for HTTP requests.
- The default HTTP Listener port is `7777`, but this port may differ for your specific installation. You can obtain the correct value for your installation by examining the assigned to the "port" variable in the `httpd.conf` configuration file.

3. Re-register the instance with OracleAS Single Sign-On:

Run the following command to re-register the instance with OracleAS Single Sign-On:

```
ORACLE_HOME/sso/bin/ssoreg.sh
    -oracle_home_path orcl_home_path
    -site_name instance_name_you_specified_during_upgrade
    -config_mod_osso TRUE
    -mod_osso_url effective_URL_of_the_partner_application
    -u userid
```

In this example:

- The *effective_URL_of_the_partner_application* is in this URL format:

```
http://virtual_servername:load_balancer_port
```

- Replace *userid* with the Oracle owner.

Note that at this point in the procedure, the upgraded OracleAS Identity Management Oracle home should be a fully working 10*g* (10.1.4.0.1) OracleAS Identity Management instance running against the OracleAS Metadata Repository database. The load balancer is still pointing to only this new, upgraded instance.

4. Change the Oracle Delegated Administration Services `orcldasurlbase` attribute in the directory server, using the following steps:

a. Start Oracle Directory Manager (`oidadmin)` and connect to the Oracle Internet Directory.

The `oidadmin` tool is located in the following directory in the destination Oracle home:

```
DESTINATION_ORACLE_HOME/bin/
```

b. In the System Objects Navigator, navigate to the `cn=OperationURLs` entry as follows:

```
Entry Management ->
  cn=OracleContext ->
     cn=Products ->
        cn=DAS ->
           cn=OperationURLs
```

c. After you select the `cn=OperationURLs` entry, locate the orcldasurl attribute on the Properties tab in the right pane of the Oracle Directory Manager window.

d. Change the `orcldasurlbase` attribute so it references the URL for the Oracle Delegated Administration Services:

```
http://virtual_server_name:load_balancer_non_ssl_listen_port
```

B.5.4.4 Task 4d: Finish the Upgrade of the First OracleAS Identity Management Instance

Perform the following steps to finish the upgrade of the first OracleAS Identity Management instance in the OracleAS Cluster (Identity Management) environment:

1. Enable the monitoring of the instance by Oracle Enterprise Manager Application Server Control by following the instructions in Section 9.1.2.1, "Enabling Monitoring of OracleAS Single Sign-On and Oracle Delegated Administration Services in Application Server Control".

2. Update the `mod_oc4j` load balancing directive in the destination Oracle home:

   a. Locate and open the following configuration file with a text editor:

   ```
   DESTINATION_ORACLE_HOME/Apache/Apache/mod_oc4j.conf
   ```

   b. Within the `mod_oc4j.conf` file, add the following line before the `</IfModule>` element:

   ```
   Oc4jSelectMethod roundrobin:local
   ```

3. Update the DCM configuration:

   ```
   DESTINATION_ORACLE_HOME/dcm/bin/dcmctl updateConfig -d -v
   ```

   Note that using only the `-d` and `-v` arguments to the `dcmctl updateConfig` command updates all the component information for DCM. The command also stops some of the processes in the Oracle Identity Management Oracle home.

4. Stop and then start all the processes in the Oracle Identity Management Oracle home:

   ```
   DESTINATION_ORACLE_HOME/opmn/bin/opmnctl stopall
   DESTINATION_ORACLE_HOME/opmn/bin/opmnctl startall
   ```

5. To ensure that Oracle Application Server maintains the state of stateful Web applications across DCM-Managed OracleAS Cluster, you need to configure state replication for the Web applications.

   Configure state replication only on the first node where Oracle Delegated Administration Services is installed.

   To configure state replication for the OC4J_Security instance, do the following:

   1. Using the Application Server Control Console, navigate to the Application Server Home page for the instance that contains Oracle Delegated Administration Services.
   2. Click **OC4J_SECURITY** link on the Application Server Home page.
   3. Click **Administration** link on the OC4J Home Page.
   4. Click **Replication Properties** link in the Instance Properties area.

5. Scroll to the Web Applications section of the page (Figure B–2).
6. Select the **Replicate session state** checkbox.

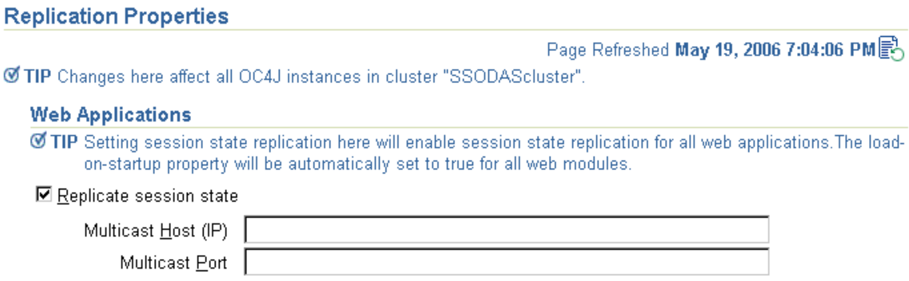
   Optionally, you can provide the multicast host IP address and port number. If you do not provide the host and port for the multicast address, it defaults to host IP address 230.230.0.1 and port number 9127. The host IP address must be between 224.0.0.2 through 239.255.255.255. Do not use the same multicast address for both HTTP and EJB multicast addresses.

   Note: When choosing a multicast address, ensure that the address does not collide with the addresses listed in:

   `http://www.iana.org/assignments/multicast-addresses`

   Also, if the low order 23 bits of an address is the same as the local network control block, `224.0.0.0 - 224.0.0.255`, then a collision may occur. To avoid this problem, provide an address that does not have the same bits in the lower 23 bits of the address as the addresses in this range.

Figure B–2 Web State Replication Configuration



Replication Properties

Page Refreshed **May 19, 2006 7:04:06 PM**

TIP Changes here affect all OC4J instances in cluster "SSODAScluster".

Web Applications

TIP Setting session state replication here will enable session state replication for all web applications.The load-on-startup property will be automatically set to true for all web modules.

☑ Replicate session state

Multicast Host (IP)

Multicast Port

B.5.5 Task 5: Using Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository

1. Make sure that the OracleAS Identity Management instance (including Oracle Internet Directory) that you upgraded in Section B.3.5, "Task 4: Upgrade the First OracleAS Identity Management Instance" is up and running.

   If it is not running, start the Identity Management instance (including Oracle Internet Directory) as follows:

   ```
   ORACLE_HOME/opmn/bin/opmnctl startall
   ```

2. Upgrade the Metadata Repository in the newly upgraded database as described in Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository", with the following exception:

   On the MRUA command line, enter the address of the load balancer in place of the `oid_host` and `oid_ssl_port` arguments.

   Note that the values you enter for the `-oid_host` argument and `-oid_ssl_port` arguments must match the value of the corresponding properties defined in following configuration file in the Identity Management Oracle home:

   ```
   IDENTITY_MANAGEMENT_HOME/config/ias.properties
   ```

For example:

```
OIDhost=sys42.acme.com
OIDsslport=636
```

3. When MRUA finishes processing, verify that the schemas have been upgraded, as described in Section 8.3, "Task 3: Verify the Success of the OracleAS Metadata Repository Upgrade".

B.5.6 Task 6: Installing Subsequent OracleAS Cluster (Identity Management) Instances

After you upgrade the first OracleAS Identity Management instance in the cluster, and after you upgrade the OracleAS Metadata Repository, you can then install the additional OracleAS Identity Management instances in the OracleAS Cluster (Identity Management):

1. Make sure that the Oracle Internet Directory is up and running on the first OracleAS Identity Management instance.
2. Make sure that the OracleAS Metadata Repository database and listener are up and running.
3. Make sure that the Load Balancer is configured to direct traffic only to the first Identity Management instance.
4. Install the new 10*g* (10.1.4.0.1) OracleAS Identity Management Oracle home by following the instructions in the section "Installing OracleAS Cluster (Identity Management) on Subsequent Nodes," in the *Oracle Application Server Installation Guide*.
5. Reconfigure Load Balancer and test the installation.

   After a successful installation of the subsequent OracleAS Identity Management Oracle home, configure the Load Balancer to route requests to the new instance.
6. Repeat this procedure for any additional and subsequent OracleAS Identity Management installations that will be part of the cluster.

B.5.7 Task 7: Verify the Upgrade and Decommission the 10*g* Release 2 (10.1.2) Oracle Homes

After you have upgraded the first Oracle Identity Management instance in the cluster and you have added the remaining cluster members, you can then verify that the upgrade was successful and then decommission the 10*g* Release 2 (10.1.2) Oracle homes.

For more information, refer to Chapter 10, "Verifying the Upgrade and Decommissioning the Source Oracle Homes".

B.6 Upgrading an OracleAS Cluster (Identity Management) 10*g* Release 2 (10.1.2) Distributed Configuration

The following sections describe how to upgrade from a distributed 10*g* Release 2 (10.1.2) OracleAS Cluster (Identity Management) environment to 10*g* (10.1.4.0.1):

- Task 1: Review the Distributed OracleAS Cluster (Identity Management) Upgrade Requirements
- Task 2: Upgrade the Database That Hosts the OracleAS Metadata Repository for the Distributed Environment

- Task 3: If Necessary, Upgrade Any 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2.0.2) in the Distributed Environment
- Task 4: Upgrade the First Oracle Internet Directory Oracle Home in the Distributed Environment
- Task 5: Upgrade the First OracleAS Single Sign-On Oracle Home
- Task 6: Using Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository
- Task 7: Installing Subsequent Oracle Internet Directory Instances
- Task 8: Installing Subsequent OracleAS Single Sign-On Instances
- Task 9: Verify the Upgrade and Decommission the 10g Release 2 (10.1.2) Oracle Homes

B.6.1 Task 1: Review the Distributed OracleAS Cluster (Identity Management) Upgrade Requirements

The following sections describe the requirements you must meet in order to upgrade from a 10*g* Release 2 (10.1.2) distributed OracleAS Cluster (Identity Management) configuration to a 10*g* (10.1.4.0.1) distributed OracleAS Cluster (Identity Management) configuration:

- OracleAS Identity Management Configuration Requirements
- Requirements for Colocated Versus Distributed OracleAS Identity Management
- OracleAS Metadata Repository Storage Requirements
- OracleAS Cluster (Identity Management) Backup Requirements

B.6.1.1 OracleAS Identity Management Configuration Requirements

Before you use this procedure, note that the Identity Management instances you are upgrading must be 10*g* Release 2 (10.1.2) intances that were installed using the procedures documented in "Installing in High Availability Environments: OracleAS Cluster (Identity Management)" in the 10*g* Release 2 (10.1.2) *Oracle Application Server Installation Guide*.

B.6.1.2 Requirements for Upgrading a Distributed OracleAS Cluster (Identity Management) Configuration

OracleAS Identity Management consists of components that can also be installed separately:

- Oracle Internet Directory (OID)
- OracleAS Single Sign-On (SSO)
- Oracle Delegated Administration Services (DAS)
- Oracle Directory Integration Platform (DIP)

This procedure does not include support for Oracle Application Server Certificate Authority (OCA).

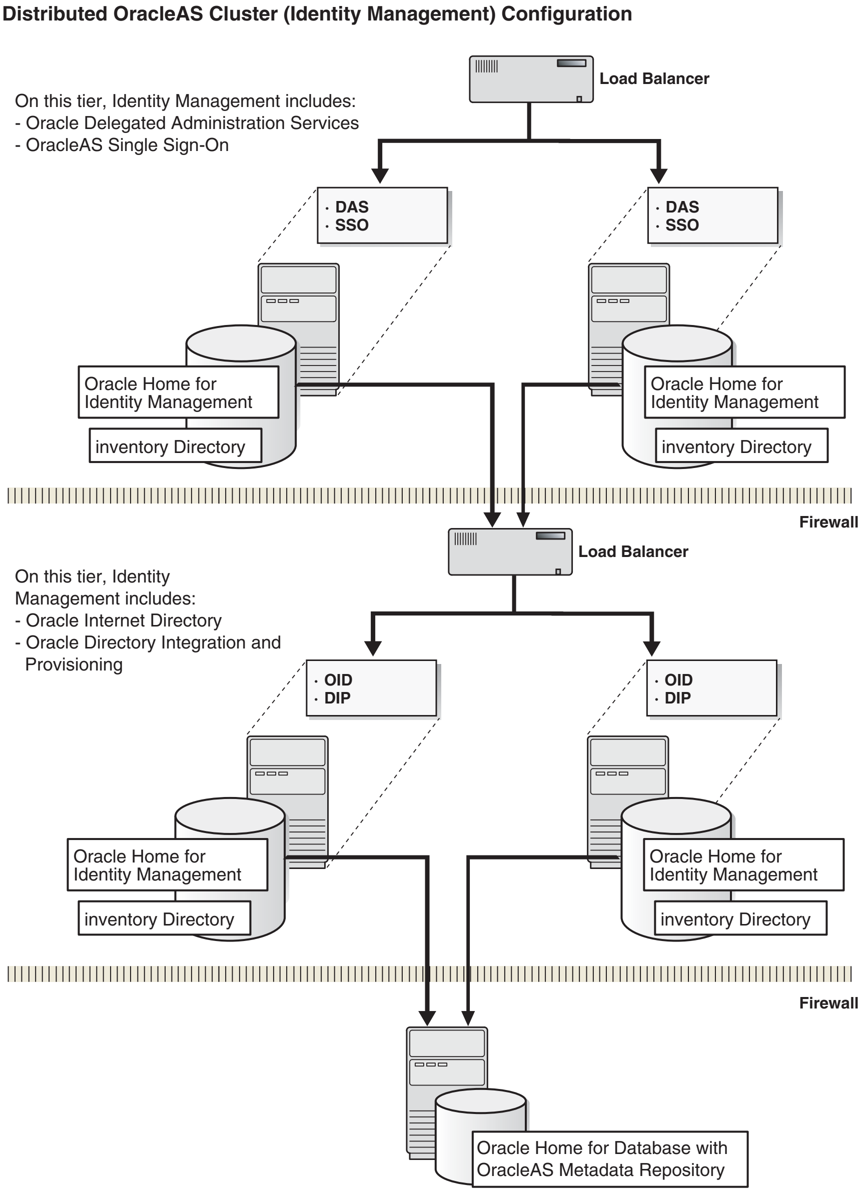
This procedure describes how to upgrade a **distributed** OracleAS Cluster (Identity Management) 10*g* Release 2 (10.1.2) installation, where the Identity Management components are separated into two tiers. One tier contains the Oracle Application Server Single Sign-On and Oracle Delegated Administration Services components and the second tier contains the Oracle Internet Directory and Oracle Directory Integration Platform components.

> **See Also:** Section B.5, "Upgrading an OracleAS Cluster (Identity Management) 10g Release 2 (10.1.2) Colocated Configuration" for information about upgrading a **colocated** OracleAS Identity Management configuration, where all Identity management components are installed in one Oracle home.

A distributed OracleAS Cluster (Identity Management) configuration allows administrators to install the OracleAS Single Sign-On and Oracle Delegated Administration Services components in a the DMZ and the Oracle Internet Directory on the internal network inside the firewall.

Figure B–3 shows such a distributed OracleAS Cluster (Identity Management) 10*g* Release 2 (10.1.2) environment.

Figure B–3 10g Release 2 (10.1.2) OracleAS Cluster (Identity Management) Distributed Upgrade Starting Point


Distributed OracleAS Cluster (Identity Management) Configuration
Load Balancer
On this tier, Identity Management includes:
- Oracle Delegated Administration Services
- OracleAS Single Sign-On
· DAS
· SSO
· DAS
· SSO
Oracle Home for Identity Management
inventory Directory
Oracle Home for Identity Management
inventory Directory
Firewall
Load Balancer
On this tier, Identity Management includes:
- Oracle Internet Directory
- Oracle Directory Integration and Provisioning
· OID
· DIP
· OID
· DIP
Oracle Home for Identity Management
inventory Directory
Oracle Home for Identity Management
inventory Directory
Firewall
Oracle Home for Database with OracleAS Metadata Repository

B.6.1.3 OracleAS Metadata Repository Storage Requirements

This procedure assumes the database that hosts the OracleAS Metadata Repository is an Oracle Real Application Clusters (RAC) Database. Specifically, the procedure described in this section was tested on a two-node RAC environment. However, it is assumed that this procedure also applies to:

- A single-instance database
- A Real Application Clusters database consisting of more than two nodes

The requirement for Real Application Clusters is a shared-storage configuration. The implementation of the shared volume is vendor-specific. The procedures in this section should be applicable to all Operating systems and clusters but were developed and tested in a Linux environment. Specifically, the following shared storage options are supported:

- Raw devices
- Cluster filesystem (for example, OCFS on Linux)
- Network filesystem (for example, supported NAS devices)

Although cluster and volume management software is vendor-specific, the steps and considerations provided in this section apply specifically to customers wishing to optionally implement Oracle's Automated Storage Management (ASM).

B.6.1.4 OracleAS Cluster (Identity Management) Backup Requirements

Before you begin this transformation procedure, take a complete, full software backup of everything in the Oracle Home and related directories for the OracleAS Metadata Repository and the OracleAS Identity Management instances.

In addition, shut down all processes and perform a full cold database backup of the middle tiers and Infrastructure Oracle homes.

B.6.2 Task 2: Upgrade the Database That Hosts the OracleAS Metadata Repository for the Distributed Environment

Before you can upgrade to OracleAS Cluster (Identity Management), you must upgrade the database that hosts the OracleAS Metadata Repository to a supported database.

For detailed instructions on upgrading the database that hosts the OracleAS Metadata Repository, see Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository".

Note: When applying database patchsets, be sure to carefully review the patchset README for your specific platform. The instructions for installing patchsets can vary significantly from platform to platform. For example, some platforms, such as Linux, might require you to install a specific version of Oracle Universal Installer before proceeding with the patschset installation.

B.6.3 Task 3: If Necessary, Upgrade Any 10*g* (9.0.4) Middle Tiers to 10*g* Release 2 (10.1.2.0.2) in the Distributed Environment

There are certain upgrade scenarios where you might have to upgrade any 10*g* (9.0.4) middle tiers in your Oracle Application Server environment to 10*g* Release 2 (10.1.2).

For more information, refer to Chapter 5, "Upgrading 10g (9.0.4) Middle Tiers to 10g Release 2 (10.1.2)".

B.6.4 Task 4: Upgrade the First Oracle Internet Directory Oracle Home in the Distributed Environment

After the database that hosts the OracleAS Metadata Repository has been upgraded to a supported version, and after any middle tiers have been upgraded to 10*g* Release 2 (10.1.2), you can now upgrade the first OracleAS Identity Management Oracle home in the Rack-Mounted Identity Management configuration.

When you upgrade the first OracleAS Identity Management Oracle home, you also upgrade the OracleAS Identity Management schemas in the OracleAS Metadata Repository.

Note that in a distributed OracleAS Cluster (Identity Management) configuration, the OracleAS Single Sign-On instances are clustered together in a Distributed Configuration Management (DCM) Cluster. This ensures synchronization between the configurations of the different Identity Management components on all of the Identity Management instances.

To upgrade the first Oracle Internet Directory Oracle home, use the following steps.

> **Note:** If you are upgrading a distributed OracleAS Cluster (Identity Management) environment, be sure that the first OracleAS Identity Management instance you upgrade represents one of the OracleAS Single Sign-On Oracle homes.

1. Make sure that the other OracleAS Identity Management Instances in the environment are down.

   Only the Oracle Internet Directory instance that you are upgrading first should be up and running. If necessary, shut down the other OracleAS Identity Management instances.

2. Configure the Oracle Internet Directory Load Balancer to direct traffic only to the OracleAS Identity Management instance you are about to upgrade.

   All Requests should be directed only to the Oracle Internet Directory instance you are about to upgrade. The other OracleAS Identity Management instances in the environment should be shut down.

3. Use the Oracle Universal Installer and the Oracle Application Server 10*g* (10.1.4.0.1) installation procedure to upgrade the Oracle Internet Directory instance.

   Refer to Section 7.5.3, "Upgrading Distributed OracleAS Identity Management Configurations" for complete instructions on upgrading the first Oracle Internet Directory instance.

4. Perform any post-upgrade procedures that apply to your OracleAS Identity Management environment.

   Refer to Section 9.2, "Task 2: Perform Oracle Internet Directory Post-Upgrade Steps" for more information.

B.6.5 Task 5: Upgrade the First OracleAS Single Sign-On Oracle Home

Follow the steps described in Table B–4 to upgrade the first OracleAS Single Sign-On Oracle home in the distributed OracleAS Cluster (Identity Management) 10*g* Release 2 (10.1.2) environment.

Table B–4 Steps Required to Upgrade the First OracleAS Single Sign-On Oracle Home in a Distributed OracleAS Cluster (Identity Management) Environment

Step	Description	More Information
1	Start the OracleAS Single Sign-On instance that you are about to upgrade.	Only the Oracle Internet Directory instance that you upgraded first and the current OracleAS Single Sign-On instance that you plan to upgrade next should be up and running. If necessary, shut down the other OracleAS Identity Management instances.

Table B–4 (Cont.) Steps Required to Upgrade the First OracleAS Single Sign-On Oracle Home in a Distributed OracleAS Cluster (Identity Management) Environment

Step	Description	More Information
2	Configure the OracleAS Single Sign-On Load Balancer to direct traffic only to the OracleAS Identity Management instance you are about to upgrade.	All requests should be directed only to the OracleAS Single Sign-On instance you are about to upgrade. The other OracleAS Single Sign-On instances in the environment should be shut down.
3	Use the Oracle Universal Installer and the Oracle Application Server 10*g* (10.1.4.0.1) installation procedure to upgrade the OracleAS Single Sign-On instance.	Refer to Section 7.5.3, "Upgrading Distributed OracleAS Identity Management Configurations" for complete instructions on upgrading the first OracleAS Single Sign-On instance.
4	Perform any post-upgrade procedures that apply to the OracleAS Single Sign-On Oracle home.	Refer to Section 9.3, "Task 3: Perform OracleAS Single Sign-On Post-Upgrade Steps" for more information.
5	Reconfigure the DCM cluster to which the OracleAS Single Sign-On instance belongs.	Refer to Section B.5.4.2, "Task 4b: Reconfigure the DCM Cluster" and perform the steps defined in that section in the OracleAS Single Sign-On Oracle home.
6	Configure the Oracle HTTP Server and OracleAS Single Sign-On to work with the newly upgraded OracleAS Single Sign-On instance.	Refer to Section B.5.4.3, "Task 4c: Configure Oracle HTTP Server and OracleAS Single Sign-On" and perform the steps defined in that section in the OracleAS Single Sign-On Oracle home.
7	Complete the upgrade of the first OracleAS Single Sign-On Oracle home.	Refer to Section B.5.4.4, "Task 4d: Finish the Upgrade of the First OracleAS Identity Management Instance" and perform the steps in that section in the OracleAS Single Sign-On Oracle home.

B.6.6 Task 6: Using Metadata Repository Upgrade Assistant to Upgrade the Component Schemas in the OracleAS Metadata Repository

1. Make sure that the OracleAS Identity Management instance (including Oracle Internet Directory) that you upgraded in Section B.3.5, "Task 4: Upgrade the First OracleAS Identity Management Instance" is up and running.

   If it is not running, start the Identity Management instance (including Oracle Internet Directory) as follows:

   ```
   ORACLE_HOME/opmn/bin/opmnctl startall
   ```

2. Upgrade the Metadata Repository in the newly upgraded database as described in Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository", with the following exception:

   On the MRUA command line, enter the address of the load balancer in place of the `oid_host` and `oid_ssl_port` arguments.

   Note that the values you enter for the `-oid_host` argument and `-oid_ssl_port` arguments must match the value of the corresponding properties defined in following configuration file in the Identity Management Oracle home:

   ```
   IDENTITY_MANAGEMENT_HOME/config/ias.properties
   ```

   For example:

```
OIDhost=sys42.acme.com
OIDsslport=636
```

3. When MRUA finishes processing, verify that the schemas have been upgraded, as described in Section 8.3, "Task 3: Verify the Success of the OracleAS Metadata Repository Upgrade".

B.6.7 Task 7: Installing Subsequent Oracle Internet Directory Instances

After you upgrade the first Oracle Internet Directory instance, upgrade the first OracleAS Single Sign-On instance, and upgrade the OracleAS Metadata Repository, you can then install the second Oracle Internet Directory and Oracle Delegated Administration Services instance in the OracleAS Cluster (Identity Management):

1. Make sure that the first Oracle Internet Directory is up and running on the first OracleAS Identity Management instance.
2. Make sure that the OracleAS Metadata Repository database and listener are up and running.
3. Make sure that the Oracle Internet Directory Load Balancer is configured to direct traffic only to the first Oracle Internet Directory instance.
4. Install a new 10*g* (10.1.4.0.1) Oracle Internet Directory Oracle home by following the instructions specific to Oracle Internet Directory installation in the section "Installing OracleAS Cluster (Identity Management) on Subsequent Nodes," in the *Oracle Application Server Installation Guide*.

   This step involves running Oracle Universal Installer and installing a new 10*g* (10.1.4.0.1) Oracle Internet Directory and Oracle Delegated Administration Services Oracle home. During the installation, respond to the installation prompts. In particular, be sure to do the following:

   - On the Select Installation Type screen, select **Oracle Identity Management**.
   - On the Select Configuration Options screen:
     - Select **Oracle Internet Directory**. Do not select Oracle Application Server Single Sign-On.
     - Do not select **Oracle Application Server Delegated Administration Services**.
     - Select **Oracle Directory Integration Platform** if you need this component.
     - Do not select **Oracle Application Server Certificate Authority (OCA)**.
     - Select **High Availability and Replication**.
5. Reconfigure the Load Balancer and test the installation.

   After a successful installation of the subsequent Oracle Internet Directory Oracle home, configure the Load Balancer to route requests to the new instance.
6. Repeat this procedure for any additional and subsequent Oracle Internet Directory installations that will be part of the cluster.

B.6.8 Task 8: Installing Subsequent OracleAS Single Sign-On Instances

After you upgrade the first Oracle Internet Directory instance, upgrade the first OracleAS Single Sign-On instance, upgrade the OracleAS Metadata Repository, and install any subsequent Oracle Internet Directory instances, you can then install any subsequent OracleAS Single Sign-On instances in the OracleAS Cluster (Identity Management):

1. Make sure that the Oracle Internet Directory instances and the first OracleAS Single Sign-On is up and running.
2. Make sure that the OracleAS Metadata Repository database and listener are up and running.
3. Make sure that the OracleAS Single Sign-On Load Balancer is configured to direct traffic only to the first OracleAS Single Sign-On instance.
4. Install a new 10*g* (10.1.4.0.1) OracleAS Single Sign-On Oracle home by following the instructions specific to OracleAS Single Sign-On installation in the section "Installing OracleAS Cluster (Identity Management) on Subsequent Nodes," in the *Oracle Application Server Installation Guide*.

   This step involves running Oracle Universal Installer and installing a new 10*g* (10.1.4.0.1) Oracle Internet Directory and Oracle Delegated Administration Services Oracle home. During the installation, answer the installation prompts. In particular, be sure to do the following points:

   - On the Select Installation Type screen, select **Oracle Identity Management**.
   - On the Select Configuration Options screen:
     - Do not select **Oracle Internet Directory**.
     - Select **Oracle Application Server Single Sign-On**.
     - Select **Oracle Application Server Delegated Administration Services**.
     - Select **Oracle Directory Integration Platform** if you need this component.
     - Do not select **Oracle Application Server Certificate Authority (OCA**).
     - Select **High Availability and Replication**.
   - On the Create or Join an OracleAS Cluster (Identity Management) page, select **Join an Existing Cluster**.
   - On the Specify Existing OracleAS Cluster Name screen enter the name of the Oracle Identity Management cluster you want to join.
   - On the Specify HTTP Load Balancer Host and Ports screen, be sure to enter the same values for every OracleAS Single Sign-On node in the cluster:
     - **HTTP Listener: Port:** Enter the port number that you want Oracle HTTP Server to listen on. **Enable SSL:** Select this option if you want to configure Oracle HTTP Server for SSL on this port.
     - **HTTP Load Balancer: Hostname:** Enter the name of the HTTP virtual server configured on your load balancer. Enter the same virtual server name that you configured on the load balancer.
     - **HTTP Load Balancer: Port:** Enter the port for the HTTP virtual server. **Enable SSL:** Select this option if this port is for SSL communications only.
5. Reconfigure the Load Balancer and test the installation.

   After a successful installation of the subsequent Oracle Internet Directory Oracle home, configure the Load Balancer to route requests to the new instance.
6. Repeat this procedure for any additional and subsequent Oracle Internet Directory installations that will be part of the cluster.

B.6.9 Task 9: Verify the Upgrade and Decommission the 10*g* Release 2 (10.1.2) Oracle Homes

After you have upgraded the first Oracle Identity Management instance in the cluster and you have added the remaining cluster members, you can then verify that the upgrade was successful and then decommission the 10*g* Release 2 (10.1.2) Oracle homes.

For more information, refer to Chapter 10, "Verifying the Upgrade and Decommissioning the Source Oracle Homes".

C

Using the Data Migration Method of Upgrading OracleAS Identity Management

Use the following sections to learn more about an alternative method of upgrading your OracleAS Identity Management environment:

- Differences Between Data Migration and Typical OracleAS Identity Management Upgrade Procedures
- Using the Data Migration Method of Upgrading OracleAS Identity Management

C.1 Differences Between Data Migration and Typical OracleAS Identity Management Upgrade Procedures

Before you use the instructions in this chapter, review Table C–1, which describes the differences between data migration and the more typical OracleAS Identity Management upgrade procedures described in Chapter 7, "Using Oracle Universal Installer to Upgrade Oracle Identity Management".

Use this table to be sure you use the upgrade procedure best suited for your OracleAS Identity Management environment.

Table C–1 Comparison of Data Migration and Typical OracleAS Identity Management Upgrade Procedure

Typical OracleAS Identity Management Upgrade	Data Migration Upgrade
Use Oracle Universal Installer to automatically: 1. Upgrade the OracleAS Metadata Repository database. 2. Install a new OracleAS Identity Management Oracle home. 3. Upgrade the OracleAS Identity Management schemas in the OracleAS Metadata Repository. 4. Copy configuration data to the new OracleAS Identity Management Oracle home.	1. Use Oracle Universal Installer to install a new OracleAS Identity Management environment, including Oracle Internet Directory, OracleAS Single Sign-On, and the required OracleAS Metadata Repository. 2. Use command-line tools to manually export the Oracle Identity Management data in the source OracleAS Identity Management environment and then use command-line tools to restore the data to the destination Oracle Identity Management 10*g* (10.1.4.0.1) database.
All upgrade tasks are performed on one host on the same platform.	You can migrate your OracleAS Identity Management data from one host to another, and you can migrate data from one platform to another (for example, from UNIX to Microsoft Windows).

Table C–1 (Cont.) Comparison of Data Migration and Typical OracleAS Identity Management Upgrade Procedure

Typical OracleAS Identity Management Upgrade	Data Migration Upgrade
After the upgrade, you use the destination Oracle home and the original source Oracle home is decommissioned.	After the data migration, you can continue using both the source and destination installations. The source installation is left untouched.
This upgrade can be used only to upgrade from a previous version to a newer version.	This procedure can be used to upgrade to a newer version of Oracle Application Server or to move data between installations of the same version.
During the upgrade, the OracleAS Identity Management services are down.	During this upgrade, there is no downtime required, although Oracle Internet Directory must be in read-only mode while the data in the directory is backed up.
The upgrade is relatively quick and less time-consuming because many of the steps are automated.	The upgrade procedure will usually take longer than a typical OracleAS Identity Management upgrade because many of the steps are manual.

C.2 Using the Data Migration Method of Upgrading OracleAS Identity Management

Use the following steps to upgrade OracleAS Identity Management using the data migration method.

Task 1 Install a new, complete 10*g* (10.1.4.0.1) OracleAS Identity Management environment

You can install any of the supported OracleAS Identity Management topologies described in the *Oracle Application Server Installation Guide*. The new 10*g* (10.1.4.0.1) OracleAS Identity Management environment must include its own OracleAS Metadata Repository and database.

Review the following requirements when installing and configuring the new OracleAS Identity Management environment:

- The database name you select during the installation must not conflict with the database in the source environment.
- Do not install any other application server component against the new Identity management instance until the data migration is complete.
- Do not load any user data before data migration is complete.
- Test and verify that all identity management components are working smoothly.

During the installation, note the application server instance name, the `ias_admin` password, and the `system` database user password that you specify for the new install. You will use this information during the remaining steps in the upgrade procedure.

Task 2 Back up the OracleAS Identity Management data in the source environment

1. Set the Oracle Internet Directory to read-only mode.

   a. Create an LDIF file; for example, `mod.ldif`, with the following content:

```
dn:
changetype : modify
replace: orclservermode
orclservermode: ro
```

b. Run the following command to execute the LDIF file:

```
SOURCE_ORACLE_HOME/bin/ldapmodify
    -h source_oid_host
    -p port
    -D cn=orcladmin
    -w orcladmin_password
    -v
    -f mod.ldif
```

Setting Oracle Internet Directory to read-only is not required, but if you do not set the directory to read-only, any changes made while you are backing up the directory will not be included in the backup.

2. Back up the Oracle Internet Directory by using the following commands:

```
SOURCE_ORACLE_HOME/bin/ldifwrite
        -c db_connect_string
        -b "cn=oraclecontext"
        -f bkp1.ldif
SOURCE_ORACLE_HOME/bin/ldifwrite
        -c db_connect_string
        -b "dc=com"
        -f bkp2.ldif
```

In these examples, replace *db_connect_string* with the Oracle Internet Directory database connect string. If you do not provide this string, it defaults to the value of the ORACLE_SID environment variable.

Also in this example, it is assumed that `dc=com` is the root of the subscriber. If you have additional subscribers, then execute an equivalent `ldifwrite` command for the root of each subscriber.

> **See Also:** "ldifwrite" in the *Oracle Identity Management User Reference*

3. Merge `bkp1.ldif` and `bkp2.ldif` into one file; for example, merge the two files into a file called `bkp.ldif` and save the file in a known location so you can later load it into the new destination Oracle Internet Directory.

4. Set the source Oracle Internet Directory back to read-write mode.

   a. Create an LDIF file; for example, `modrw.ldif`, with the following content:

```
dn:
changetype : modify
replace: orclservermode
orclservermode: rw
```

   b. Run the following command to execute the LDIF file:

```
SOURCE_ORACLE_HOME/bin/ldapmodify
    -h source_oid_host
    -p port
    -D cn=orcladmin
    -w orcladmin_password
    -v
    -f modrw.ldif
```

Task 3 Back up the OracleAS Single Sign-On data in the source environment

Back up the OracleAS Single Sign-On data using the following command:

```
SOURCE_ORACLE_HOME/sso/bin/ssomig
    -export
    -s orasso
    -p source_database_orasso_schema_password
    -c source_SSO_database_connect_string
    -log_d full_log_directory_path
```

In this example:

- Replace *source_database_orasso_schema_password* with the database schema password for OracleAS Single Sign-On.

  This password is randomized during installation of the OracleAS infrastructure. To obtain the password, see Appendix B of the *Oracle Application Server Single Sign-On Administrator's Guide*.

- Replace *source_SSO_database_connect_string* with the net service name for the OracleAS Single Sign-On database.

- Replace *full_log_directory_path* with the name of the log directory.

  This directory must be writable. The log file, the export configuration file, and the dump file are written here. Use the absolute path for the directory when running the script. The default is `ORACLE_HOME/sso/log`.

  > **See Also:** "Export and Import Script: Syntax and Parameters" in the *Oracle Application Server Single Sign-On Administrator's Guide*

Task 4 Prepare the destination OracleAS Identity Management Oracle home for Data Migration

1. Back up the local registration information from the destination OracleAS Identity Management so it can be restored after you migrate the data from the source OracleAS Identity Management instance.

   Note that the data saved in this backup file includes the password for the new 10*g* (10.1.4.0.1) ORASSO schema. You will need to retrieve this password from the backup registration LDIF file that you create in this step.

   To back up the local registration information, including the ORASSO password, enter the following command:

   ```
   DESTINATION_ORACLE_HOME/ldap/bin/remtool
      -backupmetadata
      -replica oidhost:oidport/repdnpwd
      -bkup ldiffilename
   ```

   In this example:

   - Replace *oidhost* with the host name of the destination Oracle Internet Directory.
   - Replace *oidport* with the port at which the destination Oracle Internet Directory is listening.
   - Replace *repdnpwd* with the replication DN password of the destination Oracle Internet Directory, which by default is the same as the `cn=orcladmin` password after the installation.

- Replace *ldiffilename* with the name of the `ldif` file that will contain the backed up registration data.

  See Also: "remtool" in the *Oracle Identity Management User Reference*

2. Merge the destination OracleAS Identity Management schema with the source OracleAS Identity Management schema:

```
DESTINATION_ORACLE_HOME/bin/schemasync
    -srchost source_oid_hostname
    -srcport source_oid_port_number
    -srcdn source_oid_privileged_DN
    -srcpwd source_oid_privileged_DN_password
    -dsthost destination_oid_hostname
    -dstport destination_oid_port
    -dstdn destination_oid_privileged_dn
    -dstpwd destination_oid_privileged_DN_password
    -ldap
```

   In this example, replace *source_oid_privileged_DN* and *destination_oid_privileged_DN* with the distinguished name of the user used to bind to the directory. This user must have permissions to modify the directory schema, for example the super user (`cn=orcladmin`).

   The `-ldap` parameter is optional. If you include the `-ldap` parameter, then the schema changes are applied directly from the source Oracle Internet Directory to the destination Oracle Internet Directory. If you do not include the `-ldap` parameter, then the new attribute definitions are saved to the following LDIF file:

```
ORACLE_HOME/ldap/odi/data/attributetypes.ldif
```

   And, the object class definitions are saved to the following LDIF file:

```
ORACLE_HOME/ldap/odi/data/objectclasses.ldif
```

   Any errors that occur during the schema synchronization are logged in the following log files:

```
ORACLE_HOME/ldap/odi/log/attributetypes.log
ORACLE_HOME/ldap/odi/log/objectclasses.log
```

   See Also: "schemasync " in the *Oracle Identity Management User Reference*

3. Stop the Oracle Internet Directory in the destination Oracle home using OPMN:

```
DESTINATION_ORACLE_HOME/opmn/bin/opmnctl stopall
```

4. Clean up any conflicting data from the destination Oracle Internet Directory by running the following commands:

```
DESTINATION_ORACLE_HOME/ldap/bin/bulkdelete
    connect="db_connect_string"
    basedn="cn=OracleContext"
DESTINATION_ORACLE_HOME/ldap/bin/bulkdelete
    connect="db_connect_string"
    basedn="dc=com"
```

   This example assumes that `dc=com` is the root of the subscriber. If you have additional subscribers, then use an equivalent `bulkdelete` command for the root of each additional subscriber.

Task 5 Load the source Oracle Internet Directory data into the destination Oracle Internet Directory

1. Copy the `bkp.ldif` file to the destination host; use an appropriate file transfer method, such as FTP.

2. Comment any ACL attributes in the LDIF file that are not defined in the directory schema.

   With the 10*g* (10.1.4.0.1) release, Oracle Internet Directory introduces a new restriction for Access Control Lists (`orclaci` and `orclentrylevelaci` attributes). Specifically, you cannot specify attribute names that are not defined in directory schema. As a result, while adding or migrating entries from previous Oracle Internet Directory releases, the load operation will fail if any entries have attribute names that are not defined in the directory schema.

   To avoid this problem, in the `bkp.ldif` file, comment any ACLs that have undefined attributes.

   For example, the following 10*g* Release 2 (10.1.2) entry uses undefined attributes that are identified with bold text:

   ```
   orclaci: access to attr=(orclUserApplnProvStatus,orclUserApplnProvStatusDesc,
    orclUserProvFailureCount) by group="cn=oracledasedituser,cn=groups,
    cn=OracleContext,dc=us,dc=oracle,dc=com" (read,search,write,compare) by
    group="cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=oracle,
    dc=com" (read,search,write,compare) by self (read,search,nowrite,compare)
    by * (none)
   ```

   To avoid this problem, comment the entry as follows, before loading or verifying the LDIF file.

   ```
   # orclaci: access to attr=(orclUserApplnProvStatus,orclUserApplnProvStatusDesc,
   # orclUserProvFailureCount) by group="cn=oracledasedituser,cn=groups,
   # cn=OracleContext,dc=us,dc=oracle,dc=com" (read,search,write,compare) by
   # group="cn=oracledascreateuser,cn=groups,cn=OracleContext,dc=us,dc=oracle,
   # dc=com" (read,search,write,compare) by self (read,search,nowrite,compare)
   # by * (none)
   ```

3. Verify the backup data in the LDIF file:

   ```
   DESTINATION_ORACLE_HOME/ldap/bin/bulkload
      connect="destination_oid_connect_string"
      check=true
      restore=true
      file="path_to_bkp.ldif/bkp.ldif"
   ```

   In this example, replace *path_to_bkp.ldif* with the path to the location where you stored the backup LDIF files.

   After running the `bulkload check` command, check the contents of the following log files:

   ```
   DESTINATION_ORACLE_HOME/ldap/log/bulkload.log
   DESTINATION_ORACLE_HOME/ldap/load/badentry.ldif
   ```

   If necessary, perform the `bulkload` command repeatedly on the `ldif` file until no errors are reported in the log files.

   For example, look for these common error messages:

   - **Error Message:** `DN Error --- DN "<DN of the error entry>", rc=0`

Action: An entry in the `ldif` file has an invalid DN and cannot be loaded into the destination Oracle Internet Directory. Remove this entry from the `ldif` file.

- **Error Message:** `ERROR * gslsbzCheckDupAttrValinEntry : Dupl Value {X- ORCLLMV}4F6500711D4185249B624840E0439040 found`

  Action: An entry in the `ldif` files has duplicate values for Password verifiers. Clean up the entries that have duplicate password verifiers.

4. Load the source Oracle Internet Directory data into the destination Oracle Internet Directory:

```
DESTINATION_ORACLE_HOME/ldap/bin/bulkload
   connect="destination_oid_connect_string"
   generate=true
   check=true
   restore=true
   load=true
   file="path_to_bkp.ldif/bkp.ldif"
```

In this example, replace *path_to_bkp.ldif* with the path to the location where you stored the backup LDIF files.

Check the log files again to be sure no errors were generated while the data was loaded into the destination Oracle Internet Directory. Errors in this step (such as index creation errors) can cause serious problems later.

Task 6 Obtain the ORASSO Schema Password for the Destination Database

When you migrate the OracleAS Single Sign-On data to the destination database, you will need the password for the ORASSO schema.

You can obtain this password from the registration data backup LDIF file, which you created with remtool in "Task 4, "Prepare the destination OracleAS Identity Management Oracle home for Data Migration".

1. Use a text editor to open the registration data LDIF file, which you created in Task 4, "Prepare the destination OracleAS Identity Management Oracle home for Data Migration"
2. Locate the following entry in the LDIF file:

```
orclresourcename=ORASSO,
  orclReferenceName=database_global_name,
  cn= IAS Infrastructure Databases,
  cn=IAS, cn=Products, cn=OracleContext
```

The password is stored as the value of attribute `orclpasswordattribute` of this entry.

For example, in the following example, ORASSO schema password is `welcome1`.

```
dn: OrclResourceName=ORASSO,
    orclReferenceName=orcl.myhostdb1.us.oracle.com,
    cn=IAS Infrastructure Databases,
    cn=IAS,
    cn=Products,
    cn=OracleContext
orclflexattribute1: true
orclpasswordattribute: welcome1
orclresourcename: ORASSO
objectclass: orclResourceDescriptor
```

```
objectclass: top
```

3. Close the backup LDIF file without saving any changes to the file.

Task 7 Migrate the OracleAS Single Sign-On data

1. Copy the files created when you backed up the OracleAS Single Sign-On data in the source environment in Step 3 to the destination host.

   Use an appropriate method for copying the files to the destination host, such as FTP. The files to copy are `ssomig.dmp` and `ssoconf.log`. By default, these files are created in the following directory:

   ```
   DESTINATION_ORACLE_HOME/sso/log
   ```

2. Enter the following command to import the Single Sign-On data:

   ```
   DESTINATION_ORACLE_HOME/sso/bin/ssomig
       -import
       -overwrite
       -s orasso
       -p destination_orasso_schema_password
       -c source_SSO_database_connect_string
       -log_d  full_log_directory_path
       -log_f imp.log
   ```

   In the above example:

   - Replace *full_log_directory_path* with the directory location where you have copied SSO data files (`ssomig.dmp` and `ssoconf.log`).
   - Replace *destination_orasso_schemas_password* with the ORASSO schema password of the destination database. You should have obtained this password in Task 6, "Obtain the ORASSO Schema Password for the Destination Database".

     See Also: "Export and Import Script: Syntax and Parameters" in the *Oracle Application Server Single Sign-On Administrator's Guide*

Task 8 Completing the OracleAS Identity Management Data Migration

1. Start the Oracle Internet Directory in the destination Oracle home using the `oidmon` command utility:

   ```
   DESTINATION_ORACLE_HOME/opmn/bin/oidmon connect=destination_oid_db start
   ```

   It is important that you use `oidmon` and not OPMN for this step because `oidmon` starts only the Oracle Internet Directory processes and not any of the other OPMN-managed components in the Oracle home.

2. Restore the local registration information for the destination OracleAS Identity Management Oracle home that you saved in Task 4, "Prepare the destination OracleAS Identity Management Oracle home for Data Migration", as follows:

   a. Open the file where local registration information is stored and comment all lines that start with attribute name "authpassword".

      For example:

      ```
      dn: orclApplicationCommonName=im1014.myhost.mydomain.com,cn=IAS Instances,
       cn=IAS, cn=Products, cn=OracleContext
      objectclass: top
      objectclass: orclApplicationEntity
      ```

```
orclapplicationcommonname: im1014b.stadd54.us.oracle.com
userpassword: {SHA}lyWKMuTVIxQ5p8IvhHcIxyGIQxY=
#authpassword;oid: {SASL/MD5}trJGtjPG5zHYJ2a6BvIqJg==
#authpassword;oid: {SASL/MD5-DN}HGuSwmmhGqW9zm37F7HhOA==
#authpassword;oid: {SASL/MD5-U}K343/kWyrYqRR/Wi1ArXMA==
```

b. Restore the local registration information, as follows:

```
DESTINATION_ORACLE_HOME/bin/ldapadd
    -h destination_oid_hostname
    -p destination_oid_port
    -v
    -f locreg.ldif
    -D super_user_DN
    -w bindpassword
    -c
```

In this example, it is assumed that you saved the local registration information in a file called `locreg.ldif`.

Note that while restoring the local registration entries, the addition of some entries will fail. This is expected and you will see errors as shown in the following example:

```
adding new entry cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
ldap_add: Already exists
ldap_add: additional info: Object already exists
adding new entry orclApplicationCommonName=ORASSO_SSOSERVER,
  cn=SSO,cn=Products,cn=OracleContext
ldap_add: Already exists
ldap_add: additional info: Object already exists
```

3. If Oracle Delegated Administration Services is configured, modify the entries for the service using the following steps.

The entries for Oracle Delegated Administration Services and OracleAS Single Sign-On must refer to the local, destination instance of the service. However, due to migration procedure, these entries will be pointing to source Oracle home. These values need to be replaced with the correct information appropriate to the destination Oracle home:

a. Open the `locreg.ldif` file you created in Task 3, "Back up the OracleAS Single Sign-On data in the source environment", and then locate and copy the Oracle Delegated Administration Services URL from the file contents.

The DN of the DAS URL container entry is as follows:

```
"cn=OperationURLs, cn=DAS, cn=Products, cn=OracleContext"
```

It is usually the next-to-last entry in the file.

b. Create an LDIF file called `change_das_url.ldif` with the following contents:

```
dn: cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
changetype: modify
replace: orcldasurlbase
orcldasurlbase: URL_from_backup_file
```

c. Execute the following command to change the DAS URL:

```
DESTINATION_ORACLE_HOME/bin/ldapmodify
    -p destination_directory_port
    -h destination_directory_host
    -D super_user_DN
    -w super_user_password
    -f change_das_URL.ldif
```

4. If OracleAS Single Sign-On is configured, modify the OracleAS Single Sign-On (ORASSO) schema password using the following steps:

   a. Create an LDIF file called `change_sso_password.ldif` with the following contents:

   ```
   dn: orclApplicationCommonName=ORASSO_SSOSERVER,cn=SSO,cn=Products,
         cn=OracleContext
   changetype: modify
   replace: userpassword
   userpassword: specify_a_new_password
   ```

   b. Execute the following command to modify the password of OracleAS Single Sign-On entry in Oracle Internet Directory:

   ```
   DESTINATION_ORACLE_HOME/bin/ldapmodify
        -p consumer_port
        -h consumer_host
        -D super_user_DN
        -w super_user_password
        -f change_sso_password.ldif
   ```

   c. Change directory to the following directory in the destination Oracle home:

   ```
   DESTINATION_ORACLE_HOME/sso/admin/plsql/sso
   ```

   d. Log in to the database using SQL*Plus and the destination Oracle home ORASSO schema password.

   At this point in the procedure, you should have obtained the ORASSO schema password as described in "Task 6, "Obtain the ORASSO Schema Password for the Destination Database".

   e. Run the `ssooconf.sql` script by issuing the following command:

   ```
   SQL> @ssooconf.sql
   ```

   This script prompts for following values.

   ```
   Enter value for new_oid_host :
   Enter value for new_oid_port :
   Enter value for new_ssoserver_password :
   Enter value for new_ldapusessl :
   ```

   In response to the **Enter value for new_ssoserver_password** prompt, enter the new Oracle Application Server Single Sign-On password that you specified in the `change_sso_password.ldif` LDIF file in Step 4a.

   For all other prompts, just accept the defaults by pressing the Enter or Return key.

5. Reset the `ias_admin` instance password using the following command:

```
DESTINATION_ORACLE_HOME/bin/resetiASpasswd.sh
    cn=orcladmin orcladmin_pwd complete_path_to_destination_oracle_home
```

See Also: "Changing Instance Passwords in Oracle Internet Directory" in the *Oracle Application Server Security Guide*

6. If you are using the data migration procedure to upgrade Oracle Internet Directory to 10*g* (10.1.4.0.1), the password policies that were migrated to the new directory will, by default, no longer behave as intended after they are loaded into the 10*g* (10.1.4.0.1) directory.

   To update the password policies so they will work in the new 10*g* (10.1.4.0.1) environment, use the following procedure:

   a. Add the following paths to the LD_LIBRARY_PATH environment variable:

      On Linux or Solaris systems:

      ```
      DESTINATION_ORACLE_HOME/lib
      DESTINATION_ORACLE_HOME/network/lib
      ```

      On 64 bit Solaris systems:

      ```
      DESTINATION_ORACLE_HOME/lib32
      DESTINATION_ORACLE_HOME/network/lib32
      ```

   b. Use the following command-line tool to update the password policies in the 10*g* (10.1.4.0.1) Oracle Internet Directory:

      ```
      java -cp
          DESTINATION_ORACLE_HOME/ldap/postcfg/oidca.jar:DESTINATION_ORACLE_
      HOME/jlib/ldapjclnt10.jar
          oracle.ldap.oidinstall.backend.OIDUpgradePasswordPolicies
          host
          port
          bindDN
          bindPassword
          ORACLE_HOME
          protocol
      ```

      Note that all the arguments shown in the previous example must be entered on one line. They are shown in this format to make it easier to identify the required arguments.

      Table C–2 describes the arguments and the values you must provide.

   c. After you run the password policies command-line tool, you can review the actions performed by the tool by reviewing the log file at:

      ```
      DESTINATION_ORACLE_HOME/ldap/log/ppUpgrade.log
      ```

Table C–2 Arguments to the Oracle Internet Directory Password Policies Command-Line Tool

Argument	Description
host	The name of the host computer on which Oracle Internet Directory 10*g* (10.1.4.0.1) is running.
port	The port on which Oracle Internet Directory 10*g* (10.1.4.0.1) is listening.
bindDN	The Distinguished Name (DN) of a privileged admin user (usually, `cn=orcladmin`).
bindPassword	The user password associated with the DN you provided as the bindDN.
ORACLE_HOME	The Oracle home for Oracle Internet Directory instance

Table C–2 (Cont.) Arguments to the Oracle Internet Directory Password Policies Command-Line Tool

Argument	Description
protocol	Use this optional argument to specify that you are using a secure (SSL) connection to the directory. If you are using SSL, enter "ssl" in place of *protocol* in the example.

7. Upgrade the `oraclecontext` and `subscriber` context for the destination OracleAS Identity Management installation, as follows:

> **Note:** This step (upgrading the `oraclecontext` and `subscriber` context) is applicable only when the source OracleAS Identity Management and the destination OracleAS Identity Management are of different versions. For example, you must run this step when using data migration to upgrade from 10*g* (9.0.4) to 10*g* (10.1.4.0.1).

a. Run the following command to upgrade the Oracle Internet Directory metadata as part of a migration from a previous version of OracleAS Identity Management to 10*g* (10.1.4.0.1):

```
DESTINATION_ORACLE_HOME/bin/oidca mode=UPGRADE
    -silent
    dbuser=DBA_user
    dbpwd=DBA_user_password
    connstr=TNS_alias_db_connect_string
    sudn=oid_superuser_dn
    supwd=oid_superuser_password
    iasinstance=app_server_instance_name
    iaspwd=ias_admin_password
```

Table C–3 describes the arguments and values you should provide when you specify UPGRADE mode for `oidca`.

Note that all the arguments shown in the previous example must be entered on one line. They are shown in this format to make it easier to identify the required arguments.

Table C–3 Summary of Arguments To Use For oidca in UPGRADE Mode

Argument	Description
dbuser	Any database user account that has DBA privileges. The SYSTEM user account has DBA privileges and can be used for this connection.
dbpwd	Password of database account specified in **dbuser** argument. For SYSTEM user account, the password was specified during the installation.
connstr	Connect string for the Destination Oracle home database.
sudn	The super user DN, which is `cn=orcladmin`.
supwd	The password of the super user DN. By default the super user DN password is set to same password as the at the time of install.
iasinstance	The name of Oracle Application Server instance that you specified at the time of install.
iaspwd	The `ias_admin` password that you specified at the time of install.

b. Run the following command to upgrade the Oracle Directory Integration Platform metadata:

```
DESTINATION_ORACLE_HOME/bin/oidca mode=DIPUPGRADE
   -silent
   oidhost=oid_host
   sslport=oid_ssl_port
   sudn=oid_user_dn
   supwd=oid_user_password
   odspwd=oid_db_schema_password
   connstr=TNS_Alias_connect_string
   iasinstance=1014_iasinstance_name
   iaspwd=ias_admin_password
   -migrateprofiledata
   masteroidhost=host_of_oid_in_source_environment
   masteroidport=ssl_or_nonssl_port_in_source_environment [-ssl]
   mastersudn=user_dn_of_oid_in_source_environment
   mastersupwd=user_password_of_oid_in_source_environment
```

Note that if you are using the SSL port for the `masteroidport` parameter, you must include the `-ssl` argument to identify it as an SSL port.

The arguments shown in the previous example must be entered on one line. They are shown in this format to make it easier to identify the required arguments.

Table C–4 describes the arguments and values you should provide when you specify DIPUPGRADE mode for `oidca`.

Table C–4 Summary of Arguments To Use For oidca in DIPUPGRADE Mode

Argument	Description
oidhost	Host name where destination Oracle Internet Directory server is running
sslport	SSL port of destination Oracle Internet Directory server; you must specify the SSL port of the directory; you cannot use the non-SSL port with the `oidca` command in DIPUPGRADE mode.
sudn	The super user DN, which is `cn=orcladmin`.
supwd	The password of the super user DN. By default the super user DN password is set to same password as the at the time of install.
odspwd	The password of ODS database user account. By default the ODS user password is same as `ias_admin` password, which you specified at the time of install.
connstr	Connect string for the Destination Oracle home database.
iasinstance	The name of Oracle Application Server instance that you specified at the time of install.
iaspwd	The `ias_admin` password that you specified at the time of install.
masteroidhost	The host name where source Oracle Internet Directory is running
masteroidport	The port number of source Oracle Internet Directory
mastersudn	The super user DN of source Oracle Internet directory. It is normally "cn=orcladmin"

Table C–4 (Cont.) Summary of Arguments To Use For oidca in DIPUPGRADE Mode

Argument	Description
mastersupwd	The password of the super user DN of the source Oracle Internet Directory.

8. Stop the Oracle Internet Directory using the `oidmon` utility:

```
DESTINATION_ORACLE_HOME/bin/oidmon connect=destination_oid_db stop
```

9. Start the Oracle Internet Directory and all the components in the destination Oracle home using OPMN:

```
DESTINATION_ORACLE_HOME/opmn/bin/opmnctl startall
```

D

Reviewing the Upgrade Log Files

Often, you can troubleshoot common problems by reviewing the log files generated by Oracle Universal Installer and by the Metadata Repository Upgrade Assistant. Refer to the following sections for more information:

- Reviewing the Oracle Universal Installer Log Files
- Reviewing the MRUA Log Files
- Reviewing the OracleAS Portal Repository Upgrade Log Files

D.1 Reviewing the Oracle Universal Installer Log Files

When you use Oracle Universal Installer to upgrade your upgrade OracleAS Identity Management or the OracleAS Metadata Repository database, you can troubleshoot certain upgrade issues by reviewing the log files generated by Oracle Universal Installer.

Two sets of Oracle Universal Installer log files are saved on disk:

- The installer generates the following log files:

  ```
  oraInventory_location/logs/installActionstimestamp.log
  oraInventory_location/logs/oraInstalltimestamp.err
  oraInventory_location/logs/oraInstalltimestamp.out
  DESTINATION_ORACLE_HOME/install/make.log
  ```

- The configuration assistants generates log files in the *DESTINATION_ORACLE_HOME*/`cfgtoollogs` directory.

Note that if you want to access the log files created by the configuration assistants, you need to exit the installer first. The log files are inaccessible if the installer is still in use.

The location of the Oracle inventory directory (*oraInventory_location* in the previous example) is saved in the following file:

- On Solaris systems:

  ```
  /var/opt/oracle/oraInst.loc
  ```

- On Linux systems:

  ```
  /etc/oraInst.loc
  ```

D.2 Reviewing the MRUA Log Files

When you run MRUA, the utility generates a set of log files that you can use to troubleshoot, verify, or analyze the OracleAS Metadata Repository upgrade process. For more information, see the following sections:

- Guidelines for Using the MRUA Log Files
- Locating the MRUA Log Files

D.2.1 Guidelines for Using the MRUA Log Files

If the MRUA output indicates that one or more of the component upgrades failed, review the MRUA log files, or any component log files referenced from the MRUA log files.

If the OracleAS Portal upgrade fails, then see Section D.3, "Reviewing the OracleAS Portal Repository Upgrade Log Files" for information on how to proceed.

If, by reviewing the log files, you are able to identify a solution to the upgrade failure, then you can implement your solution and re-run MRUA. When you re-run MRUA, any components that were upgraded successfully during the previous run will not be affected. However, MRUA will attempt to upgrade any components that were not upgraded successfully during a previous run of the utility.

Contact Oracle Support for any errors that are not documented or that cannot be resolved by following documented actions. Note that some errors that occur will require the repository to be restored from backup, the problem to be resolved, and another upgrade to be run.

D.2.2 Locating the MRUA Log Files

The log files are located in the following directory in the Oracle home of the OracleAS Metadata Repository you are upgrading:

```
METADATA_REPOSITORY_ORACLE_HOME/upgrade/logs
```

MRUA generates three log files that are of particular interest when you are troubleshooting upgrade issues. The name of the log file includes the exact time the MRUA session was run. This makes it easy to identify a log file for a particular MRUA session.

For example, the three log files generated when you run MRUA at 12:36 PM on September 16, 2004 would appear as follows in the logs directory:

```
mrua2004-09-16_12-36-36PM.log
mrua2004-09-16_12-36-36PM.err
mrua2004-09-16_12-36-36PM.out
```

Table D–1 shows the three log file types and the content you can expect to find in each one.

Table D–1 Summary of the Log Files Generated by MRUA

MRUA Log File	Description
`mrua<timestamp>.log`	The log file is a good place to start if you are troubleshooting a particular problem with the OracleAS Metadata Repository upgrade. This file contains a high-level summary of all the actions performed by MRUA; as a result, it can help you isolate a specific component that was not upgraded successfully.

Table D–1 (Cont.) Summary of the Log Files Generated by MRUA

MRUA Log File	Description
`mrua<timestamp>.err`	The error file contains any errors or stack traces generated during the upgrade process. These errors should contain information that help you diagnose and address specific upgrade errors.
`mrua<timestamp>.out`	The output file is the largest of the three MRUA log files and it contains the most comprehensive data about the MRUA session. Use this log file to determine exactly when a particular problem occurred to and see the output generated by the MRUA subcomponents.

D.3 Reviewing the OracleAS Portal Repository Upgrade Log Files

This section provides information about the OracleAS Portal upgrade log files. If the OracleAS Portal upgrade fails, carefully review this section in its entirety before attempting to troubleshoot the upgrade failure.

Note that if the OracleAS Portal components were upgraded to 10*g* Release 2 (10.1.2) successfully, then there is no need to examine the log files.

When upgrading OracleAS Portal by running MRUA, the log files are generated into a single directory:

```
ORACLE_HOME/upgrade/temp/portal
```

Note that any already existing log files in the relevant directory will be renamed to include a time stamp, so that they are not overwritten.

Table D–2 Summary of the Repository Upgrade Log Files Generated by OracleAS Portal

Log File	Description
upgrade.log	The log file generated by the 10*g* (9.0.4) to 10*g* Release 2 (10.1.2) OracleAS Portal upgrade. This file will always be generated if the starting version is 10*g* (9.0.4), as long as the checks performed at the beginning of the upgrade succeed.
precheck.log	The log file generated for the checks performed before the 10*g* (9.0.4) to 10*g* Release 2 (10.1.2) upgrade. This file is generated before the script begins making modifications to the repository, or when a manual upgrade from 10*g* (9.0.4) is run in -precheck mode. If there are errors in `precheck.log`, the 10*g* (9.0.4) to 10*g* Release 2 (10.1.2) upgrade will not run and the `upgrade.log` file will not be generated.

At the end of each one of these log files, there is either a success message or a summary of all the errors that occur earlier in the file. These summary messages include references to line numbers. You can go to those lines earlier in the log file to see the errors in their context.

Caution: Any portals running after an upgrade that was not clean are not supported by Oracle.

Look up any errors found in the precheck or upgrade log files using Section E.3, "Portal Repository Upgrade Messages" as a reference. Resolve any errors and warnings that have documented actions. Any errors that occur after the precheck phase require the repository to be restored from backup, the problem resolved and another upgrade run. Contact Oracle Support for any errors that are not documented or that cannot be resolved by following documented actions. When undocumented errors are found, do not attempt to run the upgrade again, run any further steps, alter any files, modify the OracleAS Portal schema, or access the OracleAS Portal instance in your browser.

The following is an example of the end of the log file after a successful upgrade (note the "Upgrade completed successfully" message and the lack of error messages):

```
>>> Running upg/common/popinv.pl
### Upgrade completed successfully
>>> Running tmp/popinv.sql
Portal SQL script started at Thu Apr 22 20:56:23 2004
Connected.
Updating patch inventory.
Upgrade Ended at Thu Apr 22 20:56:24 2004
```

E

OracleAS Metadata Repository Upgrade Error Messages

This section includes a description of the error messages that might be generated during the upgrade of the OracleAS Metadata Repository. Refer to the following sections for more information:

- Section E.1, "Error Messages Generated By the Metadata Repository Upgrade Assistant"
- Section E.2, "UDDI Registry OracleAS Metadata Repository Upgrade Error Messages"
- Section E.3, "Portal Repository Upgrade Messages"

E.1 Error Messages Generated By the Metadata Repository Upgrade Assistant

This section describes the error messages generated by the Metadata Repository Upgrade Assistant.

Error: MRUA was unable to connect to SSL port of OID

Cause: When MRUA prompted you for the password for the Oracle Internet Directory superuser (`cn=orcladmin`) account, you entered an incorrect password.

Action: Check to be sure that you entered the password correctly. Run MRUA again and enter the correct the value when prompted for the `cn=orcladmin` password.

Cause: The Oracle Internet Directory instance is down or not available, or you entered the wrong Oracle Internet Directory host name or secure port on the MRUA command line.

Action: Check to be sure that the host name and SSL port you identified for the Oracle Internet Directory represent a valid Oracle Internet Directory instance that is up and running.

The value of the `-oid_host` argument and `-oid_ssl_port` arguments must match the value of the corresponding properties defined in following configuration file in the Identity Management Oracle home:

```
IDENTITY_MANAGEMENT_HOME/config/ias.properties
```

For example:

```
OIDhost=sys42.acme.com
```

```
OIDsslport=636
```

Error: MRUA was unable to open XML file: ***xml_file_name***

Cause: The Metadata Repository Upgrade Assistant was unable to open a required XML file specific for one of the Oracle Application Server components. As a result, the schema for that component cannot be upgraded in the OracleAS Metadata Repository.

Action: Note the name of the file and make sure that you are running MRUA from an account with access rights to the file referenced in the error message.

Specifically, be sure you are logged in to the computer where the OracleAS Metadata Repository is running as the same user who installed the Release 2 (9.0.2) or 10*g* (9.0.4) OracleAS Metadata Repository.

If you are logged in as the appropriate user, note the name of the problem file and contact Oracle support.

Error: MRUA was unable to dynamically load plugins

Cause: The Metadata Repository Upgrade Assistant was unable to load a required plugin, which is part of the MRUA software designed upgrade a specific component schema.

Action: Contact Oracle Support.

Error initializing plug-in

Cause: The Metadata Repository Upgrade Assistant was unable to initialize a required plugin, which is part of the MRUA software designed upgrade a specific component schema.

Action: Contact Oracle Support.

Error: Component upgrade failed

Cause: The Metadata Repository Upgrade Assistant was unable to upgrade one of the Oracle Application Server components.

Action: Review the MRUA log files to determine which component upgrade failed and then contact Oracle Support.

For more information, see Section D.2, "Reviewing the MRUA Log Files".

Error: Component upgrade returned improper status

Cause: The Metadata Repository Upgrade Assistant was unable to determine whether or not one of the Oracle Application Server components was upgraded successfully.

Action: Review the MRUA log files to determine which component generated the improper status and then contact Oracle Support.

SQL script ***script_name*** **does not exist!**

Cause: A required file is missing or cannot be read by the Metadata Repository Upgrade Assistant.

Action: Be sure you are logged in to the computer as the same user who installed the Release 2 (9.0.2) or 10*g* (9.0.4) OracleAS Metadata Repository. The account you are using to run MRUA must have access rights to all the upgrade files.

If you are running from the OracleAS Metadata Repository Upgrade Assistant and Utilities CD–ROM, be sure the CD is mounted properly.

Contact Oracle Support.

Warning: Verify that database version *database_version* has been certifed with AS

Cause: You are attempting to run the Metadata Repository Upgrade Assistant against a database that was not yet certified with OracleAS when the release shipped.

Action: Review Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository" for detailed information about the database version requirements.

Unable to load PL/SQL package DBMS_IAS_UPGRADE

Cause: The Metadata Repository Upgrade Assistant was unable to load a required PL/SQL package.

Action: Be sure you are logged in to the computer as the same user who installed the Release 2 (9.0.2) or 10*g* (9.0.4) OracleAS Metadata Repository. The account you are using to run MRUA must have access rights to all the upgrade files.

If you are running from the OracleAS Metadata Repository Upgrade Assistant and Utilities CD–ROM, be sure the CD is mounted properly.

Contact Oracle Support.

Unable to load PL/SQL package DBMS_IAS_VERSION

Cause: The Metadata Repository Upgrade Assistant was unable to load a required PL/SQL package.

Action: Be sure you are logged in to the computer as the same user who installed the Release 2 (9.0.2) or 10*g* (9.0.4) OracleAS Metadata Repository. The account you are using to run MRUA must have access rights to all the upgrade files.

If you are running from the OracleAS Metadata Repository Upgrade Assistant and Utilities CD–ROM, be sure the CD is mounted properly.

Contact Oracle Support.

Protocol error: Plug-in raised an exception:

Cause: A software error has occurred while upgrading one of the Oracle Application Server component schemas.

Action: Review the MRUA log files to determine which component failed, and then contact Oracle Support.

For more information, see Section D.2, "Reviewing the MRUA Log Files".

FAILURE: Some OracleAS plug-ins report failure during upgrade.

Cause: One or more Oracle Application Server component upgrades have failed.

Action: Review the MRUA log files to determine which components failed. For more information, see Section D.2.1, "Guidelines for Using the MRUA Log Files".

Error: Upgrade from OracleAS release *release_number* is not allowed

Cause: You attempted to upgrade from a release that is not supported for this upgrade operation.

Action: Review Chapter 2, "Oracle Application Server Upgrade Concepts" for information about the supported upgrade paths.

Error: Some OracleAS components not set to VALID status in app_registry. Check mrua.log file

Cause: One or more of the Oracle Application Server components returned a status that is not valid.

Action: Review the MRUA log files to determine which component failed; then, contact Oracle Support.

For more information, see Section D.2, "Reviewing the MRUA Log Files".

Error: ***component_name*** **component version is:** ***release_version***

Cause: The Metadata Repository Upgrade Assistant cannot upgrade the schema for the Oracle Application Server component referenced in the error message because the version number for the component is invalid.

Action: Review the MRUA log files for any additional information; then, contact Oracle Support.

For more information, see Section D.2, "Reviewing the MRUA Log Files".

Error: SQL version and status query failed for component ***component_name***

Cause: The Metadata Repository Upgrade Assistant encountered an error when it attempted to verify the version number of the schema for the referenced component.

Action: Review the MRUA log files for any additional information; then, contact Oracle Support.

For more information, see Section D.2, "Reviewing the MRUA Log Files".

E.2 UDDI Registry OracleAS Metadata Repository Upgrade Error Messages

Error: Current UDDI Component has wrong version {0}.

Cause: UDDI database schema version is incorrect.

Action: Manually inspect the VERSION table in UDDISYS schema. You may need help from a system administrator or a database administrator.

Error: UDDI Upgrade is having problem with DB.

Cause: Some generic database exceptions have been thrown and caught.

Action: Contact the system administrator, the database administrator, or contact Oracle Support Services with the full error message.

Error: UDDI Upgrade is having problem closing DB Connection.

Cause: Exception generated while closing a database connection.

Action: Contact the system administrator, the database administrator, or contact Oracle Support Services with the full error message.

Error: UDDI Upgrade sql script execution failed.

Cause: Exception during UDDI upgrade-related SQL execution.

Action: Contact the system administrator, the database administrator, or contact Oracle Support Services with the full error message.

Error: UDDI Upgrade sqlldr execution failed.

Cause: Exception during Oracle SQL*Loader execution.

Action: Contact the system administrator, the database administrator, or contact Oracle Support Services with the full error message.

E.3 Portal Repository Upgrade Messages

This section contains error messages that are specific to the OracleAS Portal Repository upgrade. Error messages that are generated after the upgrade has progressed past the precheck stage indicate that the OracleAS Portal schema has had modifications. If you receive any error messages after the precheck step, you must fix the problem, restore your database from its backup, and then run the upgrade again. This section contains the following subsections:

- Numbered Error Messages (WWU-00001 to WWU-24999)
- Numbered Warning Messages (WWU-25000 to WWU-49999)
- Unnumbered Error Messages
- Unnumbered Warning Messages

E.3.1 Numbered Error Messages (WWU-00001 to WWU-24999)

WWU-00001: An unexpected exception was raised during the upgrade prechecks:

Cause: An unexpected error caused the upgrade to abort.

Action: Based on the details in the message, correct the problem and run the upgrade again.

WWU-00002: The value of the shared_pool_size database parameter was not high enough for the upgrade.

Cause: The value of the shared_pool_size database parameter is too low.

Action: Increase the value of the shared_pool_size database parameter to 20 MB or greater. Run the upgrade again.

WWU-00003: The value of the java_pool_size database parameter was not high enough for the upgrade.

Cause: The value of the java_pool_size database parameter is too low.

Action: Increase the value of the java_pool_size database parameter to 20 MB or greater. Run the upgrade again.

WWU-00004: The optimizer_mode database parameter was incorrectly set to RULE.

Cause: The optimizer_mode database parameter is incorrectly set to RULE.

Action: Change the optimizer_mode database parameter to CHOOSE. Run the upgrade again.

WWU-00005: There was insufficient free space in the default tablespace.

Cause: There is less than 20 MB of free default tablespace.

Action: Create at least 20 MB of free default tablespace. Run the upgrade again.

WWU-00006: There was insufficient free space in the temporary tablespace.

Cause: There is less than 10 MB of free temporary tablespace.

Action: Create at least 10 MB of free temporary tablespace. Run the upgrade again.

WWU-00007: The _system_trig_enabled database parameter was incorrectly set to FALSE.

Cause: The _system_trig_enabled database parameter is incorrectly set to FALSE.

Action: Set the value for the _system_trig_enabled database parameter to TRUE, or do not set it. Run the upgrade again.

WWU-00008: There were jobs running in the DBMS jobs queue during the upgrade.

Cause: The upgrade cannot progress because there are DBMS jobs running.

Action: Either kill the DBMS jobs, or wait for them to finish before restarting the upgrade. Check the "Analyze Product Schema" step in the upgrade log for more information on the running jobs.

WWU-00009: The DBMS job queue was disabled. There were jobs that would have run immediately if it were enabled.

Cause: Jobs submitted for the current repository may not run properly under the upgraded version.

Action: You have two options: 1. Remove the jobs from the queue. 2. Re-enable the job queue by raising the job_queue_processes database parameter to a value greater than 0, and allow the jobs to complete. For a list of all jobs, look under the "Analyze Product Schema" step in the upgrade log.

WWU-00010: Some jobs in the DBMS job queue were incorrectly configured.

Cause: There are OracleAS Portal jobs in the DBMS job queue that were either incorrectly submitted as another user, or submitted as the OracleAS Portal user with another default schema or default privilege.

Action: Remove these jobs from the job queue. The upgrade correctly resubmits any jobs that are missing. For a list of all jobs, look under the "Analyze Product Schema" step in the upgrade log.

WWU-00011: Concurrent sessions were running for the schema you are upgrading.

Cause: Other sessions are running on the OracleAS Portal schema.

Action: Make sure the OracleAS 10g middle-tier is shut down and there are no other connections to the schema being upgraded. Look under "Open Sessions" in the upgrade log for a list of open sessions for the schema.

WWU-00012: Not all components of the JVM installation were present in the database or valid.

Cause: SYS Java objects are not present in the database or are invalid.

Action: Recompile the invalid Java objects in SYS. If this fails, reinstall the JVM in the database following the instructions found in the Oracle database documentation.

WWU-00013: Tables with UPG_ prefix were found in the OracleAS Portal schema.

Cause: The upgrade is aborted when UPG_ prefix tables are present in the OracleAS Portal schema.

Action: Back up all tables with the UPG_prefix, then delete them from the OracleAS Portal schema.

WWU-00014: Obtaining Oracle Text information failed.

Cause: An error occurred during the attempt to retrieve information about the Oracle Text installation.

Action: Ensure that the Oracle Text component is correctly installed. If necessary, reinstall the Oracle Text component. For installation instructions, refer to the *Oracle Application Server Portal Configuration Guide*.

WWU-00015: Oracle Text schema (CTXSYS) does not exist.

Cause: The database does not contain the CTXSYS schema. This indicates that Oracle Text is not installed.

Action: Install the Oracle Text component in the database. For installation instructions, refer to the *Oracle Application Server Portal Configuration Guide*.

WWU-00016: Oracle Text indextype is invalid or does not exist.

Cause: The Oracle Text context indextype is not valid or does not exist. This may indicate a problem with the Oracle Text installation.

Action: Ensure the Oracle Text context indextype is present and valid. If necessary, reinstall the Oracle Text component. For installation instructions, refer to the *Oracle Application Server Portal Configuration Guide*.

WWU-00017: Some Oracle Text packages are invalid.

Cause: Packages in the Oracle Text schema (CTXSYS) that begin with DRI or CTX_ are invalid.

Action: Revalidate the Oracle Text invalid packages. If necessary, reinstall the Oracle Text component. For installation instructions, refer to the *Oracle Application Server Portal Configuration Guide*.

WWU-00018: Oracle Text version does not match the database version.

Cause: The version of the database is more recent than the Oracle Text component. This may indicate that the Oracle Text component upgrade was not successful. Oracle Text manual upgrade steps may have failed or been omitted. On some platforms, this may also indicate that patch 2658339 was not applied.

Action: Depending on the situation, either rerun the Oracle Text upgrade or download and apply the patch.

WWU-00019: Could not find the schema(s) on which Portlet Builder (Web View) applications are based.

Cause: The schema on which the Portlet Builder application is based is missing.

Action: There are two ways to fix this issue: 1. Drop the applications that are using the schema. 2. Recreate the missing schema and all objects in it.

WWU-00020: One or more one-off patches with schema changes have been applied.

Cause: One or more one-off patches that include schema changes have been applied to the OracleAS Portal schema. The upgrade cannot proceed because these changes have not been tested with this release of the upgrade scripts.

Action: See if a version of the upgrade based on the next patchset has been released on Metalink. If so, download and run the new version. If not, wait until it is released.

WWU-00021: The following mandatory object(s) are missing or invalid:

Cause: Mandatory objects that OracleAS Portal relies on are invalid or are not present in the database. If they are missing due to a faulty upgrade of the database, this could also cause failures in the OracleAS Portal upgrade.

Action: Review the database installation and upgrade procedures. If the object is present but invalid, run the rdbms/admin/utlrp.sql script under the database Oracle home to recompile all invalid objects.

WWU-00022: Version %0 of Oracle Portal/WebDB is not supported for upgrade.

Cause: The OracleAS Portal version being upgraded is not supported by this upgrade installation.

Action: If your OracleAS Portal instance is version 9.0.2, 9.0.2.3, or 9.0.2.6, be sure you have followed the instructions for applying Patch 2778342 mentioned in the Oracle Application Server 10g Upgrading to 10g Release 2 (10.1.2) upgrade guide.

If you are starting with version 3.0.9, follow the instructions on http://portalcenter.oracle.com/upgrades to upgrade to version 9.0.4. If you are running a different version, it is not supported by this upgrade installation. Contact Oracle support.

WWU-00023: Version %0 of Oracle Database is not supported for upgrade.

Cause: The version of the database against which the upgrade was run is not supported for this upgrade.

Action: Upgrade to the minimum database version of Oracle9i Database 9.0.1.5 Enterprise or Standard edition.

WWU-00024: The compatible database parameter is less that 9.0.0.

Cause: The compatible database parameter is set to less than 9.0.0.

Action: Set the value of the compatible database parameter to at least 9.0.0.

WWU-00025: VPD was not installed properly.

Cause: One of the VPD checks has failed.

Action: This error is followed by a detailed message. Resolve the issue by examining the information provided in the message.

WWU-00026: VPD context value is not set.

Cause: The OracleAS Portal login trigger that sets the VPD context is disabled or is not installed.

Action: Verify that the OracleAS Portal login trigger was installed and enabled on the database. If you must install the trigger, run the wwhost/logintrg.sql script from SQL*Plus while logged in as SYS user. You'll find this script under the upgrade directory.

WWU-00027: VPD context value is incorrect.

Cause: The login trigger(s) is not setting the correct context.

Action: Verify that the login trigger is correctly installed. To install the trigger, run the wwhost/logintrg.sql script from SQL*Plus while logged in as SYS user. You'll find this script under the upgrade directory.

WWU-00028: Portal schema user is not set up to use VPD.

Cause: The OracleAS Portal schema user has the EXEMPT ACCESS POLICY system privilege.

Action: Revoke the EXEMPT ACCESS POLICY privilege from the OracleAS Portal schema user by running the following SQL command in SQL*Plus: 'REVOKE EXEMPT ACCESS POLICY FROM PORTAL_SCHEMA_NAME;'. In this command, replace PORTAL_SCHEMA_NAME with the actual OracleAS Portal schema name. Also verify that the OracleAS Portal schema user does not inherit the EXEMPT ACCESS POLICY privilege from any of its assigned roles.

WWU-00029: VPD is not being enforced in the database.

Cause: A problem occurred in the database that caused the VPD check to fail.

Action: Consult the database documentation to find possible actions.

WWU-00031: %0 Unable to bind as the application.

Cause: An error was encountered while connecting to the Oracle Internet Directory server.

Action: The error message above may provide more information about the cause. Make sure that the Oracle Internet Directory server is up and running on host %1 and port %2 and OracleAS Portal has been wired correctly against it.

WWU-01000: Back up the database before running the upgrade.

Cause: You have answered n (no) when asked if the schema has been backed up.

Action: Back up the database, and restart the upgrade.

WWU-01001: Connection to the Portal repository failed.

Cause: Incorrect OracleAS Portal schema, password, or connect string.

Action: Supply the correct OracleAS Portal schema, password, and connect string.

WWU-01002: Connection as SYS to the Portal repository failed.

Cause: An invalid SYS password was supplied, or the orapw file is missing.

Action: Supply the correct SYS password. If the password is correct, verify that you can connect remotely to SYS as SYSDBA using an orapwSID file. Refer to the Oracle database documentation for instructions on creating an orapw file.

WWU-01003: An unexpected exception was raised:

Cause: An unexpected error caused the upgrade to abort.

Action: Based on the details in the message, correct the problem, restore the database from backup, and run the upgrade again.

WWU-01004: Missing strings reported in %0 file:

Cause: The sqlldr utility encountered issues when trying to load message translation data.

Action: Look for specific issues in the .bad file and the corresponding .log file in the upgrade tmp directory. Give these to Oracle Customer Support along with the upgrade logs.

WWU-01005: Version not updated, fatal errors found in upgrade log.

Cause: This message indicates that the earlier version of OracleAS Portal will not be updated to the new version. Errors have occurred in the upgrade that will prevent OracleAS Portal from functioning properly. A summary of the errors is listed at the end of the upgrade log.

Action: Search through the errors in the log and apply any fixes mentioned. Then restore the database from backup and run another upgrade. If this fails, or if unexpected errors are encountered, contact Oracle Customer Support.

WWU-01007: Unable to create directory %0.

Cause: You do not have the required permissions to create the directory.

Action: Change the permissions on the parent directory.

WWU-01008: Write permission not available for directory %0.

Cause: You do not have the required permissions to write to the directory.

Action: Change the permissions on the directory, or specify a different temporary directory, then rerun the upgrade.

WWU-01009: Unable to create %0. Check permissions on the directory.

Cause: The permissions on the temporary directory do not allow the creation of a login.sql script for the user profile.

Action: Change the permissions on the temporary directory, and run the upgrade again.

WWU-01010: SQL*Plus version %0 not supported for upgrade.

Cause: The version of SQL*Plus you are trying to execute is not supported for this upgrade.

Action: Verify that the version of bin/sqlplus under the Oracle Home is at least 9.0.1.

WWU-01011: Restart the upgrade.

Cause: You have answered n (no) when asked if input details are correct.

Action: Correct the input details, and restart the upgrade.

E.3.2 Numbered Warning Messages (WWU-25000 to WWU-49999)

WWU-25000: Removed session cleanup job: %0 from the SYS schema.

Cause: The session cleanup job usually exists in the OracleAS Portal schema. However, an earlier operation, such as the database upgrade, has resulted in removing this job as a part of the upgrade.

Action: If the database instance where the upgrade is being performed does not contain any other OracleAS Portal schema, then no action is required. This is because the session clean-up job gets created in the OracleAS Portal schema during upgrade. However, if there are other OracleAS Portal schemas in the database instance, then verify that they all have their respective session clean-up jobs. Run the script wwc/ctxjget.sql under the upgrade directory from SQL*Plus in an OracleAS Portal schema to check whether the session clean-up job exists. If this job is missing in any OracleAS Portal schema, then you can create it by running the script wwc/ctxjsub.sql in that schema from SQL*Plus.

WWU-25001: VPD check found some issues.

Cause: One of the VPD checks has failed.

Action: This warning is followed by a detailed message. Resolve the issue by examining the information provided in the message.

WWU-25003: Portlet Builder (WebView) components have unknown issues.

Cause: The Portlet Builder components (packages) are invalid.

Action: Try resolving the cause of the errors when compiling the packages that are listed in the log. For example, a report may be based on a table that has been dropped. In this case, the report is no longer valid, so you can drop the report.

WWU-25004: Only %0% of the components in the wwv_modules$ table are production components.

Cause: This informational message indicates that there is a relatively large number of archive versions of Portlet Builder components (formerly WebView). This may be because in Oracle9iAS Portal 3.0.9, a new version of a component was created each time the component was edited and saved.

Action: Delete as many of the archive versions of components as possible. This reduces the size of the tables where attributes for all the archive versions are stored.

WWU-25005: Table without VPD policy: %0

Cause: The VPD policy on the table indicated in the message was not installed properly in the OracleAS Portal schema.

Action: If the table indicated in the message is not part of the OracleAS Portal product, it is safe to ignore the warning.

WWU-26000: Component %0 has errors. Check that all the objects it is based on are present.

Cause: The component is based on one or more missing objects. For example, a Query By Example report was based on table MY_TABLE. Then MY_TABLE is dropped.

Action: Supply the missing object. If the component is no longer being used, delete it using the OracleAS Portal Navigator.

WWU-26001: Non-Portal objects have errors. See %0 for details.

Cause: Non-OracleAS Portal objects in the OracleAS Portal schema cannot be compiled and have errors.

Action: Find out what is causing the object not to compile, and rectify it.

E.3.3 Unnumbered Error Messages

An unexpected exception was raised: <exception and where it occurred>

Cause: An unexpected error caused the script to abort.

Action: Based on the details in the message, correct the problem, restore your database from its backup and run the upgrade script again.

An unexpected exception was raised during the upgrade prechecks: <exception where it occurred>

Cause: An unexpected error caused the script to abort.

Action: Based on the details in the message, correct the problem and run the upgrade script again. For example:

If the following lines are found in the log, then the error may be because Oracle Text is not installed correctly.

```
### PHASE I STEP 8: Perform pre upgrade checks
Upgrade step started at Fri Apr 4 02:28:18 2003
Running upg/common/utlchvpd.sql
Connected
Calling DoPreChecks()
Starting precheck at Fri Apr 4 02:28:21 2003
Calling upg/common/sysuppre.sql
Connected.
```

ERROR: An unexpected exception was raised during the upgrade prechecks:

```
ORA-00942: table or view does not exist
----- PL/SQL Call Stack -----
object handle line number object name
80bc68c4 76 anonymous block
80bc68c4 380 anonymous block
```

Verify if the Oracle Text component is installed and reinstall it if it does not exist. Refer to the Oracle Application Server Portal Configuration Guide.

Back up your database before running the upgrade.

Cause: You have answered n (no) when asked if the schema has been backed up.

Action: Back up the database and restart the script.

Connection as SYS to the Portal repository failed.

Cause: An invalid SYS password was supplied or the orapw file is missing.

Action: Supply the correct SYS password.If the password is correct, make sure you can connect to SYS as `sysdba` by creating a `orapw<SID>` file in the database Oracle Home's `dbs` directory by running orapwd with the same password used by the SYS database account.

Connection to the Portal repository failed.

Cause: Incorrect Oracle9*i*AS Portal schema, password or connect string.

Action: Supply the correct Oracle9*i*AS Portal schema, password or connect string.

Dropping Oracle Text Indexes has failed, upgrade cannot continue.

Cause: Dropping the Oracle Text indexes, or removing the synchronization or optimization jobs has failed. Find the output of the `uptxtdrp` script in the upgrade log to see what should be done. The entire `uptxtdrp.log` is appended to the error message output in the upgrade log.

Action: If the error was encountered while dropping the Oracle Text indexes, make sure that all the Oracle Text indexes are dropped before restarting the upgrade. For information about dropping Oracle Text indexes, refer to the *Index Maintenance* chapter of the *Oracle Text Application Developer's Guide*.

If the error was encountered while removing the synchronization or optimization jobs, make sure that these jobs are removed from the job queue before restarting the upgrade. For information about breaking or removing jobs, refer to the *Managing Job Queues* chapter of the *Oracle9i Database Administrator's Guide*.

After upgrading, manually recreate the Oracle Text indexes and the synchronization and optimization jobs if you wish to use Oracle Text searching in your OracleAS Portal. Refer to the Oracle Application Server Portal Configuration Guide for complete instructions.

Environment variable ORACLE_HOME is not set.

Cause: The ORACLE HOME environment variable is not set.

Action: Review your environment and set the Oracle Home environment variable.

Error: Could not determine the version of OracleAS Portal

Cause: An error occurred while determining the version of OracleAS Portal.

Action: This message is followed by the actual exception, which occurred. Resolve the error by examining the information provided and run MRUA again.

Error: OracleAS Portal version {0} is not supported for upgrade on Oracle Database 10g

Cause: The OracleAS Portal version must be at least 9.0.2.3.

Action: Download the Oracle9*i*AS 9.0.2.3 patchset from Metalink and apply it on your application server infrastructure and middle-tier. Then run the upgrade again.

Failed to rename <*file/directory*>

Cause: You do not have the required permissions on the parent directory.

Action: Change the permissions on the parent directory.

Getting password of <*schema-name*> schema

Cause: Failed to retrieve the password of the schema <*schema-name*>.

Action: The error is followed by the actual exception which occurred. Try to fix the error and restart the upgrade.

granting execute on <schema>.<procedure> to <application_schema> as <schema>--ORA-01001:invalid cursor

Cause: The schema or procedure is missing. For example:

```
ERROR: granting execute on SCHEMA1.CHECK_SAL to SCHEMA1B as
SCHEMA1--ORA-01001:invalid cursor
```

In this case, there is a form in a database provider based on `SCHEMA1B`, on the procedure `SCHEMA1.CHECK_SAL` and either the procedure `CHECK_SAL` is missing or one of the schemas `SCHEMA1` or `SCHEMA1B` is missing. Therefore, the form will not run. However, it would not have run before the upgrade either.

Action: Determine if the form or database provider is obsolete. If it is obsolete, delete it. If not, supply the missing schema or procedure.

GUID and/or DN are not available for %string% subscriber.

Cause: Could not get the globally unique identifier and/or the distinguished name for the named identity management realm from the Portal repository.

Action: Make sure that the identity management realm has been configured properly.

Invalid profile status value: %string%

Cause: The value specified for profile status is invalid.

Action: Please use only ENABLED or DISABLED for the profile status.

Missing strings reported in <filename> file: <strings>

Cause: `SQLLDR` encountered issues when trying to load the languages.

Action: Look at the corresponding log and the `.log` and `.bad` files from `<upgrade_tmp_dir>` for specific issues. Give these to Oracle Support along with the upgrade logs.

Obtaining Oracle Text information failed. Please check Oracle Text has been correctly installed. Reinstall Oracle Text schema (CTXSYS) if necessary.

Cause: An error has occurred whilst attempting to retrieve information about the Oracle Text installation.

Action: Ensure the Oracle Text component is correctly installed. If necessary, reinstall the Oracle Text component. Refer to the *Oracle Application Server Portal Configuration Guide* for complete instructions.

ORA-04031: unable to allocate <n> bytes of shared memory ("shared pool","unknown object","session heap","frame segment") (WWC-44847)

Cause: The shared pool size database parameter is too small.

Action: The value for this parameter depends on the size of your Oracle9*i*AS Portal. It may need to be several hundred megabytes for large Oracle9*i*AS Portals to avoid encountering this problem. Increase the shared pool size in your database and restart your upgrades after restoring from a backup.

ORA-1031: insufficient privileges

Cause: The sysdba connection to the database has failed due to insufficient privileges.

Action: To connect to SYS as sysdba, create the `orapw<SID>` file in the database Oracle Home's dbs directory by running `orapwd` with the same password used by the SYS database account.

ORA-29521: referenced name javax/ejb/<class> could not be found

Cause: The instructions contained in Metalink Note 222437 to facilitate Oracle9*i*AS Portal working on an Oracle 9.2 database have not yet been applied. Here is an example of the error:

```
Loading Java Classes - soap.jar
errors : class oracle/soap/providers/ejbprov/<class>
ORA-29521: referenced name javax/ejb/<name> could not be found
The following operations failed
class oracle/soap/providers/ejbprov/<provider>: resolution
exiting : Failures occurred during processing
```

Action: Restore your repository back to its Oracle9*i*AS Portal 9.0.2 state and follow the instructions contained in the Metalink Note 222437.1 available from the Oracle Metalink Web site at `http://metalink.oracle.com`. Run the upgrade again after the steps have been completed.

Oracle Text indextype is invalid or does not exist. Revalidate the invalid indextype. If necessary, reinstall the Oracle Text schema (CTXSYS).

Cause: The Oracle Text context indextype is not valid or does not exist. This may indicate a problem with the Oracle Text installation.

Action: Ensure the Oracle Text context indextype is present and valid. If necessary, reinstall the Oracle Text component. Refer to the Oracle Application Server Portal Configuration Guide.

Oracle Text schema (CTXSYS) does not exist, please install it.

Cause: The database does not contain the CTXSYS schema. This indicates that Oracle Text is not installed.

Action: Install the Oracle Text component in the database. Refer to the Oracle Application Server Portal Configuration Guide.

Oracle Text version does not match the database version. Check that Oracle Text has been correctly upgraded. Reinstall the Oracle Text schema (CTXSYS) if necessary.

Cause: The database version is more recent that the Oracle Text component. This may indicate that the Oracle Text component was not upgraded correctly. The Oracle Text manual upgrade steps may have been omitted or failed. However, on certain platforms, this may also indicate that patch 2658339 has not been applied.

Action: Run the Oracle Text upgrade again or download and apply the patch depending on your situation.

OracleAS Portal 9.0.2 -> 9.0.4 upgrade failed. See <*upgrade-log-file*> for details.

Cause: Errors were encountered in the 9.0.2 to 9.0.4 portion of the upgrade.

Action: Search through the errors in the log file and make a note of any fixes mentioned. Then restore the database from backup, apply the fixes, and run the upgrade again.

OracleAS Portal 9.0.2 -> 9.0.4 upgrade precheck failed. See <*precheck-log-file*> for details.

Cause: Errors were encountered during the precheck run of the 9.0.2 to 9.0.4 portion of the upgrade.

Action: Search through the errors in the log file and apply any fixes mentioned. Then run the upgrade again.

OracleAS Portal 9.0.4 -> 10.1.2 upgrade completed with errors. See <*upgrade-log-file*> for details.

Cause: Errors were encountered in the 9.0.4 to 10.1.2 portion of the upgrade.

Action: Search through the errors in the log file and make a note of any fixes mentioned. Then restore the database from backup, apply the fixes, and run the upgrade again.

OracleAS Portal 9.0.4 -> 10.1.2 upgrade precheck failed. See <*precheck-log-file*> for details.

Cause: Errors were encountered during the precheck run of the 9.0.4 to 10.1.2 portion of the upgrade.

Action: Search through the errors in the log file and apply any fixes mentioned. Then run the upgrade again.

Patch Failed with status code: <status>

Cause: A patch installation has failed.

Action: Look at the upgrade log file for details.

Please delete all tables with UPG_ prefix from the Portal schema.

Cause: `UPG_ prefix` tables exist in the Oracle9*i*AS Portal schema. The upgrade is aborted.

Action: Delete all tables with the `UPG_ prefix` from the Oracle9*i*AS Portal schema. Backup the tables before removing them.

Portal schema user is not set up to use VPD.

Cause: The Oracle9*i*AS Portal schema user has the EXEMPT ACCESS POLICY system privilege.

Action: Revoke the EXEMPT ACCESS POLICY privilege from the Oracle9*i*AS Portal schema user by running the following SQL command in SQL*Plus:

```
revoke exempt access policy from <portal_schema_user>;
```

Also verify the Oracle9*i*AS Portal schema user does not inherit the EXEMPT ACCESS POLICY privilege from any of its assigned roles.

Portal version not supported by VPD check utility.

Cause: The VPD check does not support your current version of Oracle9*i*AS Portal.

Action: Verify your Oracle9*i*AS Portal version is supported by this upgrade.

Post-Upgrade tasks not done, fatal errors found in upgrade log.

Cause: This message indicates that the post upgrade scripts have not been executed. These tasks require a completed upgrade and your upgrade has errors. A summary of the errors are listed at the end of the upgrade log.

Action: Attempt to fix any errors listed. Search through this chapter and apply any fixes mentioned. Then restore from your backup and run another upgrade. If this fails, contact Oracle Support.

An example of a post-upgrade task is checking whether VPD is enabled correctly. Another example of a post-upgrade task is verifying if the SSO Partner Configuration has been run.

Problem running sqlplus.

Cause: The upgrade script was unable to execute the SQL*Plus command.

Action: Make sure that `bin/sqlplus` exists under your Oracle Home, and that you have permissions to execute it.

Restart the upgrade script.

Cause: You have answered n (no) when asked if input details are correct.

Action: Correct the perceived problem and restart the upgrade script.

Simultaneous upgrades cannot be run from the same location.

Cause: You are trying to run multiple simultaneous upgrades from the same location.

Action: Wait until the upgrade you started earlier finishes before starting another one. If a previous upgrade (run using `upgrade.csh`) terminated abnormally (for example, with `Ctrl+C`), the lock file created during upgrade (`upgcsh.lok`) is not deleted. Therefore, if you attempt to start another upgrade, you will see this message. In this case you will need to manually delete the lock file. You should delete this lock file only when an upgrade has abnormally terminated, not if an upgrade is actually running. You can find the lock file in the location from where you ran the upgrade script.

Some Oracle Text packages are invalid. Revalidate the invalid packages. If necessary, reinstall the Oracle Text schema (CTXSYS).

Cause: Packages in the Oracle Text schema (`CTXSYS`) beginning with `DRI` or `CTX_` are invalid.

Action: Revalidate the Oracle Text invalid packages. If necessary, reinstall the Oracle Text component. Refer to the Oracle Application Server Portal Configuration Guide.

SQL Error: %*string*% LDAP Error: %*string*%. Unexpected Error occured while connecting to the Oracle Internet Directory as Application entry.

Cause: An attempt was made to connect to the Oracle Internet Directory using the application credentials stored in the OracleAS Portal repository. However, this attempt failed. Some possible reasons for this failure are given below:

- OracleAS Portal has not been configured correctly for the Oracle Internet Directory.
- Oracle Internet Directory server is not running.
- An unexpected error was encountered.

Action: Make sure that the Oracle Internet Directory is up and running. Reconfigure OracleAS Portal for the Oracle Internet Directory. Also review the message logged before this error message and take appropriate action.

SQL*Plus version <version> not supported for upgrade.

Cause: The version of SQL*Plus you are trying to execute is not current enough.

Action: Verify that the version of `bin/sqlplus` under your Oracle Home is at least 9.0.1.

System triggers are disabled in the database.

Cause: System triggers are disabled in your database configuration file.

Action: Verify that the `_system_trig_enabled` parameter is set to TRUE in your database's `init.ora` file. If it is not, set it to TRUE and restart your database.

The allocated java_pool_size parameter for the database is not sufficient for the Installation/Upgrade. Increase the java_pool_size and run the upgrade again.

Cause: The java pool size parameter is too small.

Action: Increase the java pool size parameter to 20 MB or greater. Refer to the documentation, if necessary, then run the upgrade again.

The allocated shared_pool_size parameter for the database is not sufficient for the Installation/Upgrade. Increase the shared_pool_size and run the upgrade again.

Cause: The shared pool size parameter is too small.

Action: Increase the shared pool size to 20 MB or greater. Refer to the documentation, if necessary, then run the upgrade again.

The compatibility level of the database is not supported for upgrade.

Cause: If the compatible init parameter is not set to at least 9.0.0, then the upgrade aborts.

Action: Set the compatible init parameter to at least 9.0.0 in your `init.ora` file.

The database blocksize is less than the recommended value.

Cause: The database blocksize is less than 8K.

Action: Create a new Oracle9*i* database with a minimum blocksize of 8K. Use the database import/export utilities to move your Oracle9*i*AS Portal from your prior database to the new one.

The DBMS job queue is disabled, and there are jobs which would run immediately if it were enabled. Please re-enable the job queue and wait for these jobs to complete, or remove them, before restarting the upgrade.

Cause: Jobs submitted under a previous version of Oracle9*i*AS Portal may not run properly under OracleAS Portal 9.0.4 and higher.

Action: Re-enable the job queue and allow the jobs to complete, or remove them.

The following invalid Portal objects exist in the Portal schema:

Cause: There are invalid Oracle9*i*AS Portal objects in the Portal schema.

Action: Investigate the invalid Oracle9*i*AS Portal objects in the Oracle9*i*AS Portal schema and fix the source of the problem. Run the upgrade again.

The following mandatory object(s) are missing or invalid: <[obj_type]owner.obj_name>

Cause: Mandatory objects which Oracle9*i*AS Portal relies on are not present in the database or are invalid. If they are missing due to a faulty upgrade of the database, it could cause failures in the Oracle9*i*AS Portal upgrade as well.

Action: Review your database installation and upgrade procedures. If the object is present but invalid, run the utlrp.sql script located in rdbms/admin of your database Oracle Home in an installation to recompile all invalid objects in the database.

The Java Option is not enabled in the chosen database. This product installation requires the Java option of the database to be enabled. Enable the Java Option and run the upgrade again.

Cause: Java is not installed in the database or there was a problem during the Java portion of the database upgrade.

Action: Enable the Java Option and run the upgrade again.

The JVM installation is not proper. Please check if you have the JVM installed or if there are invalid java objects in SYS

Cause: SYS java objects are not present in the database or are invalid.

Action: Recompile the invalid java objects in SYS. If this fails, reinstall the JVM in the database.

The LDAP parameters stored in the preference store are either incorrect or missing.

Cause: The OracleAS Portal repository has not been configured correctly for the Oracle Internet Directory.

Action: Please reconfigure OracleAS Portal repository for the Oracle Internet Directory.

The Optimizer Mode should not be set to RULE.

Cause: The optimizer mode is incorrectly set as `RULE`.

Action: Change the optimizer mode to `CHOOSE` and run the upgrade again.

The system triggers are not enabled. Set the _system_trig_enabled flag in the Oracle parameters file to TRUE and run the upgrade again.

Cause: The system triggers are not enabled.

Action: Set the system triggers enabled flag in the Oracle parameters file to TRUE and run the upgrade again.

There are concurrent sessions running for the schema you are upgrading.Verify that there are no other sessions running during the upgrade.

Cause: There are other sessions running on the Oracle9iAS Portal schema.

Action: Make sure your OracleAS 10*g* Release 2 (10.1.2) middle tier is shut down and no other connections are made to the schema being upgraded. Check the Analyze Product Schema step in the upgrade log for more information on the concurrent sessions.

There are currently jobs running in the DBMS jobs queue. Either kill them or wait for them to finish before restarting the upgrade.

Cause: There are DBMS jobs running.

Action: Either kill the DBMS jobs or wait for them to finish before restarting the upgrade. Check the Analyze Product Schema step in the upgrade log for more information on the running jobs.

There are currently jobs in the DBMS job queue which are incorrectly configured. Please remove these jobs before restarting the upgrade.

Cause: There are Oracle9*i*AS Portal jobs in the DBMS job queue which were either incorrectly submitted as another user, or submitted as the Oracle9*i*AS Portal user with another default schema or default privilege user.

Action: Remove these jobs from the job queue. The upgrade correctly resubmits any jobs that are missing.

There is not sufficient free space in the default tablespace.

Cause: There is less than 20MB of free default tablespace.

Action: Create at least 20MB of free default tablespace. Run the upgrade again.

There is not sufficient free space in the temporary tablespace.

Cause: There is less than 10M of free temporary tablespace.

Action: Create at least 10M of free temporary tablespace. Run the upgrade again.

Unable to bind as the application. LDAP Error: %string%

Cause: An error was encountered while connecting to the Oracle Internet Directory Server.

Action: The line following the error may provide more information about the cause. Make sure that the Oracle Internet Directory Server is up and running and the Portal has been wired correctly against it.

Unable to create directory <upgrade_tmp_dir>

Cause: You do not have permissions to create the temporary directory.

Action: Change your permissions on the parent directory.

Unable to create <log_file_name>. Check permissions on the directory.

Cause: The upgrade log file could not be created.

Action: Change your permissions on the directory where the upgrade log is written or specify a different log file location and run the upgrade again.

Unable to create <user_profile>. Check permissions on the directory.

Cause: The permissions on the temporary directory do not allow the creation of a login.sql script for the user profile.

Action: Change your permissions on the temporary directory and run the upgrade again.

Unable to get the application GUID. LDAP Error: %string%

Cause: Could not get the globally unique identifier for the application entry stored in the Oracle Internet Directory.

Action: The line following the error may provide more information about the cause. Make sure that the Oracle Internet Directory Server is up and running and the Portal has been wired correctly against it.

Unable to unbind. LDAP Error: %string%

Cause: An error was encountered while closing the connection with the Oracle Internet Directory.

Action: The line following the error may provide more information about the cause. Take corrective action as appropriate.

Updating External Application IDs: <string>

Cause: This is an internal error that may occur when converting the external application identifiers.

Action: Report this error to Oracle Support and provide them the output files for upgrade.

Updating provisioning profile: %string%

Cause: An error was encountered while updating the provisioning profile.

Action: The string may provide more information about the cause of error. Take appropriate action to resolve the error.

Unknown error happened in VPD check utility: <check_step>

Cause: An unexpected error happened during the specified step. A subsequent message following this one will contain details about the error.

Action: If the situation described in the details can be corrected, do so.

Version not updated, fatal errors found in upgrade log.

Cause: This message indicates that the version of Oracle9*i*AS Portal will not be updated to the new version. Errors have occurred in the upgrade which will prevent Oracle9*i*AS Portal from functioning properly. A summary of the errors is listed at the end of the upgrade log.

Action: Attempt to fix any errors listed. Search through this chapter and apply any fixes mentioned. Then restore from your backup and run another upgrade. If this fails, contact Oracle Support.

> **Note:** Only certain fatal errors are detected in this check. It is possible for the version to be updated even if other fatal errors are encountered.

Version <version> not supported for upgrades in this release.

Cause: Unsupported Oracle9*i*AS Portal version.

Action: Make sure you are running the upgrade on a supported Oracle9*i*AS Portal version (9.0.2.0, 9.0.2.2, 9.0.2.3, or 9.0.2.6).

Version <version> of Oracle Database is not supported for upgrade.

Cause: Incorrect RDBMS version.

Action: Upgrade to the minimum database version of Oracle9*i* Database 9.0.1.4 Enterprise or Standard editions.

Version <version> of Oracle Portal/WebDB is not supported for upgrade.

Cause: Incorrect Oracle9*i*AS Portal version.

Action: Make sure you are running on a supported Oracle9*i*AS Portal version (9.0.2.0, 9.0.2.2, 9.0.2.3, or 9.0.2.6).

VPD has not been installed properly.

Cause: One of the VPD checks has failed.

Action: This error is followed by a detailed message. Resolve the issue by examining the information provided in the message.

VPD is not being enforced in database.

Cause: A problem occurred in the database that caused the VPD check to fail.

Action: Consult your database documentation to find possible actions.

Write permission not available for directory <upgrade_tmp_dir>.

Cause: You do not have permissions to write to the temporary directory.

Action: Change your permissions on the temporary directory or specify a different temporary directory location and run the upgrade again.

E.3.4 Unnumbered Warning Messages

<n> session cleanup job(s) detected in the SYS schema.

Cause: The session cleanup job is a job that usually exists in the Oracle9*i*AS Portal schema. However, an earlier operation such as the database upgrade resulted in creating this job in the SYS schema. For example:

```
WARNING: 1 session cleanup job(s) detected in the SYS schema.
```

Action: This message is informational only. No action is required.

Component <APPLICATION_SCHEMA>.<COMPONENT_NAME> has errors. Please check that all the objects it is based on are present.

Cause: The component is based on one or more missing objects. For example, a QBE is created based on table `MY_TABLE`. Then `MY_TABLE` is dropped. For example:

```
WARNING: Component SCOTT.MY_QBE has errors. Please check that all the objects
it is based on are present.
```

Action: Supply the missing object. If the component is no longer being used, delete it using the OracleAS Portal Navigator.

Could not parse <select_statement> as <schema_name>

Cause: An object on which a Portlet Builder calendar is based is missing. This happens when:

- The table on which the calendar is based is missing.
- The schema on which the database provider containing the calendar is based on is missing.

Examples:

```
WARNING: Could not Parse select a1.HIREDATE the_date, a1.ENAME the_name, null
the_name_link, null the_date_link, null the_target from test_1.EMP_1 a1 order
by a1.HIREDATE as TEST_1.

WARNING: Could not Parse select b2.HIREDATE the_date, b2.ENAME the_name, null
the_name_link, null the_date_link, null the_target from test_2.EMP_2 b2 order
by b2.HIREDATE as TEST_2.
```

This warning usually occurs while upgrading a Oracle9*i*AS Portal which was created using Oracle export/import. Not all of the schemas on which the Portlet Builder components are based were imported. Calendars which show this warning cannot be used unless the missing objects are supplied, and the calendar component is regenerated.

Action: Supply the missing objects and regenerate the component.

Could not refresh OMNIPORTLET provider.

Cause: The refresh of the OminPortlet provider failed because the provider is not accessible.

Action: Verify that the OmniPortlet Web provider is accessible on the portal's middle-tier. After verification, refresh this provider from the Portlet Repository.

Default JPDK instance URL is not present. So, provider is registered using url http://host:port/.

Cause: At the time of upgrade, when the seeded OmniPortlet, Web Clipping, and OracleAS Portal Building Tools providers are registered, it is assumed that these providers are deployed on the same middle-tier as identified in the Default JPDK Instance URL. You can view this value by completing the following steps:

1. Log on to your OracleAS Portal.

2. Click the **Administer** tab.
3. In the Services portlet, click the **Global Settings** link.
4. Click the **Configuration** tab.
5. Locate the **Default JPDK Instance URL** field. Usually this value is `<portal_middle_tier_protocol>://<portal_middle_tier_host>:<portal_middle_tier_port>/jpdk/servlet/soaprouter/`. If there is no value in this field, you will receive the warning mentioned above in your upgrade log.

Action: Run the following script to update the URLs for these providers:

```
ORACLE_HOME/portal/upg/plsql/upg/9025-9026/wws/updmturl.sql
```

The script updates the middle-tier URL for the PORTLETBLDGTOOLS, OMNIPORTLET, and WEBCLIPPING providers in the providers table. This script is not run from the upgrade script. Run it in standalone mode to update the URLs. For example:

```
@updmturl.sql http my.domain.com 80
```

where:

- `http` is the middle-tier's protocol
- `my.domain.com` is the middle-tier's host
- `80` is the middle-tier's port

Document size for file <file_path> is null

Cause: The upgrade found an item on a page which appears to have a document attached but this document does not actually exist. This indicates a data inconsistency in the data for the item. The item will be upgraded but its document will not be accessible. It is unlikely that the document was accessible in Oracle9*i*AS Portal 9.0.2 either.

Action: Delete the item and recreate it.

External Application IDs have been updated. However, some customizations have been lost because of the large number of applications. Please reduce the number of external applications and ask the users to customize again.

Cause: You have a very large number of external applications. The customizations for these applications have exceeded the maximum physical limit for their storage. As a result, some customizations may have been lost.

Action: Reduce the number of external applications on the SSO server. Edit the defaults for the external applications portlet and advise the users to check their customizations.

Non Portal Objects have errors. See <upgrade_tmp_dir>/nonportal.log for details.

Cause: Non-Oracle9*i*ASPortal objects in the Oracle9*i*AS Portal schema cannot be compiled and have errors.

Action: Find out what is causing the object not to compile and rectify it. One reason these errors could occur is because deprecated or changed Oracle9*i*AS Portal APIs are being referenced and these APIs do not work in the latest release. Refer to the PDK information on `http://portalcenter.oracle.com`.

Only <n> % of components in wwv_modules$ table are production components.

Cause: This informational message indicates there are too many archive versions of Portlet Builder (formerly WebView) components. This may be because in Oracle9*i*AS Portal 3.0.9 a new version of a component was created each time the component was edited and saved. For example:

```
WARNING: Only 38 % of components in wwv_modules$ table are production
components.
```

Action: Delete as many of the archive versions of components as possible. This reduces the size of the tables where attributes for all the archive versions are stored.

Portlet Builder (WebView) components have unknown issues.

Cause: The Portlet Builder components (packages) are invalid.

Action: Try resolving the cause of the errors when compiling the packages listed in the log. For example, a report may be based on a table and the table has been dropped. In this case, the report is no longer valid, so you can drop the report.

Region ID = <region ID> on page ID = <page ID> and site ID = <site ID> was not converted to a sub-page links region

Cause: The region on the page was not successfully converted to a sub-page links region during the upgrade, since it contained items other than just the sub-page display items.

Action: The user must first move all the existing items in the region to a different region on the page. After making this change, the user can edit the region properties to convert it to a sub-page links region. Alternatively, a sub-page links region can also be created on the page.

Region ID = <region ID> on template ID = <template ID> and site ID = <site ID> was not converted to a sub-page links region

Cause: The region on the template was not successfully converted to a sub-page links region during the upgrade, either because there were items other than just the sub-page display items on the template itself, or on the pages based on the template. In this case, there were far too many items found in the region, so individual warnings for all pages based on the template could not be reported.

Action: The user must first move all the existing items in the region to a different region on the template/page. After making this change, the user can edit the region properties to convert it to a sub-page links region. Alternatively, a sub-page links region can also be created on the template.

Removed session cleanup job: <job_id> from the SYS schema.

Cause: The session cleanup job is a job that usually exists in the Oracle9*i*AS Portal schema. However, an earlier operation such as the database upgrade has resulted in removing this job as a part of the upgrade. For example:

```
WARNING: Removed session cleanup job: 63 from the SYS schema.
```

Action: If the database instance where the upgrade is being performed does not contain any other Oracle9*i*AS Portal schema, then no action is required. This is because the session cleanup job gets created in the Oracle9*i*AS Portal schema during upgrade. However, if there are other Oracle9*i*AS Portal schemas in the database instance, then it must be verified that they all have their respective session cleanup jobs. Run the following script from `sqlplus` in a Oracle9*i*AS Portal schema to check whether the session cleanup job exists:

```
ORACLE_HOME/portal/upg/plsql/wwc/ctxjget.sql
```

If this job is missing in any Oracle9*i*AS Portal schema then you can create it by running the script `ctxjsub.sql` from `sqlplus` in that schema, located in the same directory.

Subpage item (title: <item title>) on site id <site_id> and page <page_name> was not upgraded because other items exist in the same region.

Cause: The subpage item was obsoleted but could not be replaced by a subpage region type because there were other items in the same region.

Action: Create a new subpage type region on the page where the warning message appears.

Table without VPD policy: <table_name>

Cause: The VPD policy on the table indicated in the message was not installed properly in your Oracle9*i*AS Portal schema.

Action: If the table indicated in the message is not part of the Oracle9*i*AS Portal product, it is safe to ignore the warning. If the table is one of the following, it is also safe to ignore this warning:

- `WWPRO_OFFLINE_PRO_PORTLET$`
- `WWPRO_OFFLINE_PRO_PORTLET_NLS$`
- `WWPRO_PORTLET_METADATA_USER$`

In all other cases, there may have been a problem with a previous installation or upgrade procedure. Contact Oracle Support for more information.

Template region ID = <region ID> on page ID = <page ID> and site ID = <site ID> was not converted to a Sub-Page Links region

Cause: The region on the template was not successfully converted to a sub-page links region during the upgrade, either because there were items other than just the sub-page display items on the template itself, or on the pages based on the template.

Action: The user must first move out all the existing items in the region to a different region on the template/page. After making this change, the user can edit the region properties to convert it to a sub-page links region. Alternatively, a sub-page links region can also be created on the template.

The DBMS job queue is currently disabled. It must be re-enabled for proper Portal operation.

Cause: The DBMS job queue must be enabled for proper operation. It may have been disabled by setting the system parameter `job_queue_processes` to 0, or by restricting logins.

Action: Make sure `job_queue_processes` is set to one or greater, and that logins are not restricted by changing the system disable restricted session.

The following invalid non-Portal objects exist in the Portal Schema

Cause: Oracle9*i*AS Portal and non-Oracle9*i*AS Portal objects are compiled separately. For Oracle9*i*AS Portal objects, compilation problems are reported as errors. However, for non-Oracle9*i*AS Portal objects, compilation problems are reported as warnings, since they should not cause the upgrade to be considered a failure.

Action: Examine the generated file `<upgrade_tmp_dir>/nonportal.log` and fix the compilation problems associated with your objects. Compilation errors in your packages may cause your portlets to render incorrectly.

User/Role <schema> does not exist. Applications based on <schema> will have errors.

Cause: A database provider (formerly called application) schema is missing. For example:

```
WARNING User/Role SCOTTB does not exist. Application based on SCOTTB will have
errors.
```

In this case, the database provider would not have been accessible before the upgrade either.

Action: Determine if the database provider is obsolete. If it is, delete it. If not, supply the missing schema.

VPD precheck found some issues.

Cause: One of the VPD checks has failed.

Action: This warning is followed by a detailed message. Resolve the issue by examining the information provided in the message.

F
Common Issues and Workarounds

The following sections describe some common issues you might experience while upgrading to Oracle Identity Management 10*g* (10.1.4.0.1):

- OracleAS Identity Management Upgrade Problems and Solutions
- OracleAS Metadata Repository Upgrade Issues and Workarounds

F.1 OracleAS Identity Management Upgrade Problems and Solutions

The following sections provide common problems and solutions when upgrading an Oracle Application Server Infrastructure:

- Insufficient Privileges Error When Upgrading Identity Management on UNIX Systems
- Problems Encountered When Running the Oracle Internet Directory Upgrade Assistant From Oracle Universal Installer
- Problem Stopping Processes in Source Oracle Home During OracleAS Identity Management Upgrade
- Database Listener Errors When Running Configuration Assistants During OracleAS Identity Management Upgrade
- Oracle Directory Integration Platform Configuration Assistant Fails with Time Synchronization Error

F.1.1 Insufficient Privileges Error When Upgrading Identity Management on UNIX Systems

Problem

When you attempt to upgrade OracleAS Identity Management on a UNIX system, the upgrade fails. An "insufficient privileges" error appears in the following log file:

```
904_SOURCE_ORACLE_HOME/assistants/dbma/logs/trace.log
```

Specifically, the error appears as follows:

```
oracle.sysman.assistants.util.sqlEngine.SQLFatalErrorException: ORA-01031:
insufficient privileges
```

Solution

Before you start Oracle Universal Installer to begin the installation procedure, be sure to log in as a user that is a member of the DBA group for the database.

F.1.2 Problems Encountered When Running the Oracle Internet Directory Upgrade Assistant From Oracle Universal Installer

The Oracle Internet Directory upgrade assistant is one of the assistants that run near the end of the 10*g* (10.1.4.0.1) installation procedure when you are upgrading an OracleAS Identity Management installation.

You can get information about the cause of Oracle Internet Directory upgrade assistant errors by looking at the following log file:

```
ORACLE_HOME/ldap/log/oidca.log
```

Problem 1

The upgrade assistant log file (`oidca.log`) reports the following:

```
OID processes are currently running
```

This is a result of some Oracle Internet Directory or Oracle Directory Integration Platform processes not being shut down properly in the source Oracle Home.

Solution

Without exiting the Installer, open another terminal window and shut down all the processes in the source Oracle Home. Then, retry the Oracle Internet Directory upgrade assistant from the Oracle Universal Installer configuration assistants page.

Without exiting the Installer, shut down all the processes in the source Oracle Home and then retry the Oracle Internet Directory configuration assistant from the Oracle Universal Installer configuration assistants page.

> **See Also:** The corresponding version of the Oracle Internet Directory documentation to stop the Oracle Internet Directory and Oracle Directory Integration and Provisioning processes in the source Oracle Home.

If you are upgrading from 10*g* (9.0.4), you can ensure that the proper processes are shut down by using the Oracle Process Manager and Notification Server (OPMN) command utility to start and then stop all processes in the Oracle home.

For example, use the following procedure to start all the processes and then shut down all the processes. Note carefully whether or not any errors appear when you are starting or shutting down the processes:

1. Start all the processes in the OracleAS Identity Management 10*g* (9.0.4) source Oracle home using the following command:

   ```
   SOURCE_ORACLE_HOME/opmn/bin/opmnctl startall
   ```

2. Make sure that no errors occurred during startup and make sure that the Oracle Internet Directory server is up and running.

   To verify that Oracle Internet Directory is running, enter one of the following commands.

   If you are running Oracle Internet Directory on a non-secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p Non-SSL_port
   ```

   If you are running Oracle Internet Directory on a secure port:

   ```
   SOURCE_ORACLE_HOME/bin/ldapbind -p SSL_port -U 1
   ```

These commands should return a "bind successful" message.

> **See Also:** "Syntax for LDIF and Command-Line Tools" in the *Oracle Internet Directory Administrator's Guide* for more information about the `ldapbind` utility

3. Enter the following command to stop all the processes:

   ```
   SOURCE_ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

4. Use the `ldapbind` command again to verify that Oracle Universal Installer is down and not running.
5. Rerun the Oracle Internet Directory upgrade assistant.

Problem 2

The Oracle Internet Directory upgrade fails with "table or view does not exist" error.

Solution

This problem occurs when the Oracle Internet Directory upgrade assistant is run against a 9.2.0.x OracleAS Metadata Repository containing a 9.2.0.x Oracle Internet Directory.

The solution is to do the following:

1. Create table `imcfgregistry` in the 9.2.0.x Oracle Internet Directory database repository by running the following SQL statement as ODS schema:

   ```
   CREATE TABLE imcfgregistry (Component  VARCHAR2(255),
      instMode VARCHAR2(255),
      IASInstance VARCHAR2(255))
      TABLESPACE OLTS_DEFAULT MONITORING;
   ```

2. Retry the Oracle Internet Directory upgrade assistant from the Oracle Universal Installer configuration assistants screen.

Problem 3

The Oracle Internet Directory configuration assistant fails during the Configuration Assistants phase of the OracleAS Identity Management upgrade with Oracle Universal Installer.

Solution

Check the contents of the following configuration file in the destination Oracle home and verify that the file contains the correct `SERVICE_NAME` entry for your Metadata Repository. If the value assigned to this entry is incorrect, enter the correct name, save the file, and retry the assistant.

```
DESTINATION_ORACLE_HOME/network/admin/tnsnames.ora
```

F.1.3 Problem Stopping Processes in Source Oracle Home During OracleAS Identity Management Upgrade

Problem

When you run the Oracle Universal Installer to upgrade OracleAS Identity Management, a popup dialog notifies you that the installer will shut down some processes in the source Oracle home.

After the installer performs the shutdown, it checks that Oracle Internet Directory is stopped. If Oracle Internet Directory is not stopped for some reason, installer will display another popup dialog notifying you of the problem.

Solution

Examine the following log file to determine the cause of the problem:

```
DESTINATION_ORACLE_HOME/cfgtoollogs/shutdownprocesses.log
```

Resolve the problem and then manually stop Oracle Internet Directory in the source Oracle home. Once Oracle Internet Directory is stopped, continue with the OracleAS Identity Management upgrade by clicking **Continue** in Oracle Universal Installer.

> **See Also:** Chapter "Oracle Internet Directory Process Control–Best Practices" in the *Oracle Internet Directory Administrator's Guide* for information about stopping and starting Oracle Internet Directory

F.1.4 Database Listener Errors When Running Configuration Assistants During OracleAS Identity Management Upgrade

Problem

Oracle Universal Installer invokes configuration assistants at the end of the OracleAS Identity Management upgrade. Some of the configuration assistants require an Oracle Database 10*g* database listener to connect to the database. If an Oracle Database 10*g* database listener is not available, those configuration assistants fail.

Often, when this problem occurs, one of the following errors (or a similar error) appears in the installation log files:

```
java.lang.Exception: Error: Database Listener is down. Please start listener
and make sure database is up before running this script.
```

OR

```
java.sql.SQLException: Listener refused the connection with the following
error:
ORA-12500, TNS:listener failed to start a dedicated server process
```

Solution

The installer normally starts an Oracle Database 10*g* database listener in the destination Oracle home. However, if an Oracle9*i* Database listener is already running, then the installer fails to start the Oracle Database 10*g* (10.1.0.2) database listener.

The most common cause of this problem is that you missed the instruction in a pop-up dialog during the installation. This pop-up message indicates during the interview phase of the installation that there is a running database listener running and that you should stop the listener manually before proceeding.

To correct the problem, stop the existing Oracle9*i* (9.0.1.3) listener, and then start the database listener in the destination Oracle home, as follows:

1. Set the `ORACLE_HOME` environment variable to point to the destination Oracle home of upgrade.
2. Change directory to `bin` directory of the destination Oracle home.
3. Run the `lsnrctl start` command to start the listener.

After the Oracle Database 10*g* database listener is running, continue with the OracleAS Identity Management upgrade by clicking **Retry** on the Configuration Assistants page in Oracle Universal Installer.

F.1.5 Oracle Directory Integration Platform Configuration Assistant Fails with Time Synchronization Error

Problem

While upgrading a 10*g* (9.0.4) distributed OracleAS Identity Management environment, the Oracle Directory Integration Platform configuration assistant fails.

When you check the following log file, you notice an error message indicating that there is time difference of at least 250 seconds between two of the OracleAS Identity Management hosts:

```
DESTINATION_ORACLE_HOME/ldap/log/oidmon.log
```

Specifically, the error message says:

```
Time Difference of at least 250 sec found between DIP_hostname and OID_hostname.
Please sync the time between DIP-hostname and OID-hostname
```

Solution

Synchronize the system clocks on all nodes where the OracleAS Identity Management components reside so they are running within 250 seconds of each other.

When synchronizing the system clocks, make sure the clocks are set to the same time zone.

After you synchronize the clocks, rerun the Oracle Directory Integration Platform configuration assistant.

F.1.6 Errors While Running OracleAS Portal Patch Configuration Assistant During OracleAS Identity Management Upgrade

Problem

During an OracleAS Identity Management upgrade, the OracleAS Portal Patch Configuration Assistant fails. Errors in the log files show the following errors:

```
ERROR: Portal patch for invalid objects in the  CTXSYS schema failed.
ERROR: Portal patch for Oracle 10g database upgrade throws exception
java.sql.SQLException: ORA-12154: TNS:could not resolve the connect identifier
specified
java.sql.SQLException: ORA-12154: TNS:could not resolve the connect identifier
specified
```

Solution

Make sure that the TWO_TASK environment variable is not set and then try running the configuration assistant again. For example:

Example (C shell):

```
% unsetenv TWO_TASK
```

Example (Bourne or Korn shell):

```
$ unset TWO_TASK
```

F.2 OracleAS Metadata Repository Upgrade Issues and Workarounds

The following sections describe common problems and solutions when upgrading your OracleAS Metadata Repository and the database that hosts the OracleAS Metadata Repository:

- Deciding When to Upgrade an Infrastructure Database
- Verifying the Progress of the Database Upgrade Assistant During OracleAS Identity Management Upgrade
- Performance Issues When Using the Metadata Repository Upgrade Assistant (MRUA) to Upgrade the OracleAS Portal Schema
- Database Upgrade Assistant Failure During OracleAS Identity Management Upgrade
- Problem Upgrading OracleAS Portal Schemas with MRUA
- Error About "DIP" User in Database Upgrade Log Files

F.2.1 Deciding When to Upgrade an Infrastructure Database

Problem

When a newer version of Oracle Database is announced, should I upgrade the OracleAS Metadata Repository database to the new database version?

Solution

In general, use caution when upgrading your Infrastructure database to a new database version. Check Oracle *Metalink* (`http://metalink.oracle.com`) for posted articles or announcements that confirm that the database version and upgrade has been tested and is supported for an existing OracleAS Metadata Repository database.

> **See Also:** Chapter 6, "Upgrading the Database That Hosts the OracleAS Metadata Repository" for information about supported upgrade paths for the 10*g* Release 2 (10.1.2) Metadata Repository database

F.2.2 Verifying the Progress of the Database Upgrade Assistant During OracleAS Identity Management Upgrade

Problem

Oracle Universal Installer invokes Database Upgrade Assistant at the end of OracleAS Identity Management Upgrade. Database Upgrade Assistant may take a long time depending on the size and contents of the database. The installer shows progress of the Database Upgrade Assistant by displaying percentage numbers, but no details about the progress are shown on the Configuration Assistants screen in Oracle Universal Installer.

Solution

If you would like to obtain more detailed information about the progress of the Database Upgrade Assistant, examine the log files generated by the Database Upgrade Assistant. The log files reside in:

```
DESTINATION_ORACLE_HOME/admin/SID/upgrade/
```

In this example, replace *SID* with the system identifier of the database in the source Oracle home.

To obtain the timestamps of the different stages of the database upgrade, search for the string "COMP_TIME" in the log files. For example,

```
find "COMP_TIME" *.log

grep ^COMP_TIME *.log
```

The output of the command identifies each stage of the database upgrade, as well as a timestamp for each stage. For example:

```
Oracle_Server.log:COMP_TIMESTAMP DBUPG__BGN 2004-12-16 10:11:00 2453356 36660
Oracle_Server.log:COMP_TIMESTAMP UTLIP__END 2004-12-16 10:12:58 2453356 36778
Oracle_Server.log:COMP_TIMESTAMP CATALG_BGN 2004-12-16 10:27:44 2453356 37664
Oracle_Server.log:COMP_TIMESTAMP CATPROC    2004-12-16 11:18:45
Oracle_Server.log:COMP_TIMESTAMP RDBMS      2004-12-16 11:21:50
Oracle_Server.log:COMP_TIMESTAMP JAVAVM     2004-12-16 12:27:24
Oracle_Server.log:COMP_TIMESTAMP XML        2004-12-16 12:41:17
Oracle_Server.log:COMP_TIMESTAMP CATJAVA    2004-12-16 12:45:03
Oracle_Server.log:COMP_TIMESTAMP CONTEXT    2004-12-16 12:49:17
Oracle_Server.log:COMP_TIMESTAMP XDB        2004-12-16 12:56:32
Oracle_Server.log:COMP_TIMESTAMP OWM        2004-12-16 13:01:14
Oracle_Server.log:COMP_TIMESTAMP AMD        2004-12-16 13:11:04
Oracle_Server.log:COMP_TIMESTAMP ORDIM      2004-12-16 13:43:34
Oracle_Server.log:COMP_TIMESTAMP SDO        2004-12-16 13:52:30
Oracle_Server.log:COMP_TIMESTAMP WK         2004-12-16 13:56:24
Oracle_Server.log:COMP_TIMESTAMP DBUPG_END  2004-12-16 14:10:39
PostUpgrade.log:COMP_TIMESTAMP UTLRP_BGN  2004-12-16 14:12:32
PostUpgrade.log:COMP_TIMESTAMP UTLRP_END  2004-12-16 15:29:47
```

F.2.3 Performance Issues When Using the Metadata Repository Upgrade Assistant (MRUA) to Upgrade the OracleAS Portal Schema

Problem 1

The first time you run MRUA, the OracleAS Portal component (or plug-in) appears to hang or stop working while upgrading the OracleAS Portal schema.

Problem 2

If you run MRUA after the OracleAS Portal schema has already been upgraded, the OracleAS Portal MRUA plug-in, unlike other component MRUA plug-ins, does not immediately report the fact that OracleAS Portal has already been upgraded.

Solution

In most cases, no solution is necessary. Simply wait until the OracleAS Portal component of MRUA finishes processing.

The OracleAS Portal component of MRUA performs an extensive sequence of pre-checks that can take several minutes to finish.

In addition, the OracleAS Portal component of MRUA executes for a much longer period of time than any of the other plug-ins. As a result, it can take up to 40 minutes to run.

If Portal plug-in appears to be hanging, review the log files in the following directory to determine whether or not portal upgrade is progressing:

```
MRUA_HOME/temp/portal
```

Do not abort MRUA during the OracleAS Portal schema upgrade without first verifying that Portal upgrade has actually stopped processing.

F.2.4 Database Upgrade Assistant Failure During OracleAS Identity Management Upgrade

Oracle Universal Installer invokes Database Upgrade Assistant at the end of OracleAS Identity Management Upgrade. If the Database Upgrade Assistant fails, you can examine the log files generated by the Database Upgrade Assistant. The log files reside in:

```
DESTINATION_ORACLE_HOME/admin/SID/upgrade/
```

In this example, replace *SID* with the system identifier of the database in the source Oracle home.

Examine the log files and determine the cause of the failure. In most cases, it is not possible to retry the Database Upgrade Assistant. Instead, you will need to restore the source Oracle home and the database files to their state before the OracleAS Identity Management Upgrade. After the restoration, make sure that the problems which caused the Database Upgrade Assistant to fail are resolved. Then run OracleAS Identity Management Upgrade again.

F.2.5 Problem Upgrading OracleAS Portal Schemas with MRUA

Problem

When running MRUA, the OracleAS Portal upgrade fails and results in invalid versions.

The following error appears in the log files:

```
EXP-00056: ORACLE error 942 encountered
ORA-00942: table or view does not exist
EXP-00000: Export terminated unsuccessfully
Ending export at Mon May 30 02:59:21 2005
```

Solution

This error can be caused by providing an incorrect value for the `-oracle_home` argument on the MRUA command line. When running MRUA be sure to enter the Oracle home of the OracleAS Metadata Repository. This is especially important when upgrading a non-colocated Infrastructure where the OracleAS Metadata Repository is in its own Oracle home.

> **See Also:** Chapter 8, "Using MRUA to Upgrade the OracleAS Metadata Repository" for more information about the MRUA command-line arguments

F.2.6 Error About "DIP" User in Database Upgrade Log Files

Problem

After you upgrade your OracleAS Metadata Repository database as part of an upgrade to Oracle Identity Management 10*g* (10.1.4.0.1), you might see error messages in the following database upgrade log file:

```
DESTINATION_ORACLE_HOME/dbma/logs/silent.log
```

Specifically, you might see the following error about the "DIP" database user:

```
The username "'DIP'" conflicts with a required user of the same name in
Oracle Database 10g. To resolve the conflict, click No, drop the user and
create it with a different name, and then continue with the upgrade.
```

This error can be ignored.

F.2.7 MRUA Error While Upgrading the Portal Schema

Problem

The following error appears while running the Metadata Repository Upgrade Assistant:

```
Calling upgrade plugin for PORTAL
 Error: Component upgrade failed PORTAL
 Error: PORTAL component version is: 9.0.4.2.0 INVALID
```

When you check the precheck.log file, you find the following entry:

```
### ERROR: WWU-00030: Pre-Check mode encountered the following errors
###       203 : ### ERROR:  WWU-00021: The following mandatory object(s)
are missing or invalid:
###         '[SYNONYM]PUBLIC.XMLPARSER' \
###         '[SYNONYM]PUBLIC.XMLDOM' \
```

Solution

Manually create the XDB and XMLDOM tablespaces by running the following command in the OracleAS Metadata Repository Oracle home:

```
DESTINATION_ORACLE_HOME/rdbms/admin/catqm.sql xdb_pwd XDB_Tablespace_NAME TEMP_
Tablespace_NAME
```

For example:

```
DESTINATION_ORACLE_HOME/rdbms/admin/catqm.sql my_secure_pwd_231 XDB TEMP
```

> **See Also:** "Installing a New Oracle XML DB Manually Without DBCA" in Appendix A, "Installing and Configuring Oracle XML DB" of the *Oracle9i Database Server*.

Index