Oracle® Application Server 10*g*

Administrator's Guide

10*g* (9.0.4)

Part No. B10376-01

November 2003

ORACLE®

Oracle Application Server 10*g* Administrator's Guide, 10*g* (9.0.4)

Part No. B10376-01

Primary Author: Mary Beth Roeser

Contributing Authors: Priya Darshane, Pavana Jain, Lypp-Tek Khoo-Ellis, Peter LaQuerre, Theresa Robertson, Andrew Salt, Pavi Sandhu, Thomas Van Raalte

Contents

5 Managing Ports

8 Changing Infrastructure Services

9 Changing Network Configurations

10 Management Considerations for Recommended Topologies

Part IV Backup and Recovery

11 Introduction to Backup and Recovery

12 Oracle Application Server Backup and Recovery Tool

13 Backup Strategy and Procedures

B Oracle Application Server Command-Line Tools

C Oracle Application Server Port Numbers

D Metadata Repository Schemas

E printlogs Tool Syntax and Usage

Send Us Your Comments

Oracle Application Server 10*g* Administrator's Guide, 10*g* (9.0.4)

Part No. B10376-01

Oracle Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the document, and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: appserverdocs_us@oracle.com
- FAX: 650-506-7375 Attn: Oracle Application Server Documentation Manager
- Postal service:
  Oracle Corporation
  Oracle Application Server Documentation
  500 Oracle Parkway, M/S 1op6
  Redwood Shores, CA 94065
  USA

If you would like a reply, please give your name, address, telephone number, and (optionally) electronic mail address.

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This guide describes how to manage Oracle Application Server.

This preface contains these topics:

Audience

The *Oracle Application Server 10g Administrator's Guide* is intended for administrators of Oracle Application Server.

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. Standards will continue to evolve over time, and Oracle Corporation 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 additional information, visit the Oracle Accessibility Program Web site at:

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

Accessibility of Code Examples in Documentation

JAWS, a Windows screen reader, 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, JAWS 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 Corporation neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Organization

This document contains:

Part I, "Getting Started"

This part contains chapters that describe how to get started with managing Oracle Application Server.

Chapter 1, "Getting Started After Installing Oracle Application Server"

This chapter provides tasks for getting familiar with your Oracle Application Server installation.

Chapter 2, "Introduction to Administration Tools"

This chapter introduces Web-based and command-line administration tools for Oracle Application Server.

Chapter 3, "Starting and Stopping"

This chapter describes how to start and stop Oracle Application Server environments, instances, components, and clusters.

Part II, "Basic Administration"

This part contains chapters that describe basic administration tasks.

Chapter 4, "Managing Log Files"

This chapter describes how to view and manage Oracle Application Server log files.

Chapter 5, "Managing Ports"

This chapter describes how to view and change Oracle Application Server port numbers.

Chapter 6, "Managing an OracleAS Metadata Repository"

This chapter describes tasks for managing OracleAS Metadata Repositories, such as changing schema passwords, relocating datafiles, and changing the character set.

Part III, "Advanced Administration"

This part contains chapters that describe advanced administration tasks.

Chapter 7, "Reconfiguring Application Server Instances"

This chapter describes how to extend application server instances, configure additional components, and configure a J2EE and Web Cache instance to use Infrastructure Services.

Chapter 8, "Changing Infrastructure Services"

This chapter describes how to change the Infrastructure Services used by a middle-tier instance.

Chapter 9, "Changing Network Configurations"

This chapter describes how to change the hostname and IP address of an Oracle Application Server host.

Chapter 10, "Management Considerations for Recommended Topologies"

This chapter provides key considerations for managing Oracle Application Server recommended topologies.

Part IV, "Backup and Recovery"

This part contains chapters that describe how to back up and recover your Oracle Application Server environment.

Chapter 11, "Introduction to Backup and Recovery"

This chapter provides an overview of Oracle Application Server backup and recovery tools, strategies, and procedures.

Chapter 12, "Oracle Application Server Backup and Recovery Tool"

This chapter describes how to install, configure, and use the Oracle Application Server Backup and Recovery Tool.

Chapter 13, "Backup Strategy and Procedures"

This chapter describes Oracle Application Server backup strategies and procedures.

Chapter 14, "Recovery Strategies and Procedures"

This chapter describes Oracle Application Server recovery strategies and procedures.

Part V, "Appendixes"

This part contains various appendixes.

Appendix A, "Managing and Configuring Application Server Control"

This appendix provides tasks for managing and configuring Application Server Control, including starting and stopping, configuring security, enabling ODL log formatting, and enabling Enterprise Manager accessibility mode.

Appendix B, "Oracle Application Server Command-Line Tools"

This appendix provides descriptions and locations of Oracle Application Server command-line administration tools.

Appendix C, "Oracle Application Server Port Numbers"

This appendix lists Oracle Application Server default port numbers and provides information on assigning and changing them.

Appendix D, "Metadata Repository Schemas"

This appendix provides descriptions of OracleAS Metadata Repository schemas, and lists their tablespaces and datafiles.

Appendix E, "printlogs Tool Syntax and Usage"

This appendix describes how to use the `printlogs` utility for viewing log files.

Appendix F, "Auxiliary Procedures for Changing Infrastructure Services"

This appendix contains procedures changing Infrastructure Services, such as installing and setting up an LDAP-based replica, and migrating data.

Appendix G, "Examples of Administrative Changes"

This appendix provides examples of administrative changes to Oracle Application Server, which can be used for guidance when performing backup and recovery, managing OracleAS Disaster Recovery, and managing OracleAS Active Failover Cluster.

Appendix H, "Viewing Oracle Application Server Release Numbers"

This appendix describes how to view Oracle Application Server release numbers.

Related Documentation

For more information, see these Oracle resources:

- Oracle Application Server Documentation Library
- Oracle Application Server Platform-Specific Documentation on Oracle Application Server Disk 1

Printed documentation is available for sale in the Oracle Store at

`http://oraclestore.oracle.com/`

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

`http://otn.oracle.com/membership/`

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

`http://otn.oracle.com/documentation/`

Conventions

This section describes the conventions used in the text and code examples of this documentation set. It describes:

- Conventions in Text
- Conventions in Code Examples
- Conventions for Windows Operating Systems

Conventions in Text

We use various conventions in text to help you more quickly identify special terms. The following table describes those conventions and provides examples of their use.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an **index-organized table**.
Italics	Italic typeface indicates book titles or emphasis.	*Oracle Application Server 10g Concepts* Ensure that the recovery catalog and target database do *not* reside on the same disk.
`UPPERCASE monospace (fixed-width) font`	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a `NUMBER` column. You can back up the database by using the `BACKUP` command. Query the `TABLE_NAME` column in the `USER_TABLES` data dictionary view. Use the `DBMS_STATS.GENERATE_STATS` procedure.

Convention	Meaning	Example
`lowercase monospace (fixed-width) font`	Lowercase monospace typeface indicates executables, filenames, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, usernames and roles, program units, and parameter values. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter `sqlplus` to open SQL*Plus. The password is specified in the `orapwd` file. Back up the datafiles and control files in the `/disk1/oracle/dbs` directory. The `department_id`, `department_name`, and `location_id` columns are in the `hr.departments` table. Set the `QUERY_REWRITE_ENABLED` initialization parameter to `true`. Connect as `oe` user. The `JRepUtil` class implements these methods.
`lowercase italic monospace (fixed-width) font`	Lowercase italic monospace font represents placeholders or variables.	You can specify the *`parallel_clause`*. Run `U`*`old_release`*`.SQL` where *`old_release`* refers to the release you installed prior to upgrading.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
`[ ]`	Brackets enclose one or more optional items. Do not enter the brackets.	`DECIMAL (`*`digits`*` [ , `*`precision`*` ])`
`{ }`	Braces enclose two or more items, one of which is required. Do not enter the braces.	`{ENABLE | DISABLE}`
`|`	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	`{ENABLE | DISABLE}` `[COMPRESS | NOCOMPRESS]`

Convention	Meaning	Example

...	Horizontal ellipsis points indicate either:
	■ That we have omitted parts of the code that are not directly related to the example
	■ That you can repeat a portion of the code
		`CREATE TABLE ... AS subquery;`
		
		`SELECT col1, col2, ... , coln FROM employees;`

.
.
.
	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	`SQL> SELECT NAME FROM V$DATAFILE;`
		`NAME`
		`----------`
		`/fsl/dbs/tbs_01.dbf`
		`/fs1/dbs/tbs_02.dbf`
		`.`
		`.`
		`.`
		`/fsl/dbs/tbs_09.dbf`
		`9 rows selected.`

Other notation	You must enter symbols other than brackets, braces, vertical bars, and ellipsis points as shown.	`acctbal NUMBER(11,2);` `acct CONSTANT NUMBER(4) := 3;`
Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	`CONNECT SYSTEM/system_password` `DB_NAME = database_name`

UPPERCASE	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

lowercase	Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files.
	
	Note: Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.
		`SELECT last_name, employee_id FROM employees;`
		`sqlplus hr/hr`
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

Conventions for Windows Operating Systems

The following table describes conventions for Windows operating systems and provides examples of their use.

Convention	Meaning	Example
Choose Start >	How to start a program.	To start the Database Configuration Assistant, choose Start > Programs > Oracle - *HOME_NAME* > Configuration and Migration Tools > Database Configuration Assistant.
File and directory names	File and directory names are not case sensitive. The following special characters are not allowed: left angle bracket (<), right angle bracket (>), colon (:), double quotation marks ("), slash (/), pipe (|), and dash (-). The special character backslash (\) is treated as an element separator, even when it appears in quotes. If the file name begins with \ \, then Windows assumes it uses the Universal Naming Convention.	`c:\winnt"\"system32 is the same as C:\WINNT\SYSTEM32`
`C:\>`	Represents the Windows command prompt of the current hard disk drive. The escape character in a command prompt is the caret (^). Your prompt reflects the subdirectory in which you are working. Referred to as the *command prompt* in this manual.	`C:\oracle\oradata>`
Special characters	The backslash (\) special character is sometimes required as an escape character for the double quotation mark (") special character at the Windows command prompt. Parentheses and the single quotation mark (') do not require an escape character. Refer to your Windows operating system documentation for more information on escape and special characters.	`C:\>exp scott/tiger TABLES=emp QUERY=\"WHERE job='SALESMAN' and sal<1600\"` `C:\>imp SYSTEM/`*`password`*` FROMUSER=scott TABLES=(emp, dept)`
HOME_NAME	Represents the Oracle home name. The home name can be up to 16 alphanumeric characters. The only special character allowed in the home name is the underscore.	`C:\> net start Oracle`*`HOME_NAME`*`TNSListener`

Convention	Meaning	Example
ORACLE_HOME and *ORACLE_BASE*	In releases prior to Oracle8*i* release 8.1.3, when you installed Oracle components, all subdirectories were located under a top level *ORACLE_HOME* directory. For Windows NT, the default location was `C:\orant`. This release complies with Optimal Flexible Architecture (OFA) guidelines. All subdirectories are not under a top level *ORACLE_HOME* directory. There is a top level directory called *ORACLE_BASE* that by default is `C:\oracle`. If you install the latest Oracle release on a computer with no other Oracle software installed, then the default setting for the first Oracle home directory is `C:\oracle\ora`*nn*, where *nn* is the latest release number. The Oracle home directory is located directly under *ORACLE_BASE*. All directory path examples in this guide follow OFA conventions. Refer to *Oracle9i Database Getting Starting for Windows* for additional information about OFA compliances and for information about installing Oracle products in non-OFA compliant directories.	Go to the *ORACLE_BASE*`\`*ORACLE_HOME*`\rdbms\admin` directory.

What's New in Oracle Application Server Administration?

This preface introduces the new administrative features of Oracle Application Server 10*g* (9.0.4). This information is mostly useful to users who have managed Oracle9*i* Application Server (Oracle9*i*AS) Release 2 (9.0.2 and 9.0.3).

The new administrative features of Oracle Application Server 10*g* (9.0.4) include:

- Oracle Identity Management
- Improvements to Oracle Application Server Metadata Repository
- More Flexibility in the Infrastructure Installation Type
- New Features in Oracle Enterprise Manager Application Server Control
- Expanded Role of Oracle Process Manager and Notification Server (OPMN)
- New Features in Distributed Configuration Management (DCM)
- Some SSL Ports Are Not Enabled During Installation
- Simplified Starting and Stopping
- New Tools for Viewing Log Files
- Improved Port Management
- Changing Infrastructure Services Used by a Middle-Tier Instance
- New Tool for Changing the Hostname or IP Address
- New Backup and Recovery Procedures and Tool
- New High Availability Solutions

Oracle Identity Management

Identity management is the process by which various components work together to manage the security life cycle for networked entities, such as devices, processes, applications, and users. While some of this functionality existed in Oracle9*i*AS Release 2, it has been enhanced and fully integrated into a new product in Oracle Application Server 10*g* called Oracle Identity Management.

> **See Also:** *Oracle Identity Management Concepts and Deployment Planning Guide*

Oracle Identity Management provides a fine-grained delegation deployment privileges model for deploying middle tiers and Metadata Repositories. You can find information on this in several books, as shown in the following table.

Topic	See Also
Delegation of Privileges for Oracle Technology deployment—describes the delegation model and its implementation in Oracle Internet Directory	*Oracle Internet Directory Administrator's Guide*
Component Deployment Roles in Oracle Internet Directory—describes the various deployment roles and privileges required to install specific components	*Oracle Application Server 10g Installation Guide*
Common Security Considerations for Oracle Application Server administrators—describes the delegation model for component deployments	*Oracle Application Server 10g Security Guide*

Oracle Identity Management is part of the Infrastructure installation type, and contains the following components:

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

Improvements to Oracle Application Server Metadata Repository

Oracle Application Server 10*g* provides the following improvements to the Oracle Application Server Metadata Repository:

- Some schemas have been added or deleted in the OracleAS Metadata Repository.

  See Also: Appendix D, "Metadata Repository Schemas"

- In Oracle Application Server 10*g*, you can specify the following OracleAS Metadata Repository attributes during installation:
  - Service ID (SID)—the default is `asdb`
  - Global database name—the default is `asdb.`*`domainname`*
  - Location of datafiles—the default is *`ORACLE_HOME`*`/oradata`
  - Database character set
  - Password for the `SYS` user
  - Password for the `SYSTEM` user
- In Oracle9*i*AS Release 2, it was a requirement for the Oracle9*i*AS Metadata Repository to be registered with Oracle Internet Directory. In Oracle Application Server 10*g*, you can:
  - Register the OracleAS Metadata Repository with Oracle Internet Directory. This is required in order for Portal and Wireless or Business Intelligence and Forms installations to use the Metadata Repository. It is optional for J2EE and Web Cache (see next bullet).
  - Use a standalone OracleAS Metadata Repository, not registered with Oracle Internet Directory. This is handy if you have a J2EE and Web Cache installation and would like to use a Metadata Repository for the DCM repository and Oracle Application Server Managed Clusters, but do not require the single sign-on services offered by Oracle Internet Directory and Oracle Identity Management.

    See Also: *Oracle Application Server 10g Installation Guide*

- In Oracle9*i*AS Release 2, the only way to obtain an Oracle9*i*AS Metadata Repository was by installing it as part of an Infrastructure installation with Oracle Universal Installer. In Oracle Application Server 10*g*, you can obtain an OracleAS Metadata Repository in two ways:

- You can install an OracleAS Metadata Repository as part of an Infrastructure installation with Oracle Universal Installer
- You can install the OracleAS Metadata Repository into an existing Oracle9*i* database using the Oracle Application Server Repository Creation Assistant (OracleAS RepCA)

Note that both of the above methods support installing a Metadata Repository that is registered or not-registered with Oracle Internet Directory.

See Also: *Oracle Application Server 10g Installation Guide*

More Flexibility in the Infrastructure Installation Type

The Infrastructure installation type is divided into two distinct pieces:

- Oracle Identity Management
- OracleAS Metadata Repository

Oracle Application Server 10*g* provides greater flexibility for installing an Infrastructure:

- You can install Oracle Identity Management and the OracleAS Metadata Repository together in the same Oracle home. (This option was available in Oracle9*i*AS Release 2.)
- You can install only Oracle Identity Management and have it use an existing OracleAS Metadata Repository in a different Oracle home or on a different host. (This option is new in Oracle Application Server 10*g*.)
- You can install only a OracleAS Metadata Repository and register it with the Oracle Internet Directory in an Oracle Identity Management installation in a different Oracle home or on a different host. (This option was available in Oracle9*i*AS Release 2.)
- You can install only a OracleAS Metadata Repository and not register it with the Oracle Internet Directory in an Oracle Identity Management installation. (This option is new in Oracle Application Server 10*g*.)

Because the Infrastructure is divided into these two pieces that provide different services, it is often too imprecise to refer to the Infrastructure as a whole when discussing administrative operations. For example, a middle-tier instance may use Oracle Identity Management in one Infrastructure installation, and the OracleAS Metadata Repository in another Infrastructure installation. In this case, it is not accurate to refer to the "Infrastructure" used by a middle-tier instance. You will notice that Oracle Application Server 10*g* tools and documentation often refer

specifically to the Oracle Identity Management installation or OracleAS Metadata Repository used by a middle-tier instance.

New Features in Oracle Enterprise Manager Application Server Control

The Oracle9*i*AS Oracle Enterprise Manager Web site has been renamed to Oracle Enterprise Manager 10*g* Application Server Control (Application Server Control, for short).

Application Server Control is installed and configured in every Oracle Application Server installation. Each installation has its own `ias_admin` password and uses a different port for Application Server Control. There is no primary Oracle home and no `emtab` file.

Application Server Control includes the following enhancements:

- Ports Page—summarizes the port numbers used by your installation and contains links for changing port numbers

  See Also: Chapter 5, "Managing Ports"

- Log Viewer—allows you to view Oracle Application Server log files in one place and trace problems across multiple log files

  See Also: Chapter 4, "Managing Log Files"

- J2EE Applications Page—summarizes the J2EE applications deployed in an Oracle Application Server instance
- Process Management Page—allows you to configure `opmn.xml`
- Application Server Instance Status—the status of an application server instance is "up" if all components are up and "down" if at least one component is down; there is no partial up or down status
- Enable / Disable components—prevents or allows specified components to be started with your application server instance and displayed in Application Server Control

  See Also: Chapter 3, "Starting and Stopping"

- Infrastructure Page—allows you to change the Identity Management services or OracleAS Metadata Repository used by a middle-tier instance, and change OracleAS Metadata Repository schema passwords

See Also: Chapter 8, "Changing Infrastructure Services" and Chapter 6, "Managing an OracleAS Metadata Repository"

- Performance enhancements
- The `emctl` command has new syntax

See Also: Chapter 2, "Introduction to Administration Tools"

Expanded Role of Oracle Process Manager and Notification Server (OPMN)

OPMN has expanded to provide process management and monitoring for most Oracle Application Server components, and `opmnctl` is the primary command-line tool for starting and stopping.

- In Oracle9*i*AS Release 2, you used several different command-line tools to start an application server instance. In Oracle Application Server 10*g*, you use a single `opmnctl` command to start all of the components in an application server instance in the proper order.

See Also: Chapter 3, "Starting and Stopping"

- The scope of the `opmnctl` command has expanded—you can start a specified instance in the farm, all instances in the farm, and Oracle Application Server clusters.
- The `opmn.xml` file has changed to provide more power and flexibility for configuring Oracle Application Server. You can edit the `opmn.xml` file manually or using the Process Management page in Application Server Control.
- OPMN provides many other new features, including event scripts, improved monitoring, and operating system-level statistics.

See Also: *Oracle Process Manager and Notification Server Administrator's Guide*

New Features in Distributed Configuration Management (DCM)

In Oracle Application Server 10*g*, DCM and the `dcmctl` command provide many new features, including:

- DCM provides a new archiving feature. You can create an archive of the configuration of an Oracle Application Server instance or cluster, then apply the archived configuration to the same instance or cluster, or to a different instance

or cluster. DCM archiving contains all of the functionality of the deprecated `saveInstance` and `restoreInstance` commands, plus much more.

- DCM provides expanded support for managing the DCM repository when it is stored in the filesystem (file-based repository) and the DCM repository when it is stored in the OracleAS Metadata Repository (database repository).
- DCM provides support for managing OracleAS Clusters
- The `dcmctl` command and Application Server Control can be used together. There is no need to disable one while you are using the other, as in Oracle9*i*AS Release 2.
- By default, the `-v` and `-d` options are enabled for every `dcmctl` command. This provides useful error messages and diagnostic output. Oracle recommends you always use the `-v` and `-d` options, however, you can enable and disable them using the `dcmctl set` command.

See Also: *Distributed Configuration Management Reference Guide*

Some SSL Ports Are Not Enabled During Installation

For security purposes, the following SSL ports are not enabled during installation—you can selectively enable them after installation:

- Oracle HTTP Server SSL listen port

  See Also: *Oracle HTTP Server Administrator's Guide*

- OracleAS Web Cache SSL listener port

  See Also: *Oracle Application Server Web Cache Administrator's Guide*

- Application Server Control SSL port

  See Also: Appendix A, "Managing and Configuring Application Server Control"

Simplified Starting and Stopping

The `opmnctl` command now starts and stops most Oracle Application Server components, in the proper order. This has greatly simplified starting and stopping an Oracle Application Server instance.

See Also: Chapter 3, "Starting and Stopping"

New Tools for Viewing Log Files

Oracle Application Server 10*g* provides the following new tools for viewing log files:

- Log Loader—collects data from various Oracle Application Server log files and consolidates it into a single log repository

  See Also: Chapter 4, "Managing Log Files"

- Log Viewer—a feature of Application Server Control, this is a Web-based tool for viewing log files and tracing problems across multiple log files

  See Also: Chapter 4, "Managing Log Files"

- `printlogs`—a command-line tool that reads and filters log messages and prints them to standard output in a single format

  See Also: Appendix E, "printlogs Tool Syntax and Usage"

Improved Port Management

Oracle Application Server 10*g* provides the following improvements for managing ports:

- You can specify the port number to assign to a particular component during installation by creating a template file (`staticports.ini`) and launching Oracle Universal Installer with special options. This is supported for most port numbers.

  See Also: *Oracle Application Server 10g Installation Guide*

- You can view all port numbers used in an Oracle Application Server instance on the Ports Page in Application Server Control.

  See Also: Chapter 5, "Managing Ports"

- Oracle provides complete instructions for changing port numbers, including dependencies on other components.

  See Also: Chapter 5, "Managing Ports"

Changing Infrastructure Services Used by a Middle-Tier Instance

You can change the Oracle Identity Management installation or OracleAS Metadata Repository used by a middle-tier instance after installation.

See Also: Chapter 8, "Changing Infrastructure Services"

New Tool for Changing the Hostname or IP Address

Oracle Application Server 10*g* offers a new tool (`chgiphost.sh`) that allows you to update Oracle Application Server installations when you change the hostname or IP address of your host.

See Also: Chapter 9, "Changing Network Configurations"

New Backup and Recovery Procedures and Tool

Oracle Application Server 10*g* offers complete backup and recovery procedures for your Oracle Application Server environment, along with an Oracle Application Server Backup and Recovery Tool.

See Also: Part IV, "Backup and Recovery"

New High Availability Solutions

Oracle Application Server 10*g* offers many high availability solutions, including:

- OracleAS Clusters Managed Using Database Repository
- OracleAS Clusters Managed Using File-based Repository
- OracleAS Cold Failover Cluster
- OracleAS Active Failover Cluster (Limited Release)
- OracleAS Disaster Recovery

See Also: *Oracle Application Server 10g High Availability Guide*

Part I

Getting Started

This part contains information for getting started with managing Oracle Application Server.

It contains the following chapters:

- Getting Started After Installing Oracle Application Server
- Introduction to Administration Tools
- Starting and Stopping

1

Getting Started After Installing Oracle Application Server

This chapter contains tasks to help you get started managing Oracle Application Server after installation.

It contains the following topics:

1.1 Task 1: Set Up Your Operating System User Account

When you installed Oracle Application Server, you were logged in to your operating system as a particular user. You should always log in as this user to manage your installation because this user has permission to view and modify the files in your installation's Oracle home.

You should set or modify some environment variables for this user, as described in Table 1–1.

Table 1–1 Oracle Application Server Environment Variables

Environment Variable	Value
DISPLAY	*hostname*:*display_number*.*screen_number* Beginning with Oracle Application Server 10*g*, very few tools require the DISPLAY variable. Only a few tools, such as oidadmin, require it.
LD_LIBRARY_PATH	Make sure this contains the following directory: $ORACLE_HOME/lib
ORACLE_HOME	Set to the full path of the installation's Oracle home
ORACLE_SID (Infrastructure installations only)	Set to the Metadata Repository SID you supplied during installation. The default is asdb.
PATH	Make sure this contains the following directories, which contain basic commands used by all installations: $ORACLE_HOME/bin $ORACLE_HOME/dcm/bin $ORACLE_HOME/opmn/bin When you start to work with specific components, you may want to add additional directories to your path, as recommended by the component documentation.

Best Practices for Multiple Installations on One Host

If you have multiple installations of Oracle Application Server on one host, it is very important to completely set your environment when managing a particular installation.

Some Oracle Application Server commands use the ORACLE_HOME environment variable to determine which installation to operate on, and some use the directory location of the command. It is, therefore, not sufficient to simply reset your

environment variables or `cd` into a different Oracle home as you move between installations. You must fully change to the new installation as follows:

- Log in as the user that installed the installation you want to work on.

  On UNIX hosts, you may also use the `su` command to switch to the user, but be sure to use the "`-`" (dash) option so your environment is set the same as it would have been had you actually logged in as the user.

  ```
  su - user
  ```

- Set the correct environment variables for the installation, as described in Table 1–1.
- Execute commands in the Oracle home of the correct installation.

Multiple Installations by the Same User If you installed multiple installations as the same user, that is fine. Just make sure you are in the correct Oracle home and have the correct environment variables set when working on a particular installation. You may want to set up some scripts to enable you to easily change from one installation to another.

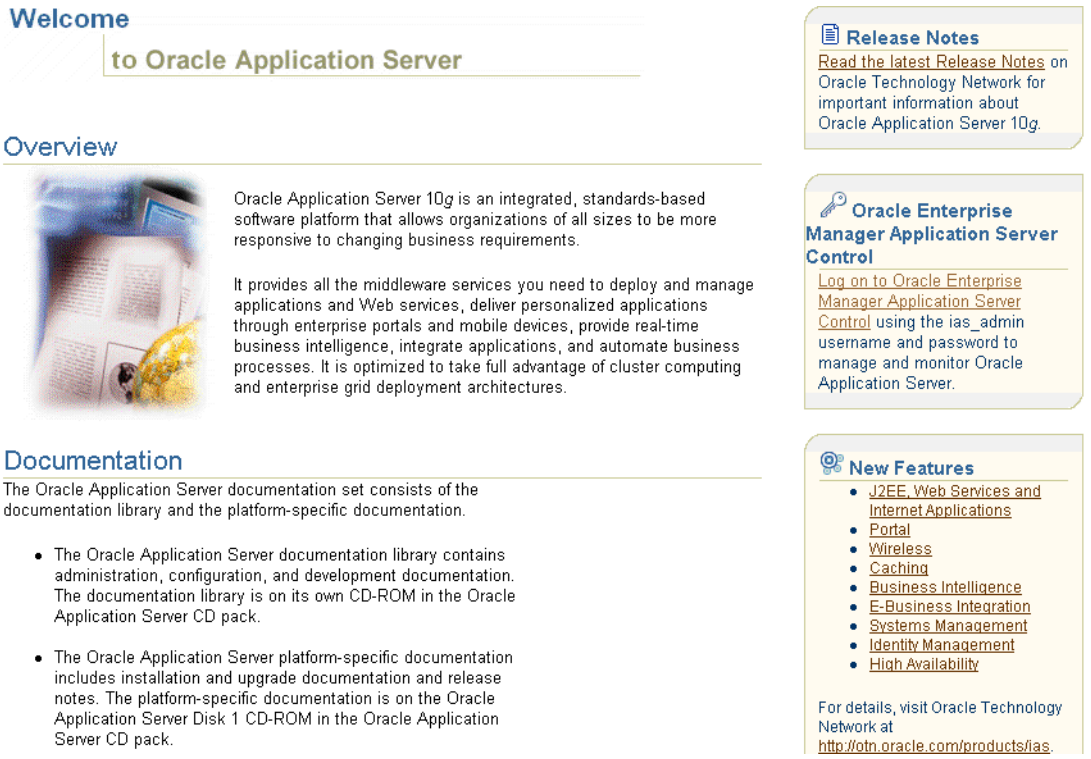
1.2 Task 2: Use the Oracle Application Server Welcome Page

The Oracle Application Server Welcome Page is a great starting point for managing your application server. It includes the following:

- Details about New Features in Oracle Application Server 10*g* (9.0.4)
- A Quick Tour that provides a graphical introduction to Oracle Application Server 10*g*
- Oracle Application Server 10*g* (9.0.4) documentation library
- Release Notes for your platform
- A link to Oracle Enterprise Manager Application Server Control—a Web-based tool for managing Oracle Application Server
- Demonstrations and code samples for Oracle Application Server components and features

Figure 1–1 shows the Oracle Application Server Welcome Page.

Figure 1–1 Oracle Application Server Welcome Page



Accessing the Welcome Page

You can locate the URL for accessing the Welcome Page on the End of Installation Screen text, which is in the following file:

ORACLE_HOME/Apache/Apache/setupinfo.txt

The Welcome Page is accessible using the HTTP listener port on your installation. For example:

http://*hostname.domain*:7777

Tip If you cannot access the Welcome Page, try the following:

1. Check `setupinfo.txt` and make sure you are using the correct URL (hostname and port number).
2. Try restarting Oracle HTTP Server:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=HTTP_Server
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=HTTP_Server
```

3. If you have OracleAS Web Cache configured, try restarting it:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=WebCache
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=WebCache
```

1.3 Task 3: Check Your Port Numbers

During installation, Oracle Application Server assigned port numbers to various components and services. It is important to check these port numbers for two reasons:

- You need to know these port numbers in order to start managing your application server.
- Oracle Application Server takes several measures to ensure that port number assignments are unique, however, it is possible that a port assignment could conflict with a non-Oracle Application Server process on your host that was not running during the installation. If you determine there is a conflict, stop the non-Oracle Application Server process and continue with the tasks in this chapter. Once you have completed the tasks in this chapter and have verified that your installation is running properly, you can consider changing Oracle Application Server port numbers.

  See Also: Chapter 5, "Managing Ports" for information on changing port numbers

You can find the complete list of port numbers in:

```
ORACLE_HOME/install/portlist.ini
```

Example 1–1 shows a sample copy of this file.

Example 1–1 A Sample portlist.ini File

```
;OracleAS Components reserve the following ports at install time.
;As a post-installation step, you can reconfigure a component to use a different
 port.
;Those changes will not be visible in this file.

[System]
Host Name = host1.mycompany.com
```

```
[Ports]
Oracle HTTP Server port =  7777
Oracle HTTP Server Listen port = 7778
Oracle HTTP Server SSL port = 4443
Oracle HTTP Server Listen (SSL) port = 4444
Oracle HTTP Server Diagnostic port = 7200
Oracle HTTP Server Jserv port = 8007
Application Server Control RMI port = 1850
Oracle Notification Server Request port = 6003
Oracle Notification Server Local port = 6100
Oracle Notification Server Remote port = 6200
Log Loader port = 44000
Java Object Cache port = 7000
DCM Java Object Cache port = 7101
Application Server Control port = 1810
Web Cache HTTP Listen port = 7777
Web Cache HTTP Listen (SSL) port = 4443
Web Cache Administration port = 4000
Web Cache Invalidation port = 4001
Web Cache Statistics port = 4002
```

Some things to note about `portlist.ini` are:

- As you view the `portlist.ini` file, you may wonder how the application server determines port assignments, or you may wish to change some of the port numbers. You should leave the port numbers as they are until you have completed the tasks in this chapter and confirmed that all of your components are running properly. Then, you can consider changing port numbers. Note that some port numbers cannot be changed, and some require additional steps for updating other components.

  See Also: Chapter 5, "Managing Ports" for information about port assignments and changing port numbers

- You may notice that `portlist.ini` contains port numbers for components you did not select during installation. This is because Oracle Application Server reserves ports for all components during installation, even those that were not configured. These port numbers will be used if you configure components after installation.

  See Also: Section 7.2, "Configuring Additional Components After Installation"

- The `portlist.ini` file contains the port numbers that were assigned during installation and is very useful for getting started. However, it is not updated if you modify port numbers after installation. Once you start managing the application server, you should use the Application Server Control Ports Page for viewing port numbers, because it displays the current port numbers.
- The default ports for Oracle Internet Directory are 389 (non-SSL) and 636 (SSL). However, many UNIX systems have these port numbers listed in `/etc/services`. This causes Oracle Application Server to assume the port numbers are in use and skip to the next port numbers in the allotted port range, which are 3060 (non-SSL) and 3130 (SSL). If you would rather use the standard port numbers (389 and 636), you can change them, after making sure you are not using those port numbers on your system.

  See Also: Section 5.6.2, "Changing Oracle Internet Directory Ports"

1.4 Task 4: Get Started with Managing Components

This task provides an introduction to managing components. It includes instructions for accessing component administration tools, post-installation notes about components, and pointers to more information.

- These components are configured in all installations:
  - Getting Started with Oracle Process Manager and Notification Server (OPMN)
  - Getting Started with Distributed Configuration Management (DCM)
  - Getting Started with Oracle HTTP Server
  - Getting Started with Oracle Application Server Containers for J2EE (OC4J)
- J2EE and Web Cache components:
  - Getting Started with OracleAS Web Cache
- Portal and Wireless components:
  - Getting Started with OracleAS Portal
  - Getting Started with OracleAS Wireless
- Business Intelligence and Forms components:
  - Getting Started with OracleAS Discoverer

- Getting Started with OracleAS Forms Services
- Getting Started with OracleAS Reports Services
- Getting Started with OracleAS Personalization

1.4.1 Getting Started with Oracle Process Manager and Notification Server (OPMN)

Oracle Process Manager and Notification Server (OPMN) manages and monitors most Oracle Application Server components. It is installed and configured in every middle-tier and Infrastructure installation and is essential for running Oracle Application Server.

To get started with OPMN, use the `opmnctl` command to query the status of the components in your installation:

```
ORACLE_HOME/opmn/bin/opmnctl status
```

Example 1–2 shows sample output from the command. It displays the component name, process type, operating system process ID (PID), and status of each process.

Example 1–2 Sample Output from opmnctl status

```
Processes in Instance: biforms.myhost.myco.com
------------------+--------------------+-------+---------
ias-component     | process-type       |   pid | status
------------------+--------------------+-------+---------
wireless          | OC4J_Wireless      |   404 | Alive
Discoverer        | PreferenceServer   |   403 | Alive
Discoverer        | OAD                |   405 | Alive
Discoverer        | OSAgent            |   402 | Alive
WebCache          | WebCacheAdmin      |   401 | Alive
WebCache          | WebCache           |   400 | Alive
HTTP_Server       | HTTP_Server        |   399 | Alive
OC4J              | OC4J_BI_Forms      |   445 | Alive
OC4J              | OC4J_Portal        |   413 | Alive
OC4J              | home               |   412 | Alive
dcm-daemon        | dcm-daemon         |   715 | Alive
LogLoader         | logloaderd         |   N/A | Down
```

Notice that the LogLoader process is always down after installation. Log Loader is a feature that compiles log messages from various log files into a single repository. You can start Log Loader after installation.

See Also: Section 4.5.1, "Starting and Stopping Log Loader"

You can use OPMN to start and stop your application server, monitor components, configure event scripts, and perform many other tasks related to process management.

See Also: *Oracle Process Manager and Notification Server Administrator's Guide*

1.4.2 Getting Started with Distributed Configuration Management (DCM)

Distributed Configuration Management (DCM) allows you to manage configuration information for application server instances, OracleAS Clusters, Oracle HTTP Server, Oracle Application Server Containers for J2EE (OC4J), Oracle Application Server Java Authentication and Authorization Service (JAZN) and OPMN.

DCM is installed and configured with every middle-tier and Infrastructure installation. All DCM installations use a DCM repository. There are two types of DCM repositories:

- Database—this repository is stored in the Metadata Repository in the `DCM` schema. This repository type is used by Portal and Wireless, and Business Intelligence and Forms installations. It is the repository for J2EE and Web Cache installations if you chose to use Managed OracleAS Clusters during installation.
- File Based—this repository is stored in the filesystem in your Oracle home. This repository type is used by J2EE and Web Cache installations if you chose to use File-based clusters during installation.

You can determine your repository type as follows:

```
ORACLE_HOME/dcm/bin/dcmctl whichFarm
```

During installation, DCM created a copy of your initial configuration with the `dcmctl saveInstance` command. If, after you start configuring your application server, you would like to return to the initial configuration, you can use the `dcmctl restoreInstance` command.

You can use DCM to save and restore configuration information, deploy applications, manage clusters, and much more.

See Also: *Distributed Configuration Management Reference Guide*

1.4.3 Getting Started with Oracle HTTP Server

Oracle HTTP Server is installed and configured with every middle-tier and Infrastructure installation.

You can access Oracle HTTP Server as follows:

`http://`*`hostname.domain`*`:`*`port`*

`port` is the Oracle HTTP Server Listen port number in:

`ORACLE_HOME``/install/portlist.ini`

For example:

`http://`*`hostname.domain`*`:7778`

When you access Oracle HTTP Server, you will see the Oracle Application Server Welcome Page.

See Also: *Oracle HTTP Server Administrator's Guide*

1.4.4 Getting Started with Oracle Application Server Containers for J2EE (OC4J)

Oracle Application Server Containers for J2EE (OC4J) is a complete Java 2 Enterprise Edition (J2EE) environment.

When you install an instance, you get the following OC4J instances, depending on your configuration:

- `home`—the default OC4J instance that comes with every middle-tier installation
- `OC4J_BI_Forms`—contains servlets that support OracleAS Reports Services and OracleAS Discoverer
- `OC4J_Portal`—contains a servlet that supports OracleAS Portal.
- `OC4J_Security`–supports Identity Management Services
- `OC4J_Wireless`—contains a servlet that supports OracleAS Wireless
- `oca`—supports OracleAS Certificate Authority

See Also: *Oracle Application Server Containers for J2EE User's Guide*

1.4.5 Getting Started with OracleAS Web Cache

If you configured OracleAS Web Cache during installation, you can access it as follows:

`http://hostname.domain:port`

port is the Web Cache HTTP Listen port number in:

ORACLE_HOME`/install/portlist.ini`

For example:

`http://hostname.domain:7777`

When you access OracleAS Web Cache, you will see the Oracle Application Server Welcome Page.

Accessing OracleAS Web Cache Manager

OracleAS Web Cache is a graphical user interface tool for configuring and monitoring OracleAS Web Cache.

You can access OracleAS Web Cache Manager by navigating to the following URL:

`http://hostname.domain:port/webcacheadmin`

port is the Web Cache HTTP Administration port number in:

ORACLE_HOME`/install/portlist.ini`

For example:

`http://hostname.domain:4000/webcacheadmin`

You can log in to OracleAS Web Cache Manager as `ias_admin` or `administrator`. The password for both accounts is the `ias_admin` password you supplied during installation.

> **See Also:** *Oracle Application Server Web Cache Administrator's Guide* for a list of post-installation configuration tasks

1.4.6 Getting Started with OracleAS Portal

If you configured OracleAS Portal during installation, you can access it as follows:

`http://hostname.domain:port/pls/portal`

port is the Web Cache HTTP Listen port number in:

ORACLE_HOME/install/portlist.ini

For example:

http://*hostname.domain*:7777/pls/portal

You can log in as portal using the ias_admin password you supplied during installation.

> **See Also:** *Oracle Application Server Portal Configuration Guide* for information on getting started and managing OracleAS Portal

1.4.7 Getting Started with OracleAS Wireless

If you configured OracleAS Wireless during installation, you can access it as follows:

http://*hostname.domain*:*port*/webtool/login.uix

port is the Web Cache HTTP Listen port number in:

ORACLE_HOME/install/portlist.ini

You can log in as orcladmin using the orcladmin password.

> **See Also:** *Oracle Application Server Wireless Administrator's Guide*

1.4.8 Getting Started with OracleAS Discoverer

If you configured OracleAS Discoverer during installation, you can access it as follows:

- Discoverer Viewer:

  http://*hostname.domain*:*port*/discoverer/viewer

- Discoverer Plus:

  http://*hostname.domain*:*port*/discoverer/plus

- Discoverer Portlet Provider:

  http://*hostname.domain*:*port*/discoverer/portletprovider

port is the Web Cache HTTP Listen port number in:

ORACLE_HOME/install/portlist.ini

> **See Also:** *Oracle Application Server Discoverer Configuration Guide* for additional steps for configuring Discoverer, including installing Discoverer workbooks and End User Layer (EUL) into each database that contains data to be analyzed

1.4.9 Getting Started with OracleAS Forms Services

If you configured OracleAS Forms Services during installation, you can access it as follows:

http://*hostname.domain*:*port*/forms90/f90servlet/admin

port is the Web Cache HTTP Listen port number in:

ORACLE_HOME/install/portlist.ini

> **See Also:** Refer to the OracleAS Forms Services online help for more information on configuring and using Forms

1.4.10 Getting Started with OracleAS Reports Services

If you configured OracleAS Reports Services during installation, you can access it as follows:

http://*hostname.domain*:*port*/reports/rwservlet/getserverinfo

port is the Web Cache HTTP Listen port number in:

ORACLE_HOME/install/portlist.ini

You can log in as `orcladmin` with the `orcladmin` password.

> **See Also:** *Oracle Application Server Reports Services Publishing Reports to the Web* for more information on configuring and using Reports

1.4.11 Getting Started with OracleAS Personalization

You must run the OracleAS Personalization Schema Creation Wizard, which creates the required schemas in the Oracle9*i* database. You can then start managing OracleAS Personalization.

See Also: *Oracle Application Server Personalization Administrator's Guide*

1.5 Task 5: Check the Status of OracleAS Metadata Repository Schemas

If you installed an OracleAS Metadata Repository, you may be interested to know the status of the various schemas accounts and passwords. This information can be found in the following tables:

- Table 1–2, " Post-Installation Status of Schemas in a Metadata Repository Registered with OID"

  Consult this table if you registered the Metadata Repository with Oracle Internet Directory.

- Table 1–3, " Post-Installation Status of Schemas in a Metadata Repository Not Registered with OID"

  Consult this table if you did not register the Metadata Repository with Oracle Internet Directory.

The tables contain the account status and initial password for each schema. They also contain recommended actions to perform immediately after installation, depending on your requirements.

To unlock an account using SQL*Plus (be sure to have your `ORACLE_HOME` and `ORACLE_SID` environment variables set before you run these commands):

```
ORACLE_HOME/bin/sqlplus "SYS/password_for_sys AS SYSDBA"
SQL> ALTER USER schema ACCOUNT UNLOCK;
```

To lock an account:

```
ORACLE_HOME/bin/sqlplus "SYS/password_for_sys AS SYSDBA"
SQL> ALTER USER schema ACCOUNT LOCK;
```

The method for changing passwords varies by schema. Refer to Section 6.2, "Changing Schema Passwords" to determine the proper way to change a password.

Table 1–2 displays the postinstallation status of schemas in a Metadata Repository registered with Oracle Internet Directory.

Table 1–2 Post-Installation Status of Schemas in a Metadata Repository Registered with OID

Schema	Account Status	Password	Recommended Action after Installation
Standard Oracle Database Schemas			
AURORAJISUTILITY$	OPEN, NO CREATE SESSION	RANDOM	
AURORAORBUNAUTHENTICATED	OPEN	RANDOM	
CTXSYS	LOCKED	RANDOM	
DBSNMP	OPEN	DBSNMP	This schema is not used by Oracle Application Server; you can change the password and lock the account
MDSYS	LOCKED	EXPIRED	
ORDPLUGINS	LOCKED	EXPIRED	
ORDSYS	LOCKED	EXPIRED	
OSE$HTTP$ADMIN	OPEN	RANDOM	
OUTLN	LOCKED	EXPIRED	
SCOTT	OPEN	TIGER	You can change the password if you want. Some demos may not work if you do so.
SYS	OPEN	Set by user during installation	
SYSTEM	OPEN	Set by user during installation	
Oracle Application Server Schemas			
DCM	OPEN	RANDOM - Stored in OID	
DISCOVERER5	OPEN	RANDOM - Stored in OID	
DSGATEWAY	OPEN	RANDOM - Stored in OID	
INTERNET_APPSERVER_REGISTRY	LOCKED, NO CREATE SESSION	EXPIRED	
IP	OPEN	RANDOM - Stored in OID	
OCA	OPEN	RANDOM - Stored in OID	

Table 1–2 (Cont.) Post-Installation Status of Schemas in a Metadata Repository Registered with OID

Schema	Account Status	Password	Recommended Action after Installation
ODS	OPEN	Same as the ias_admin password supplied during installation	
ORAOCA_PUBLIC	OPEN	RANDOM - Stored in OID	
ORASSO	OPEN	RANDOM - Stored in OID	
ORASSO_DS	OPEN	RANDOM - Stored in OID	
ORASSO_PA	OPEN	RANDOM - Stored in OID	
ORASSO_PS	OPEN	RANDOM - Stored in OID	
ORASSO_PUBLIC	OPEN	RANDOM - Stored in OID	
OWF_MGR	OPEN	RANDOM - Stored in OID	
PORTAL	OPEN	RANDOM - Stored in OID	
PORTAL_APP	OPEN	RANDOM - Stored in OID	
PORTAL_DEMO	OPEN	RANDOM - Stored in OID	
PORTAL_PUBLIC	OPEN	RANDOM - Stored in OID	
UDDISYS	OPEN	RANDOM - Stored in OID	
WCRSYS	OPEN	RANDOM - Stored in OID	
WIRELESS	OPEN	RANDOM - Stored in OID	
WK_TEST	LOCKED	EXPIRED	If you would like to run Oracle Ultra Search demos, unlock and set a password
WKPROXY	OPEN	RANDOM - Stored in OID	
WKSYS	OPEN	RANDOM - Stored in OID	

Table 1–3 displays the postinstallation status of schemas in a Metadata Repository that is not registered with Oracle Internet Directory

Table 1–3 Post-Installation Status of Schemas in a Metadata Repository Not Registered with OID

Schema	Account Status	Password	Recommended Action after Installation
Standard Oracle Database Schemas			
AURORAJISUTILITY$	OPEN, NO CREATE SESSION	RANDOM	
AURORAORBUNAUTHENTICATED	OPEN	RANDOM	
CTXSYS	LOCKED	RANDOM	
DBSNMP	OPEN	DBSNMP	This schema is not used by Oracle Application Server; you can change the password and lock the account
MDSYS	LOCKED	EXPIRED	
ORDPLUGINS	LOCKED	EXPIRED	
ORDSYS	LOCKED	EXPIRED	
OSE$HTTP$ADMIN	OPEN	RANDOM	
OUTLN	LOCKED	EXPIRED	
SCOTT	OPEN	TIGER	You can change the password if you want. Some demos may not work if you do so.
SYS	OPEN	Set by user during installation	
SYSTEM	OPEN	Set by user during installation	
Oracle Application Server Schemas			
DCM	LOCKED	EXPIRED	If you intend to use Managed OracleAS Clusters using Database Repository, unlock and set a password
DISCOVERER5	LOCKED	EXPIRED	
DSGATEWAY	LOCKED	EXPIRED	
INTERNET_APPSERVER_REGISTRY	LOCKED, NO CREATE SESSION	EXPIRED	

Table 1–3 (Cont.) Post-Installation Status of Schemas in a Metadata Repository Not Registered with

Schema	Account Status	Password	Recommended Action after Installation
IP	LOCKED	EXPIRED	
OCA	LOCKED	EXPIRED	
ODS	LOCKED	EXPIRED	
ORAOCA_PUBLIC	LOCKED	EXPIRED	
ORASSO	LOCKED	EXPIRED	
ORASSO_DS	LOCKED	EXPIRED	
ORASSO_PA	LOCKED	EXPIRED	
ORASSO_PS	LOCKED	EXPIRED	
ORASSO_PUBLIC	LOCKED	EXPIRED	
OWF_MGR	LOCKED	EXPIRED	
PORTAL	LOCKED	EXPIRED	
PORTAL_APP	LOCKED	EXPIRED	
PORTAL_DEMO	LOCKED	EXPIRED	
PORTAL_PUBLIC	LOCKED	EXPIRED	
UDDISYS	LOCKED	EXPIRED	
WCRSYS	LOCKED	EXPIRED	
WIRELESS	LOCKED	EXPIRED	
WK_TEST	LOCKED	EXPIRED	
WKPROXY	LOCKED	EXPIRED	
WKSYS	LOCKED	EXPIRED	

1.6 Task 6: Enable SSL (Optional)

During installation, SSL is not configured for some components. If you would like to enable SSL, you can consult the component documentation for instructions.

SSL is not enabled for the following components during installation:

- Oracle HTTP Server—refer to *Oracle HTTP Server Administrator's Guide*.

- OracleAS Web Cache—refer to *Oracle Application Server Web Cache Administrator's Guide*.
- Oracle Enterprise Manager Application Server Control—refer to Section A.4, "Configuring Security for Enterprise Manager Application Server Control".
- OracleAS Personalization—refer to *Oracle Application Server Release Notes* for your platform.

1.7 What's Next?

Several more tasks to get you started are:

- Learn about Oracle Application Server administration tools—refer to Chapter 2, "Introduction to Administration Tools".
- Learn how to start and stop Oracle Application Server—refer to Chapter 3, "Starting and Stopping".
- Learn about Oracle Application Server backup and recovery, and perform a backup of your installation—refer to Part IV, "Backup and Recovery".

2

Introduction to Administration Tools

This chapter introduces the Oracle Application Server administration tools.

It contains the following topics:

2.1 Overview of Oracle Application Server Administration Tools

Oracle realizes that the procedures you use to monitor and administer your application server components can vary, depending upon the size of your organization, the number of administrators you employ, and the types of components you manage. As a result, Oracle offers options for managing your Oracle Application Server installations.

These management options can be divided into the following categories:

- Managing Oracle Application Server with Oracle Enterprise Manager
- Managing Oracle Application Server from the Command Line
- Using Other Tools to Monitor the Built-In Performance Metrics

2.1.1 Managing Oracle Application Server with Oracle Enterprise Manager

The primary tool for managing Oracle Application Server—as well as your entire Oracle environment—is Oracle Enterprise Manager. To manage Oracle Application Server, you use Oracle Enterprise Manager Application Server Control.

Application Server Control is installed with every instance of Oracle Application Server. As a result, you can immediately begin managing your application server and its components from your Web browser.

Note: If you select the Oracle Application Server Metadata Repository-only installation type, Application Server Control is installed, but it is not configured or started automatically by the installation procedure. In fact, there is no need to start or use Application Server Control for the Metadata Repository-only installation type.

For information, see Section 2.5, "Managing the OracleAS Metadata Repository Database".

From Application Server Control, you can monitor and administer a single Oracle Application Server instance, a farm of application server instances, or an Oracle Application Server cluster.

Application Server Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for each application server component. The Enterprise Manager home pages make it easy to locate the

most important monitoring data and the most commonly used administrative functions—all from your Web browser.

> **See Also:** Section 2.2, "About Oracle Enterprise Manager Application Server Control"

2.1.2 Managing Oracle Application Server from the Command Line

Oracle Application Server also provides command-line interfaces to several key management technologies. After you become familiar with the architecture and components of your application server, command-line tools can help you automate your management procedures with scripts and custom utilities.

The two most important administration command-line tools are:

- `opmnctl`, which provides a command-line interface to Oracle Process Management Notification (OPMN). You can use `opmnctl` to:
  - Start and stop components, instances, and OracleAS Clusters
  - Monitor processes

  > **See Also:** Section 2.2.2, "About the Underlying Technologies" and *Oracle Process Manager and Notification Server Administrator's Guide*

- `dcmctl`, which provides a command-line interface to Distributed Configuration Management (DCM). You can use `dcmctl` to:
  - Create and remove OC4J instances and OracleAS Clusters
  - Deploy and undeploy OC4J applications
  - Archive and restore configuration information
  - Obtain configuration information

  > **See Also:** Section 2.2.2, "About the Underlying Technologies" and *Distributed Configuration Management Reference Guide*

In addition to `opmnctl` and `dcmctl`, Oracle Application Server provides many other command-line tools for performing specific tasks.

> **See Also:** Appendix B, "Oracle Application Server Command-Line Tools"

2.1.3 Using Other Tools to Monitor the Built-In Performance Metrics

After you install and start Oracle Application Server, the application server automatically begins gathering a set of built-in performance metrics. These built-in performance metrics are measured continuously using performance instrumentation inserted into the implementations of Oracle Application Server components.

Application Server Control presents a subset of these performance metrics in an organized fashion on the application server component home pages. For example, the Oracle HTTP Server metrics are presented as a series of charts on the Performance property page, which is available from the Oracle HTTP Server home page.

Alternatively, you may want to view the complete set of built-in performance metrics, or you may need to monitor a specific set of application server component metrics. As a result, Oracle Application Server also provides a set of command-line and servlet-based tools to view the Oracle Application Server built-in performance metrics directly, outside of the Application Server Control.

See Also: *Oracle Application Server 10g Performance Guide*

2.2 About Oracle Enterprise Manager Application Server Control

Oracle Enterprise Manager Application Server Control provides Web-based management capabilities designed specifically for Oracle Application Server. Using the Application Server Control, you can monitor, diagnose, and configure the components of your application server. You can deploy applications, manage security, and create and manage Oracle Application Server clusters.

The Oracle Enterprise Manager Application Server Control consists of:

- The Enterprise Manager home pages that you use to manage Oracle Application Server

  These Web pages provide you with a high-level view of your Oracle Application Server environment. You can then drill down for more detailed performance and diagnostic information.

  See Also: Section 2.2.1, "Introducing the Enterprise Manager Home Pages"

- The underlying software technologies that keep track of your application server instances and components

These technologies automatically perform many of the management tasks as you select options and functions within Application Server Control. For example, they discover the components of each application server instance, gather and process performance data, and provide access to application configuration information.

See Also: Section 2.2.2, "About the Underlying Technologies"

2.2.1 Introducing the Enterprise Manager Home Pages

Oracle Application Server provides a wide variety of software solutions designed to help you run all aspects of your business. As a result, you will want to manage Oracle Application Server from different levels of detail.

At times, you may want to manage a single application server instance; or, you may find it efficient to combine multiple instances into an Oracle Application Server cluster. At other times, you will want to manage a specific application server component.

To support these multiple levels of management, Oracle introduces the Oracle Enterprise Manager home pages. Each home page provides the information you need to monitor the performance and availability of Oracle Application Server from a particular level of management detail. Selected home pages also provide tools for configuring your Oracle Application Server components.

From each home page, you can obtain high-level information or you can drill down to get more specific information about an instance, component, or application.

Consider the following home pages that are available when you use the Application Server Control:

- Use the OracleAS Farm home page to view a set of related application server instances on your network and to create clusters that speed up the configuration and deployment of your Web applications. For more information, see Section 2.3.3, "Using the Oracle Application Server Farm Home Page".
- Use the Application Server home page to manage all aspects of an individual application server instance. For more information, see Section 2.3.2, "Using the Application Server Home Page".
- Drill down to a component home page to monitor or configure an individual component of the application server. For example, use the Oracle HTTP Server home page to monitor the performance of your Web server, or use the Oracle Containers for J2EE (OC4J) home page to deploy a custom Web-based

application. For more information, see Section 2.3.4, "Using an Oracle Application Server Component Home Page".

2.2.2 About the Underlying Technologies

Application Server Control relies on various technologies to discover, monitor, and administer the Oracle Application Server environment. Table 2–1 provides a summary of the underlying technologies leveraged by Application Server Control.

Table 2–1 Summary of the Application Server Control Underlying Technologies

Technology	Description
Dynamic Monitoring Service (DMS)	The Oracle Enterprise Manager Application Server Control uses DMS to gather performance data about your Oracle Application Server components. For more information, see *Oracle Application Server 10g Performance Guide*.
Oracle Process Manager and Notification Server (OPMN)	OPMN manages Oracle HTTP Server, OC4J, and other Oracle Application Server processes. It channels all events from different component instances to all components interested in receiving them. For more information, see *Oracle Process Manager and Notification Server Administrator's Guide*.
Distributed Configuration Management (DCM)	DCM manages configurations among application server instances that are associated with common Infrastructure Services (members of an Oracle Application Server Farm). It enables Oracle Application Server cluster-wide deployment so you can deploy an application to an entire cluster, or make a single host or instance configuration change applicable across all instances in a cluster. The Oracle Enterprise Manager Application Server Control uses DCM to make configuration changes and to propagate configuration changes and deployed applications across the cluster. For more information, see *Distributed Configuration Management Reference Guide*.
Oracle Management Agent	A local version of the Oracle Management Agent designed specifically to monitor and administer your application server components.
Oracle Management Watchdog Process	The Management Watchdog Process monitors the Management Agent and the Application Server Control to make sure both processes are running and available at all times.

2.2.3 Managing Previous Versions of Oracle Application Server

Previous versions of Oracle Application Server (specifically, Oracle9*i* Application Server 9.0.2 and 9.0.3) included the Oracle Enterprise Manager Web site, a Web-based tool that offers management capabilities similar to those provided by Application Server Control.

In fact, you can still use the Enterprise Manager Web site to manage previous versions of Oracle9*i* Application Server after you begin deploying Oracle Application Server 10*g* (9.0.4) and its Application Server Control.

However, if you are familiar with the Enterprise Manager Web site and you plan to continue managing previous versions of Oracle Application Server, you should be aware of several differences between the Enterprise Manager Web site and the new Application Server Control. In particular, you should note the following:

- Oracle9*i* Application Server (9.0.2) and Oracle9*i* Application Server (9.0.3) used one Enterprise Manager Web site to manage all the application server instances on a host.

  You could navigate to individual Enterprise Manager home pages for each application server, but only one instance of the Enterprise Manager Web site was running on the host and you managed all the application server instances from one Enterprise Manager Web site URL. This approach to application server management was convenient, but it required all application server instances to be installed and managed by the same operating system user.

- The current version of Oracle Application Server provides one Application Server Control for each application server instance on a host.

  For example, if you install two application server instances on a single host, and you want to manage both instances, two separate instances of the Application Server Control—one for each application server instance—must be started on the host.

  As a result, each application server instance provides a unique URL (specifically, a unique HTTP Server listening port number) for accessing the Application Server Control.

- If you have Oracle9*i* Application Server (9.0.2 or 9.0.3) and Oracle Application Server 10*g* (9.0.4) instances on the same host, and you have to deinstall a 9.0.2 or 9.0.3 instance, you must apply a patch to ensure Oracle Enterprise Manager continues to work after the change. Refer to the section on deinstallation of 9.0.2 or 9.0.3 instances from a computer that also contains 10g (9.0.4) instances in *Oracle Application Server 10g Installation Guide*.

See Also: Section A.1, "Starting and Stopping Application Server Control"

2.2.4 Using Application Server Control Online Help

At any time while using Application Server Control, you can click **Help** at the top of the page to get more information. In most cases, the Help window displays a help topic about the current page. Click **Help Contents** in the Help window to browse the list of help topics or to search for a particular word or phrase.

2.3 Getting Started with Application Server Control

Use the following sections to get started with the Application Server Control and become familiar with the Enterprise Manager home pages within Application Server Control:

- Displaying Oracle Enterprise Manager Application Server Control
- Using the Application Server Home Page
- Using the Oracle Application Server Farm Home Page
- Using an Oracle Application Server Component Home Page

2.3.1 Displaying Oracle Enterprise Manager Application Server Control

The following sections describe how to display the Application Server Control and introduce you to the initial home pages you should see when you display Application Server Control for the first time:

- Using the Application Server Control URL
- Displaying Application Server Control from the Welcome Page
- Understanding the Initial Application Server Control Home Page

2.3.1.1 Using the Application Server Control URL

The URL for the Application Server Control is included in the text file that displays at the end of the Oracle Application Server installation procedure. This text file is saved in the following location after you install the application server:

ORACLE_HOME/Apache/Apache/setupinfo.txt

The Application Server Control URL typically includes the name of the host computer and the port number assigned to the Application Server Control during the installation. For example:

```
http://mgmthost1.acme.com:1810
```

> **Note:** The default port for the Application Server Control is usually 1810; however, if that port is in use, the installation procedure will assign another port. Refer to the `setupinfo.txt` file for the exact port for your installation of Oracle Application Server.

2.3.1.2 Displaying Application Server Control from the Welcome Page

To view Application Server Control from the Oracle Application Server Welcome Page:

1. Display the Oracle Application Server Welcome Page by entering the following URL in your Web browser:

   `http://`*`hostname.domain`*`:`*`port`*

   For example, if you installed Oracle Application Server on a host called `sys42`, you would enter the following address in your Web browser:

   ```
   http://sys42.acme.com:7777
   ```

   > **Note:** The default port for Oracle HTTP Server (and, as a result, the Welcome page) is usually 7777, but Oracle Application Server installation procedure will use the next available port number if 7777 is unavailable. The actual port number is described in the text file (`setupinfo.txt`) that is generated and displayed at the end of the Oracle Application Server installation.

2. Click **Log on to Oracle Enterprise Manager Application Server Control**.

   Enterprise Manager displays the administrator logon dialog box.

3. Enter the Oracle Application Server administrator user name and password and click **OK**.

   The user name for the administrator user is `ias_admin`. The password the one you supplied during the installation of Oracle Application Server.

2.3.1.3 Understanding the Initial Application Server Control Home Page

When you first display Application Server Control, the initial home page you see varies depending upon whether or not the instance uses an OracleAS Metadata Repository (belongs to a farm).

See Also: *Oracle Application Server 10g Installation Guide* for your platform

Table 2–2 describes the Enterprise Manager home pages that might be used as a starting point when you first browse to Application Server Control.

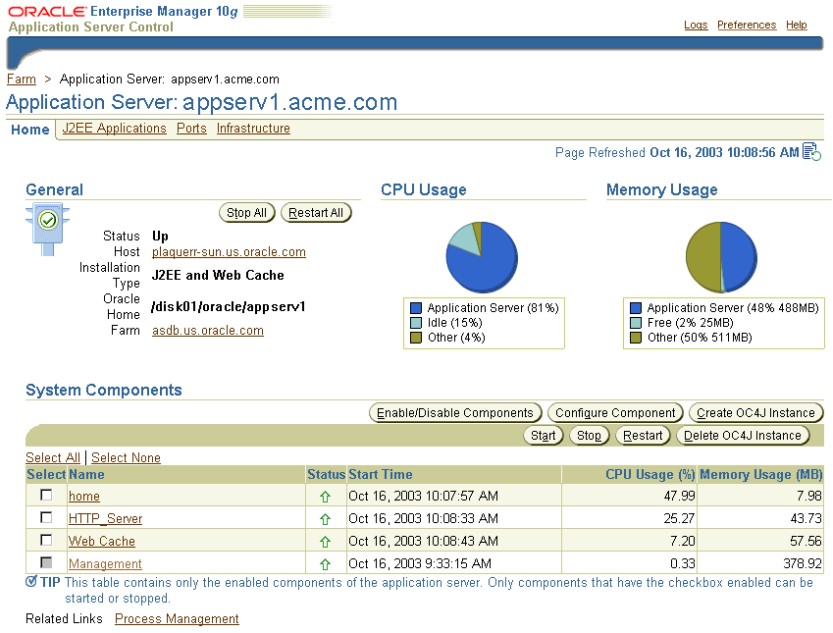
Table 2–2 Enterprise Manager Home Pages for Managing Oracle Application Server

Enterprise Manager Home Page	Description
Application Server home page	Use this home page to monitor and configure a single application server instance. For more information, see "Using the Application Server Home Page" on page 2-10. The Application Server home page is the first page you see if you have installed a single application server instance that is not using an OracleAS Metadata Repository.
OracleAS Farm home page	Use this home page to view a list of all the application server instances that use a common OracleAS Metadata Repository. For more information, see "Using the Oracle Application Server Farm Home Page" on page 2-12. The Farm home page is the first page you see if you have installed one or more application server instances that use a common set of Infrastructure Services—or more specifically, a common metadata repository.

2.3.2 Using the Application Server Home Page

From the Application Server home page (Figure 2–1), you can start and stop the application server instance, monitor the overall performance of the server, and review the components of the server. You can also drill down and examine the performance of a particular component and configure the component.

Figure 2–1 Application Server home page



If you scroll down the page, the home page provides a table that lists the components of the application server. From this table, you can also get a snapshot of how each individual component is performing.

From the **System Components** table, you can display a home page for each component of the application server.

You can perform the following management functions from the Instance home page:

- Click **Logs** at the top of the page to locate and search the various Oracle Application Server log files, as well as the Oracle Application Server Log Repository.
- Click **J2EE Applications** to display a list of the applications deployed on this instance of Oracle Application Server.
- Click **Ports** to view a list of all the ports currently in use by the various Oracle Application Server components. You can also modify many of the port assignments when necessary.

- Click **Infrastructure** to use Identity Management, Central Management, or the cluster capabilities of Oracle Application Server.
- Click **Enable/Disable Components** to control whether or not the selected components are started automatically or affected by server-wide actions, such as **Start All** or **Restart All**. When a component is disabled, you can always enable it later.

For more information, click **Help** after selecting an option on the Application Server home page.

> **See Also:** Section 2.2.4, "Using Application Server Control Online Help"

2.3.3 Using the Oracle Application Server Farm Home Page

If your application server instance uses an OracleAS Metadata Repository, your start page for Application Server Control is the OracleAS Farm home page (Figure 2–2).

> **See Also:** *Oracle Application Server 10g Installation Guide* for your platform information about installing an OracleAS Metadata Repository

The Farm home page displays a list of the standalone application server instances and Oracle Application Server clusters associated with your Infrastructure Services. Standalone instances are application server instances that are not part of an Oracle Application Server cluster.

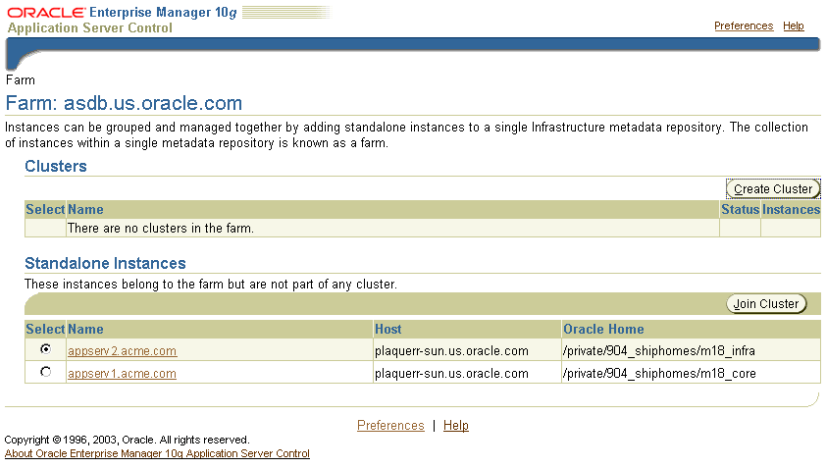
You can configure your application server instance to use Infrastructure Services by clicking **Infrastructure** on the Application Server home page. For more information, see the Enterprise Manager online help.

Using the Farm home page, you can perform the following tasks:

- Manage multiple application server instances on multiple hosts
- Drill down to the Application Server home page for each instance
- Create and manage Oracle Application Server clusters

> **See Also:** *Oracle Application Server 10g High Availability Guide* for more information about using Oracle Application Server clusters

Figure 2–2 The OracleAS Farm home page



2.3.4 Using an Oracle Application Server Component Home Page

Oracle Application Server component home pages vary from one component to another because each component has different monitoring and configuration requirements. However, most of the component home pages have the following common elements:

- A general information section that includes an icon to indicate the current state of the component and buttons for starting and stopping the component (if applicable)
- Status information, including CPU and memory usage information, so you can get a snapshot of how the component is performing
- Component-specific information, such as a virtual hosts tab on the HTTP Server home page or a list of deployed applications on the OC4J home page
- Links to administrative functions where appropriate, so you can modify the configuration of selected components. In many cases, this means you can use a graphical user interface to modify complex configuration files.

2.4 Monitoring and Diagnosing with Application Server Control

The Application Server Control is designed to encourage a top-down approach to your monitoring and diagnostic activities. For example, you can start by reviewing

the basic characteristics of your application server on the Application Server home page and then drill down to examine the performance of individual components of the server.

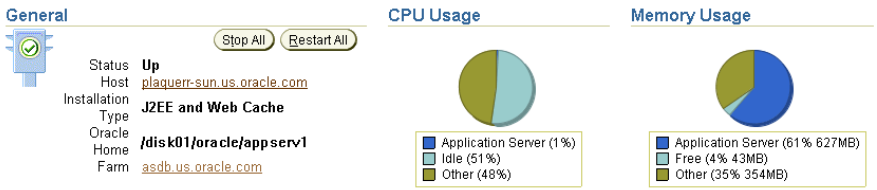
The following sections provide an outline of this monitoring methodology:

- Reviewing General Information and Resource Usage
- Reviewing the Resources of the Application Server Host
- Monitoring Application Server Components
- Monitoring Your J2EE Applications

2.4.1 Reviewing General Information and Resource Usage

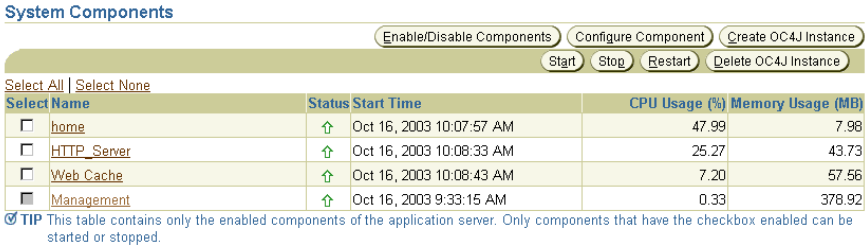
The Application Server home page provides general information about the status of your server, including the name, location, and application server availability. The home page also provides high-level information about CPU and Memory usage. When reviewing the home page, review the CPU Usage and Memory Usage charts for excessive CPU or Memory usage by the application server (Figure 2–3).

Figure 2–3 General Section of the Application Server Home Page



If you suspect that the application server is using too many resources, review the list of components to confirm that each component is up and running and to review the resource usage by each component (Figure 2–4).

Figure 2–4 System Components Table on the Application Server Home Page



Consider disabling any components that you are not currently using as part of this application server instance. Disabled components are not started when you start the application server and as a result do not consume system resources.You can always enable a disabled application server component at a later time.

> **See Also:** 'Disabling and Enabling Components" in the Enterprise Manager online help

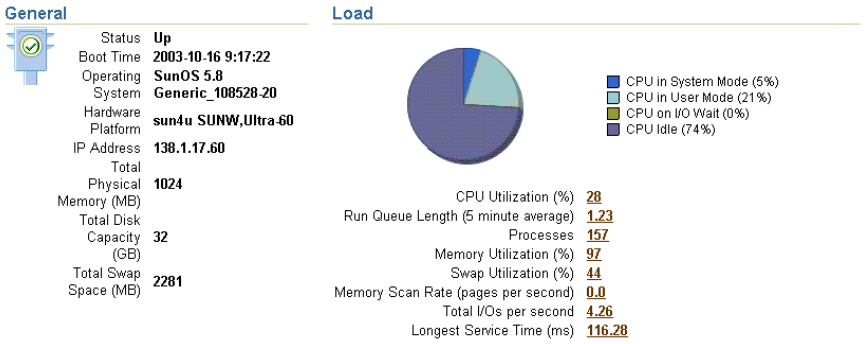
2.4.2 Reviewing the Resources of the Application Server Host

Many performance or configuration issues are directly related to a lack of available resources on the host. Before you drill down to analyze the performance and resource usage of the individual application server components, review the resources and characteristics of the application server host.

Click the host name in the General section of the Application Server home page to display the Host home page. The Host home page provides a summary of the operating system, memory, and disk capacity. The Load section of the page provides a CPU chart that breaks down the CPU usage into categories of usage; the load metrics beneath the chart provide details about system memory usage (Figure 2–5).

> **See Also:** "About Memory Usage" in the Enterprise Manager online help for information about how Enterprise Manager calculates the memory usage for your application server.

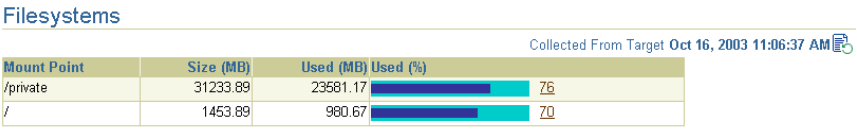
Figure 2–5 General Information and Load Statistics on the Host Home Page



Scroll to the bottom of the page to view a set of links to real-time performance metrics. If you are concerned about the CPU and Memory usage on the system, click **Top Processes** to display tables listing the processes that are using the most resources on the host.

Click **Filesystems** to display a bar chart that reveals the amount of disk space available on the application server host (Figure 2–6).

Figure 2–6 Disk Space Usage Chart Available from the Host Home Page



2.4.3 Monitoring Application Server Components

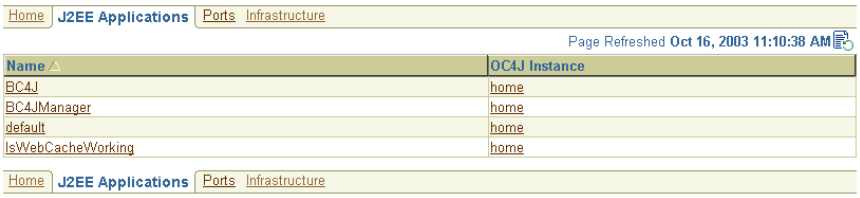
After you review the high-level performance metrics and the resources available on the application server host computer, you can then begin to look for potential issues within the individual application server components.

To diagnose problems with individual application server components, click the component name in the **System Components** table on the Application Server home page. This technique of "drilling down" to obtain more detail can help you isolate problems in a particular component or area of the application server.

2.4.4 Monitoring Your J2EE Applications

The J2EE applications you deploy and maintain with Oracle Application Server represent the most important aspects of your application server deployments. As a result, Enterprise Manager also provides a shortcut you can use to review the performance of your J2EE applications. Simply click **J2EE Applications** on the Application Server home page to display a list of the applications deployed from this application server instance (Figure 2–7).

Figure 2–7 List of Applications on the J2EE Applications Page



From this list of J2EE applications, you can navigate quickly to the OC4J instance or application page for information on the performance and availability of each application you have deployed.

2.4.5 Obtaining More Information about Monitoring Oracle Application Server

For more complete information about monitoring Oracle Application Server, refer to the Application Server Control online help and the *Oracle Application Server 10g Performance Guide*.

2.5 Managing the OracleAS Metadata Repository Database

Many features of Oracle Application Server depend upon OracleAS Infrastructure 10*g*, which uses an Oracle database to contain the OracleAS Metadata Repository.

> **See Also:** *Oracle Application Server 10g Installation Guide* for your platform

When you install the OracleAS Metadata Repository, you can choose to install a preconfigured Oracle9*i* database for the OracleAS Metadata Repository. This Oracle9*i* database comes with its own management tools.

Specifically, the OracleAS Metadata Repository database comes with the Oracle Enterprise Manager Java-based Console, which is part of the Oracle Enterprise Manager software provided with all Oracle9*i* databases.

However, this version of the Console is designed specifically to manage the OracleAS Metadata Repository database; as a result, it does not include all of the Enterprise Manager framework components, such as the Oracle Management Server, the Management Repository, or the Intelligent Agent.

> **See Also:** *Oracle Enterprise Manager Concepts* in the Oracle9*i* documentation library for more information about the Enterprise Manager framework components and architecture

When you use the Enterprise Manager Console without a Management Server or Management Repository, you are using the Console in standalone mode.

To launch the Enterprise Manager Console in standalone mode:

1. Enter the following command in the Oracle home directory of your OracleAS Infrastructure 10*g* installation:

   ```
   ORACLE_HOME/bin/oemapp console
   ```

   Enterprise Manager displays the Console login dialog box.

2. Select **Launch Standalone** and click **OK**.

   Enterprise Manager launches the Console.

3. When the Console window appears, expand the **Databases** folder in the Navigator frame.

   The OracleAS Metadata Repository database appears as an available database.

4. Click the plus sign (+) next to the database name.

   Enterprise Manager displays the Database Connect Information dialog box.

5. Enter the credentials for the OracleAS Metadata Repository database and click **OK**.

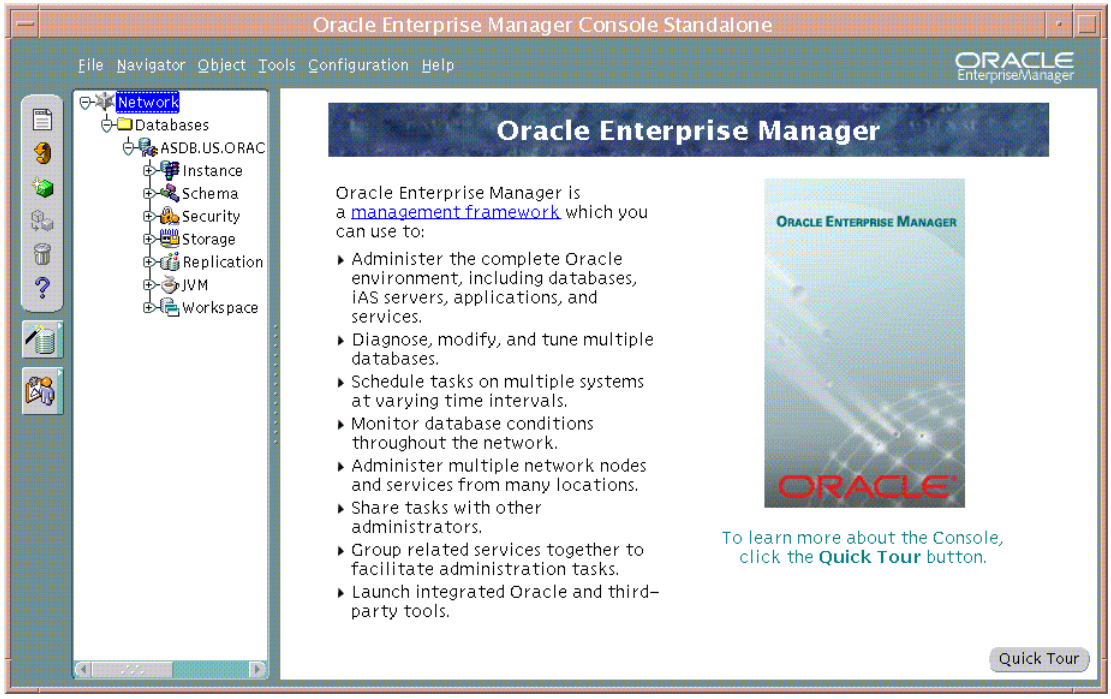
   These are the credentials you specified for the database during the OracleAS Metadata Repository installation.

   When you connect to the database, a set of database objects appear in the Navigator. Objects within the Navigator can be managed via context-sensitive menus. For example, you can perform many administration tasks from the Navigator, such as creating, editing, or dropping tablespaces.

Figure 2–8 shows the Console window after you connect to the OracleAS Metadata Repository.

See Also: *Oracle Enterprise Manager Administrator's Guide* in the Oracle9*i* documentation library and the Console online help for more information about using the Console to manage your OracleAS Metadata Repository

Figure 2–8 Managing the OracleAS Metadata Repository with the Oracle Enterprise Manager Java Console



3

Starting and Stopping

This chapter describes various procedures for starting and stopping Oracle Application Server.

It contains the following topics:

3.1 Overview of Starting and Stopping Procedures

Oracle Application Server is a flexible product that you can start and stop in different ways, depending on your requirements. This chapter contains the following sections:

- Starting and Stopping Application Server Instances

  Follow the procedures in this section when starting an instance from scratch, for example, after a reboot, or when you would like to stop your entire instance, for example, in preparation for shutting down your system.

- Starting and Stopping Components

  Use the procedures in this section after you have started your instance and would like to start or stop individual components.

- Enabling and Disabling Components

  This section describes how to disable components (prevent them from starting when you start an instance) and enable components (allow them to start when you start an instance).

- Starting and Stopping an Oracle Application Server Environment

  This section describes how to perform an orderly shutdown of your entire environment.

3.2 Starting and Stopping Application Server Instances

This section describes how to start and stop application server instances. It contains the following topics:

- Starting an Infrastructure
- Stopping an Infrastructure
- Starting a Middle-Tier Instance
- Stopping a Middle-Tier Instance

Note that Oracle provides scripts that perform the procedures in this section. You can find them on the "OracleAS RepCA and Utilities" CD-ROM in the `utilities/startup` directory.

3.2.1 Starting an Infrastructure

This section describes how to start all processes in an Infrastructure. You can follow this procedure after you have rebooted your host, or any other time you would like to start up your entire Infrastructure.

This procedure applies to all Infrastructure types:

- Identity Management and Metadata Repository

  Follow both steps to start Identity Management and the Metadata Repository.

- Metadata Repository only

  Follow only the first step to start the Metadata Repository. You do not need to perform the second step of starting Identity Management because you do not need OPMN or Application Server Control in a Metadata Repository only installation.

- Identity Management only

  Follow only the second step to start Identity Management. Make sure the Metadata Repository that supports Identity Management (residing in another Oracle home) is already started.

To start an Infrastructure:

1. If your Infrastructure contains a Metadata Repository, start it as follows:

   a. Set the `ORACLE_HOME` environment variable to the Infrastructure Oracle home.

   b. Set the `ORACLE_SID` environment variable to the Metadata Repository SID (default is `asdb`).

   c. Start the Net Listener:

      ```
      ORACLE_HOME/bin/lsnrctl start
      ```

   d. Start the Metadata Repository instance:

      ```
      ORACLE_HOME/bin/sqlplus /nolog
      SQL> connect SYS as SYSDBA
      SQL> startup
      SQL> quit
      ```

2. If your Infrastructure contains Identity Management, start is as follows:

   a. Start components:

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

This command starts OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and Oracle Internet Directory.

b. Start Application Server Control:

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

3.2.2 Stopping an Infrastructure

This section describes how to stop all processes in an Infrastructure. You can follow this procedure when you are preparing to shut down your host, or any other time you would like to stop your entire Infrastructure.

This procedure applies to all Infrastructure types:

- Identity Management and Metadata Repository

  Follow both steps to stop Identity Management and the Metadata Repository.

- Metadata Repository only

  Follow only the second step to stop the Metadata Repository.

- Identity Management only

  Follow only the first step to stop Identity Management.

To stop an Infrastructure:

1. If your Infrastructure contains Identity Management, stop it as follows:

   a. Stop Application Server Control:

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

   b. Stop components:

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

   This command stops OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and Oracle Internet Directory.

2. If your Infrastructure contains a Metadata Repository, stop it as follows:

   a. Set the `ORACLE_HOME` environment variable to the Infrastructure Oracle home.

b. Set the ORACLE_SID environment variable is set to the Metadata Repository SID (default is asdb).

c. Stop the Metadata Repository instance:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
SQL> quit
```

d. Stop the Net Listener:

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

3.2.3 Starting a Middle-Tier Instance

This section describes how to start all processes in a middle-tier instance. You can follow this procedure after you have rebooted your host, or any other time you would like to start up the entire instance.

This procedure applies to all middle-tier instance types:

- J2EE and Web Cache
- Portal and Wireless
- Business Intelligence and Forms

To start a middle-tier instance:

1. If the middle-tier instance uses Infrastructure services, such as Identity Management or a Metadata Repository, make sure they are started.
2. Start components:

   ```
   ORACLE_HOME/opmn/bin/opmnctl startall
   ```

   This command starts OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, Web Cache, Forms, and Reports.
3. Start the Application Server Control:

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

3.2.4 Stopping a Middle-Tier Instance

This section describes how to stop all processes in a middle-tier instance. You can follow this procedure when you are preparing to shut down your host, or any other time you would like to stop the entire instance.

This procedure applies to all middle-tier instance types:

- J2EE and Web Cache
- Portal and Wireless
- Business Intelligence and Forms

To stop a middle-tier instance:

1. Stop Application Server Control:

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

2. Stop components:

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

   This command stops OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, Web Cache, Forms, and Reports.

3.3 Starting and Stopping Components

You can use the following tools to start, stop, restart, and view the status of components:

- `opmnctl`—a command-line tool
- Application Server Control—a Web-based tool

These tools are completely compatible—they both use OPMN as their underlying technology for managing processes—and can be used interchangeably. For example, you can start a component using `opmnctl` and stop it using Application Server Control.

Although the two tools can be used interchangeably, they offer different features. The `opmnctl` command allows you to start and stop sub-processes within components, as well as the entire component. For example, you can start and stop Web Cache, or you can start and stop only the Web Cache Admin sub-process. Application Server Control allows you to view components that cannot be started or stopped, but whose status depends on other components. For example, it

displays the status of the Single Sign-On component, whose status depends on the HTTP_Server.

3.3.1 Starting and Stopping Using opmnctl

To start, stop, or restart a component:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=component
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=component
ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=component
```

To start, stop, or restart the sub-process of a component:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc process-type=process
ORACLE_HOME/opmn/bin/opmnctl startproc process-type=process
ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=process
```

To view the status of components and processes:

```
ORACLE_HOME/opmn/bin/opmnctl status
```

To learn more about using opmnctl, refer to *Oracle Process Manager and Notification Server Administrator's Guide*.

3.3.2 Starting and Stopping Using Application Server Control

You can start, stop, restart, and view status of components on the Application Server home page:

1. Navigate to the Application Server home page on Application Server Control. Scroll to the System Components section.
2. Select the checkboxes in the Select column for the components you want to start, stop, or restart.
3. Click the **Start**, **Stop**, or **Restart** button on the top right of the System Components section.

3.4 Enabling and Disabling Components

When you disable a component, you prevent it from starting when you start the application server instance, and you remove it from the list of System Components displayed on the Application Server home page.

When you enable a component, you allow it to start when you start the application server instance, and it appears in the list of System Components displayed on Application Server Control.

You can enable and disable components using Application Server Control. On the Application Server home page, click **Enable/Disable Components**. You can select which components to enable or disable. Notice that components that are dependent on each other are grouped, and are all enabled or disabled together.

Note: If you use the backup and recovery procedures documented in this book, you must run `bkp_restore.pl -m config` after you enable or disable components so the proper components are registered with the OracleAS Backup and Recovery Tool.

3.5 Starting and Stopping an Oracle Application Server Environment

This section provides procedures for starting and stopping an Oracle Application Server environment. An environment can consist of multiple Infrastructure and middle-tier instances distributed across multiple hosts. These instances are dependent on each other and it is important to start and stop them in the proper order.

You can follow these procedures when you need to completely shut down your Oracle Application Server environment. For example, when preparing to perform a complete backup of your environment, or apply a patch.

3.5.1 Starting an Oracle Application Server Environment

To start an Oracle Application Server environment from scratch:

1. **Start Metadata Repository-only Infrastructures.**

   If your environment has Infrastructure installations that contain only a Metadata Repository, start those in any order. Note that for these installation types, you only need to start the Metadata Repository. You do not need to start any processes with `opmnctl` and you do not need to start Application Server Control.

   See Also: Section 3.2.1, "Starting an Infrastructure"

2. **Start the Infrastructure that contains Identity Management.**

If your environment uses Identity Management, start the Infrastructure that contains Oracle Internet Directory. If this Infrastructure contains a Metadata Repository, start that before you start Oracle Internet Directory.

See Also: Section 3.2.1, "Starting an Infrastructure"

3. **Start OracleAS Clusters.**

   If your environment has middle-tier instances that are part of OracleAS Clusters, start the clusters in any order.

   See Also: *Oracle Application Server 10g High Availability Guide*

4. **Start middle-tier instances.**

   If your environment contains middle-tier instances that are not part of OracleAS Clusters, start them in any order.

   See Also: Section 3.2.3, "Starting a Middle-Tier Instance"

3.5.2 Stopping an Oracle Application Server Environment

To stop all processes in an Oracle Application Server environment:

1. **Stop OracleAS Clusters.**

   If your environment has middle-tier instances that are part of clusters, stop the clusters in any order.

   See Also: *Oracle Application Server 10g High Availability Guide*

2. **Stop middle-tier instances.**

   If your environment contains middle-tier instances that are not part of a cluster, stop them in any order.

   See Also: Section 3.2.4, "Stopping a Middle-Tier Instance"

3. **Stop the Infrastructure that contains Identity Management.**

   If your environment uses Identity Management, stop the Infrastructure that contains Oracle Internet Directory. If this Infrastructure contains a Metadata Repository, stop that as well.

See Also: Section 3.2.2, "Stopping an Infrastructure"

4. **Stop Metadata Repository-only Infrastructures.**

   If your environment has Infrastructure installations that contain only a Metadata Repository, stop those in any order.

   See Also: Section 3.2.2, "Stopping an Infrastructure"

3.6 Starting and Stopping: Special Topics

This section contains the following special topics about starting and stopping Oracle Application Server:

- Use opmnctl Instead of Other Command-Line Tools to Start and Stop
- Starting and Stopping Log Loader
- Starting and Stopping in High Availability Environments
- Resolving OC4J Errors When Starting Multiple Instances
- Shutting Down OracleAS Metadata Repository with the IMMEDIATE Option

3.6.1 Use opmnctl Instead of Other Command-Line Tools to Start and Stop

In Oracle9*i* Application Server Release 2 (9.0.2 and 9.0.3), `dcmctl` was the recommended command-line tool for starting and stopping Oracle HTTP Server, OC4J, and OPMN. Other command-line tools, such as `webcachectl`, were used to start the rest of the components.

In Oracle Application Server 10*g* (9.0.4), you should use `opmnctl` to start all components in your instance, with the exception of the following:

- OracleAS Certificate Authority—use `ocactl` to start and stop, refer to *Oracle Application Server Certificate Authority Administrator's Guide*.
- OracleAS Metadata Repository—use SQL*Plus to start and stop, refer to Section 3.2.1, "Starting an Infrastructure"and Section 3.2.2, "Stopping an Infrastructure".

3.6.2 Starting and Stopping Log Loader

The method for starting and stopping Oracle Application Server Log Loader is different from other components.

Log Loader is not started when you issue the `opmnctl startall` command or when you perform a **Start All** operation in Application Server Control. You can start Log Loader in the following ways:

- Using the following command:

  ```
  ORACLE_HOME/opmn/bin/opmnctl startproc ias-component-LogLoader
  ```

- By clicking the **Start** button on the Log Loader pager in Application Server Control. Refer to Section 4.5.1, "Starting and Stopping Log Loader" for instructions.

Log Loader is not stopped when you issue a **Stop All** operation in Application Server Control. You can stop Log Loader in the following ways:

- Using the following command:

  ```
  ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component-LogLoader
  ```

- By clicking the **Stop** button on the Log Loader pager in Application Server Control. Refer to Section 4.5.1, "Starting and Stopping Log Loader" for instructions.
- When stopping all components with the following command:

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

3.6.3 Starting and Stopping in High Availability Environments

The following high availability solutions require special procedures for starting and stopping:

- Oracle Application Server Cold Failover Cluster
- Oracle Application Server Active Failover Cluster (Limited Release)

See Also: *Oracle Application Server 10g High Availability Guide*

3.6.4 Resolving OC4J Errors When Starting Multiple Instances

If you have multiple Oracle Application Server installations on one host and you start them at the same time (for example, to start a cluster), OPMN may return an error like the following:

```
<process-type id="my_OC4J_instance">
  <process-set id="default_island">
    <process id="93388820" pid="24711" status="Stopped" index="1"
```

```
log="/disk1/oracleas/opmn/logs/OC4J~my_OC4J_instance~default_island~1"
operation="request" result="failure">
      <msg code="-21" text="failed to restart a managed process after the
maximum retry limit">
      </msg>
```

This error indicates that an OC4J instance (`my_OC4J_instance`) failed to start. The problem could be due to the fact that two different Oracle homes on the same host use the same port ranges for RMI, JMS, and AJP ports, and an OC4J instance in one Oracle home is trying to use the same port as an OC4J instance in another Oracle home.

For example, assume you have two Oracle Application Server installations on one host that reside in `ORACLE_HOME1` and `ORACLE_HOME2`. Each installation contains one or more OC4J instances, and each OC4J instance is assigned a port range for AJP, RMI, and JMS ports.

You can check OC4J port range assignments by examining the `opmn.xml` file in both Oracle homes:

ORACLE_HOME1`/opmn/conf/opmn.xml`
ORACLE_HOME2`/opmn/conf/opmn.xml`

In each file, locate the OC4J instance entries, which start with a line like the following:

```
<process-type id="home" module-id="OC4J" ... >
```

Within each entry, locate the RMI, JMS, and AJP port ranges, which looks like this:

```
<port id="ajp" range="3301-3400"/>
<port id="rmi" range="3201-3300"/>
<port id="jms" range="3701-3800"/>
```

Table 3–1 illustrates the problem of having the same OC4J port assignments in two Oracle homes—the AJP, RMI, and JMS port ranges in `ORACLE_HOME1` are identical to the AJP, RMI, and JMS port ranges in `ORACLE_HOME2`. (Note that this example only lists the relevant lines from the `opmn.xml`.)

Table 3–1 Example of Identical Port Ranges in Two Oracle Homes

OC4J Port Ranges in *ORACLE_HOME1*/opmn/conf/opmn.xml	**OC4J Port Ranges in *ORACLE_HOME2*/opmn/conf/opmn.xml**
<ias-component id="OC4J"> ... <process-type id="home" ... > ... <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> ... </process-type> <process-type id="OC4J_SECURITY" ... > ... <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> </process-type>	<ias-component id="OC4J"> ... <process-type id="home" ... > ... <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> ... </process-type> <process-type id="OC4J_SECURITY" ... > ... <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> </process-type>

Port allocation for all OC4J instances within an Oracle Application Server instance is controlled by OPMN. So, having overlapping port ranges within a single `opmn.xml` file is not a problem. However, when two OPMNs on a host start processes at the same time, there is no coordination between them on port usage.

The algorithm OPMN uses to assign a port is:

1. Choose a port from the port range that is not currently marked as allocated to any processes managed by the OPMN in the local instance.
2. Before assigning the port, check to see if the port is in use by binding to it.
3. If the port is not in use (that is, OPMN could bind to it), then unbind and assign the port to a process (such as an OC4J instance) so it can bind to it, updating internal data structures with this assignment information.

In between the time that OPMN unbinds from the port and the assigned process binds to the port, it is possible for another process to bind to the port. This could be another OPMN on the host, or any other process that happens to try to bind to the same port number.

If your port ranges assignments are the same across Oracle homes, and you received the error shown at the beginning of this section, then what probably happened is that two OPMN processes tried to bind the same port for their OC4J instances. There is no way to eliminate this problem completely (because there is a

rare chance that a non-OPMN process could try to bind to the port at the same time) but you can reconfigure OPMN to reduce the chance of encountering it.

There are two options for addressing this problem:

- Option 1: Assign Unique Port Ranges to Each Oracle Home
- Option 2: Increase the Maximum Number of Retries for Starting OC4J Instances

Option 1: Assign Unique Port Ranges to Each Oracle Home

You can assign unique OC4J port ranges to each Oracle home, as shown in Table 3–2. Then the OPMN in `ORACLE_HOME1` and the OPMN in `ORACLE_HOME2` will not attempt to use the same port numbers when assigning OPMN ports, and will not attempt to bind to the same port.

Table 3–2 Example of Using Unique Port Ranges in Two Oracle Homes

OC4J Port Ranges in *ORACLE_HOME1*/opmn/conf/opmn.xml	**OC4J Port Ranges in *ORACLE_HOME2*/opmn/conf/opmn.xml**
<ias-component id="OC4J"> ... <process-type id="home" ... > ... <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> ... </process-type> <process-type id="OC4J_SECURITY" ... > ... <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> </process-type>	<ias-component id="OC4J"> ... <process-type id="home" ... > ... <port id="ajp" range="**4601-4700**"/> <port id="rmi" range="**4701-4800**"/> <port id="jms" range="**4801-4900**"/> ... </process-type> <process-type id="OC4J_SECURITY" ... > ... <port id="ajp" range="**4601-4700**"/> <port id="rmi" range="**4701-4800**"/> <port id="jms" range="**4801-4900**"/> </process-type>

To do this:

1. Choose unique port ranges for AJP, RMI, and JMS.
2. Edit *`ORACLE_HOME2`*`/opmn/conf/opmn.xml`.
3. For each OC4J instance in the file, change AJP, RMI, and JMS to use the new unique port ranges. For example:

```
<port id="ajp" range="4601-4700"/>
<port id="rmi" range="4701-4800"/>
```

```
<port id="jms" range="4801-4900"/>
```

4. Save and close the file.
5. Reload OPMN:

   ```
   ORACLE_HOME2/opmn/bin/opmnctl reload
   ```

Option 2: Increase the Maximum Number of Retries for Starting OC4J Instances

OPMN attempts to start processes a certain number of times before declaring failure. For process types with port ranges, if the failure to start the process is due to the process not being able bind to the assigned port number, OPMN will attempt to start the process with a different port number in the specified range. You can have identical port ranges in two Oracle homes, and increase the number of times OPMN attempts to restart a process, so eventually OPMN will choose a port that works. This does not completely eliminate the problem, because there is a chance that OPMN will not find a port that works in 10 tries, but it does reduce the chance of encountering the problem.

The parameter that controls the number of retries is "retry". The default value is 2. You can increase the parameter to a higher number, for example, 10, as shown in Table 3–3.

Table 3–3 Example of Increasing the Retry Count in Two Oracle Homes

OC4J Port Ranges in *ORACLE_HOME1*/opmn/conf/opmn.xml	**OC4J Port Ranges in *ORACLE_HOME2*/opmn/conf/opmn.xml**
<ias-component id="OC4J"> ... <process-type id="home" ... > ... <start timeout="600" retry="**10**"/> ... <restart timeout="720" retry="**10**"/> <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> ... </process-type> <process-type id="OC4J_SECURITY" ... > ... <start timeout="600" retry="**10**"/> ... <restart timeout="720" retry="**10**"/> <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> </process-type>	<ias-component id="OC4J"> ... <process-type id="home" ... > ... <start timeout="600" retry="**10**"/> ... <restart timeout="720" retry="**10**"/> <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> ... </process-type> <process-type id="OC4J_SECURITY" ... > ... <start timeout="600" retry="**10**"/> ... <restart timeout="720" retry="**10**"/> <port id="ajp" range="**3301-3400**"/> <port id="rmi" range="**3201-3300**"/> <port id="jms" range="**3701-3800**"/> </process-type>

To do this, in each Oracle home:

1. Edit *ORACLE_HOME*/opmn/conf/opmn.xml.
2. For each OC4J instance in the file, increase the retry value for start and restart. For example:

   ```
   <start timeout="600" retry="10"/>
   <restart timeout="720" retry="10"/>
   ```

3. Save and close the file.
4. Reload OPMN:

   ORACLE_HOME/opmn/bin/opmnctl reload

3.6.5 Shutting Down OracleAS Metadata Repository with the IMMEDIATE Option

If you find that the Metadata Repository instance is taking a long time to shut down, you can use the following command to force an immediate shutdown:

```
SQL> shutdown immediate
```

Immediate database shutdown proceeds with the following conditions:

- No new connections are allowed, nor are new transactions allowed to be started, after the statement is issued.
- Any uncommitted transactions are rolled back. (If long uncommitted transactions exist, this method of shutdown might not complete quickly, despite its name.)
- Oracle does not wait for users currently connected to the database to disconnect. Oracle implicitly rolls back active transactions and disconnects all connected users.

The next startup of the database will not require any instance recovery procedures.

> **See Also:** *Oracle9i Database Administrator's Guide* in the Oracle9*i* Database documentation library

Part II

Basic Administration

This part describes basic administration tasks.

It contains the following chapters:

- Managing Log Files
- Managing Ports
- Managing an OracleAS Metadata Repository

4

Managing Log Files

Oracle Application Server components generate log files containing messages that record all types of events, including startup and shutdown information, errors, warning messages, access information on HTTP requests, and additional information. This chapter describes how to view and manage log files to assist in monitoring system activity and in diagnosing system problems.

It contains the following topics:

4.1 Introduction to Oracle Application Server Logging

Oracle Enterprise Manager Application Server Control (Application Server Control) lets you list and search log files across Oracle Application Server components. You can view log files from Application Server Control pages or download a log file to your local client and view the log files using another tool.

This section covers the following topics:

- Understanding Log File Data and Naming
- Using A Log Repository
- Configuring Component Logging Options

4.1.1 Understanding Log File Data and Naming

Several Oracle Application Server components use Oracle Diagnostic Logging (ODL). Using ODL, log file naming and the format of the contents of log files conforms to an Oracle standard and the diagnostic messages are written in XML. Some Oracle Application Server components do not use ODL, and write their diagnostic messages using a component specific text format. Regardless of the format of the messages that are stored in log files, ODL or text based, you can view log files using Application Server Control, or you can download log files to your local client and view them using another tool (for example a text editor, or another file viewing utility).

This section covers the following topics:

- ODL Message Formatting and ODL Log File Naming
- Log File Messages by Component

Note: Some Oracle Application Server components do not support ODL. Other components support ODL, but do not enable ODL by default.

4.1.1.1 ODL Message Formatting and ODL Log File Naming

When Oracle Application Server components run and produce ODL messages, the messages are written to diagnostic log files using XML format. Each ODL message includes a `HEADER` element containing fields with information about the message, optionally a `CORRELATION_DATA` element containing information to assist in

correlating messages across components, and a PAYLOAD element containing the message text, including optional arguments and associated values.

Using ODL, Oracle Application Server components write diagnostic log files to a logging directory and determine the names for logging directories using a component specific naming convention.

See Also:

- Section 4.6.2, "Understanding ODL Messages and OLD Log Files"
- Section 4.4.1, "Correlating Messages Across Log Files and Components"

4.1.1.2 Log File Messages by Component

Table 4–1 lists the supported message formats for each Oracle Application Server component. Several components optionally support ODL format, where ODL is not the default format.

Table 4–1 Diagnostic Message Format By Component

Component	Default Format	ODL Support	Location
BC4J	ODL	Yes	`$ORACLE_HOME/BC4J/logs/`*`OC4J_Name`*
DCM	ODL	Yes	`$ORACLE_HOME/dcm/logs`
Discoverer	Text	No	`$ORACLE_HOME/discoverer/logs` The Discoverer Viewer is an OC4J application. The log file is named `application.log` and is found under: `$ORACLE_HOME/j2ee/OC4J_BI_FORMS`
Enterprise Manager	Text	No	`$ORACLE_HOME/sysman/log`
Forms	Text	No	`$ORACLE_HOME/j2ee/OC4J_BI_FORMS/application-deployments/forms90app/`*`island`*`/application.log`
HTTP_Server	Text	Yes	`$ORACLE_HOME/Apache/Apache/logs/error_log.`*`time`*
Log Loader	ODL	Yes	`$ORACLE_HOME/diagnostics/logs`
OC4J *instance_name*	Text	Yes	`$ORACLE_HOME/j2ee/`*`instance_name`*`/log` `$ORACLE_HOME/j2ee/`*`instance_name`*`/application-deployments/`*`application_name`*`/application.log`
OID	Text	No	`$ORACLE_HOME/ldap/log`

Table 4–1 (Cont.) Diagnostic Message Format By Component

Component	Default Format	ODL Support	Location
OPMN	Text	No	`$ORACLE_HOME/opmn/logs` `$ORACLE_HOME/opmn/logs/`*component_type*`~...`
Port Tunneling	Text	No	`$ORACLE_HOME/iaspt/logs`
Reports Server	Text	No	`$ORACLE_HOME/reports/logs`
TopLink	Text	No	The log file location is specified with the `log path` configuration option in the TopLink installation directory, as: `config/toplink.xml`
Universal Installer	Text	No	`$ORACLE_HOME/cfgtoollogs/`
Web Cache	Text	No	`$ORACLE_HOME/webcache/logs`
Wireless	Text	Yes	`$ORACLE_HOME/wireless/logs`

4.1.2 Using A Log Repository

Application Server Control supports viewing diagnostic messages from a Log Repository (a Log Repository stores error logs, but does not store access logs). A Log Repository contains diagnostic messages collected from multiple log files across components. The Oracle Application Server **Log Loader** component initializes and updates the data in a Log Repository. After the Log Loader starts, at regular intervals it stores information from diagnostic log files to the Log Repository.

Using a Log Repository consolidates Oracle Application Server log file data; this allows you to use Application Server Control to easily search and view log file data generated by multiple components. Using a Log Repository can speed up the diagnostic process and reduce the resources required to support Oracle Application Server.

Note: By default, the Log Loader is not started. Use Application Server Control to start Log Loader.

See Also: Section 4.5, "Using Oracle Application Server Log Loader"

4.1.3 Configuring Component Logging Options

Administrators configure logging options to manage and limit the logging information that Oracle Application Server components generate and save.

> **Note:** Application Server Control does not directly support configuring logging options. In many cases, to configure component logging options you need to use the Application Server Control Advanced Server Properties page to edit the values in configuration files.

The logging configuration options include:

- Specifying Log File Names and Pathnames – Most Oracle Application Server components let you specify the directory for storing diagnostic log files. Specifying the diagnostic logging directory allows Administrators to manage system and network resources.
- Limiting Log File Size – As Oracle Application Server components run and generate diagnostic messages, the size of the log files increases. Oracle Application Server components use one of several strategies to deal with log file size. Some components allow log files to keep increasing in size; in this case it is the Administrator's responsibility to monitor and cleanup the log files. Other components, including OC4J let you specify configuration options that limit how much log file data is collected and saved.
- Using Log File Archiving – Certain Oracle Application Server components let you specify configuration options to control the size of diagnostic logging directories. This lets you determine a maximum size for the directories containing a component's log files. When the maximum size is reached, older logging information is deleted before newer logging information is saved.
- Setting Component Logging Levels – Certain Oracle Application Server components, including the Oracle HTTP Server, allow Administrators to configure logging levels. By configuring logging levels, the number of messages saved to diagnostic log files can be reduced. For example, you can set the logging level so that the system only reports and saves critical messages.

> **See Also:** Oracle Application Server component documentation for information on setting logging configuration options.

4.2 Listing and Viewing Log Files With Enterprise Manager

Use Oracle Enterprise Manager Application Server Control to list log files by selecting the **Logs** link on the Application Server Control. This brings up the View Logs page.

> **See Also:** Section 4.6.1, "Using the printlogs Tool to View Log Messages" for information on a command-line tool for viewing log files

This section covers the following:

- Listing Log Files for All Components
- Listing Log Files for Selected Components
- Listing Log Files from Oracle Application Server Components Pages
- Using Log Files Advanced Search
- Viewing Log File Details and Log File Contents

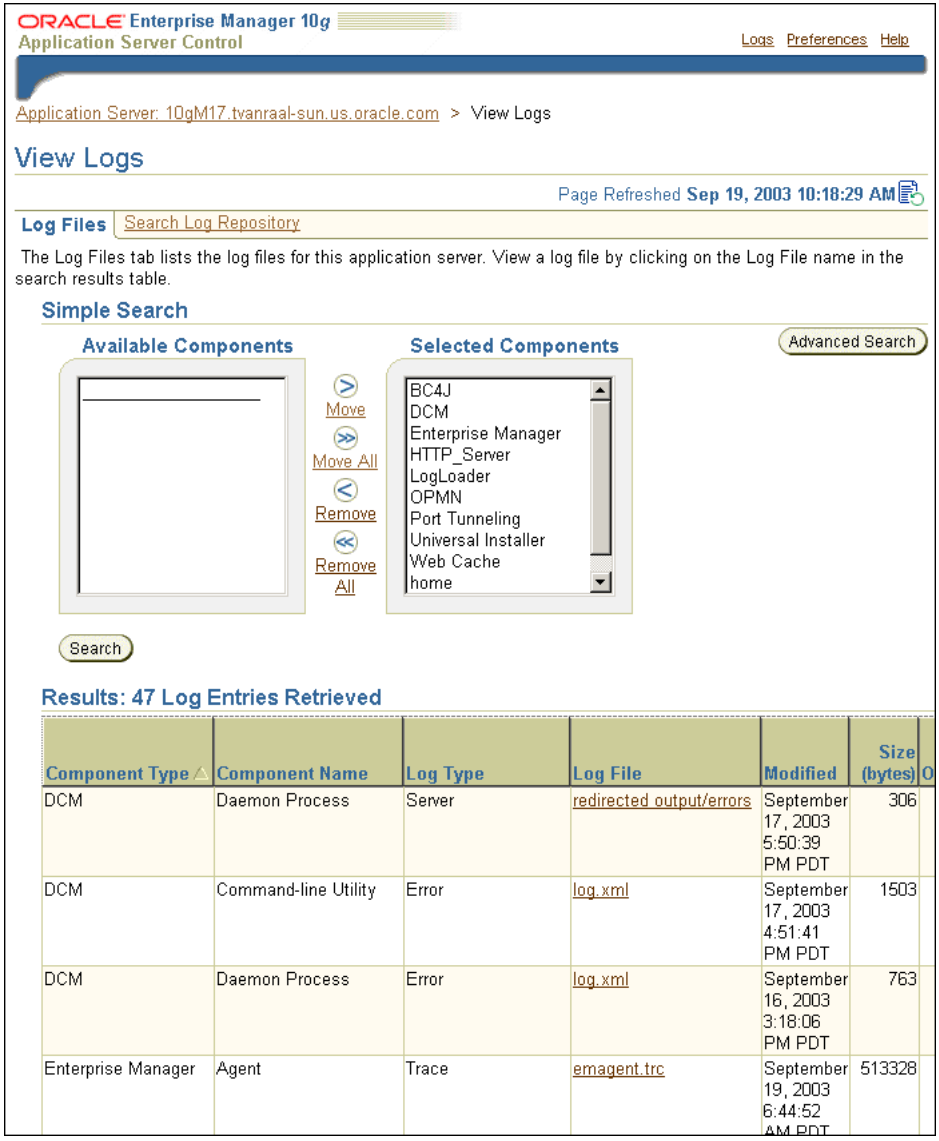
4.2.1 Listing Log Files for All Components

Selecting the **Logs** link on the Application Server Control shows the View Logs page. To list the log files, starting on the View Logs page perform the following steps:

1. Select the **Move All** button to move all available components to the **Selected Components** box.
2. Select the **Search** button to list the log files for the selected components.
3. After the search returns, the **Results** section shows log file information such as the name of the component associated with a log file and a link to the log file.

Figure 4–1 shows the Application Server Control View Logs page after a search.

Figure 4–1 Enterprise Manager View Logs Search Results



4.2.2 Listing Log Files for Selected Components

Using Application Server Control, selecting the **Logs** link shows the View Logs page. To list selected components log files, starting on the View Logs page perform the following steps:

1. Select the components whose log files you want to view from the **Available Components** box and use the **Move** button to move the selected component to the **Selected Components** box (some browsers support double clicking to move components between the boxes).
2. Select the **Search** button to list the log files for the selected components.
3. After a search returns, the Results section shows log file information such as the name of the component associated with a log file and a link to the file.

Figure 4–1 shows the View Logs page Results after a search.

4.2.3 Listing Log Files from Oracle Application Server Components Pages

After you select a system component link on the Application Server Control main page, you can view the component log files by selecting the **Logs** link. When you select this link, Application Server Control shows the View Logs page and runs a search for the component's log files. Thus, clicking on the Logs link for pages associated with a component runs a log file search for that component. You can then view the log files by selecting the Log File links shown in the **Results** section.

When you select the **Logs** link from a component page, the log file pages include a **Return to** link at the bottom of each page. The **Return to** link returns you to the component page from which you selected the **Logs** link.

4.2.4 Using Log Files Advanced Search

After selecting the **Logs** link on an Application Server Control page, the View Logs page is shown. Starting on the View Logs page, selecting the **Advanced Search** button shows the View Logs Advanced Search page. The Advanced Search page lets you list log files for Oracle Application Server components and allows you to filter the search for log files by certain log file attributes.

Starting on the View Logs Advanced Search page you can list log files using a search filter by performing the following steps:

1. Select the desired components from the **Available Components** box by using the **Move** or **Move All** buttons to move components to the **Selected**

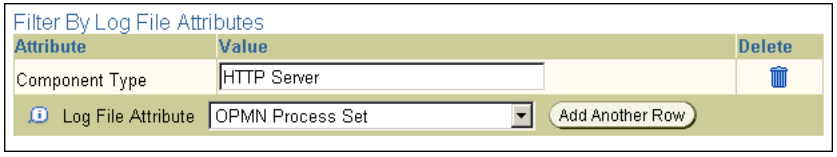
Components box (some browsers support double clicking to move components between the boxes).

2. Select a field from the **Log File Attribute** list.
3. Select the **Add Row** button to add a row for the selected log file attribute.
4. Enter the desired search value in the **Value** field.
5. If you want to select additional fields with values, select the **Add Another Row** button and enter additional values.
6. Select the **Search** button to perform the search. When the search returns, the **Results** section shows log files with matching fields.

To obtain more information on filtering using log file attributes, click the information icon next to the **Log File Attribute** list.

Figure 4–2 shows the Advanced Search Filter By Log File Attributes selection box, with the **Log File Attribute** list and the **Add Row** button.

Figure 4–2 Log Files Advanced Search Filter By Log File Attributes



4.2.5 Viewing Log File Details and Log File Contents

After selecting the **Search** button from either the View Logs Simple Search or Advanced Search page, the View Logs page shows the search output at the bottom of the page in the **Results** section. You can sort the output by selecting column headings. For example, to sort results by size, select the Size (bytes) column heading (multiple selections on a column heading toggle ascending and descending sort).

To view log file contents, select the link shown in the Log File column.

After selecting a log file link, the Log File page shows the contents of the selected log file, and supports the following:

- The Refresh list determines whether the file view is updated manually or automatically. Select **Automatically** when you want to refresh the page at regular intervals. The Log File page scrolls to the bottom when a page refreshes.

- Selecting the refresh icon next to the Page Refreshed date, on either the top or the bottom of the page, initiates manual refresh. Each refresh displays the log entries added since the last refresh.
- Selecting the **Log File** link lets you use browser features to display, print, or download the log file.

4.3 Searching Diagnostic Messages In A Log Repository

Application Server Control lets you search through diagnostic messages in a Log Repository containing messages collected from several Oracle Application Server components. The advantage of using a Log Repository is that you can search, view, and correlate diagnostic messages in a uniform way across multiple Oracle Application Server components.

This section covers the following topics:

4.3.1 Getting Started With Log Repository

To use a Log Repository for searching and viewing diagnostic messages, select the **Logs** link on a Application Server Control page and then select the **Search Log Repository** link. The Search Log Repository Simple Search and Advanced Search pages allow you to search the diagnostic messages stored in the Log Repository.

Figure 4–3 shows the Application Server Control Search Log Repository page.

The Log Repository needs to contain diagnostic messages before you can search the Log Repository. The Log Loader component initializes and updates the diagnostic messages in the Log Repository.

Note: By default, the Oracle Application Server Log Loader is not started and does not load diagnostic messages.

See Also: Section 4.5, "Using Oracle Application Server Log Loader" for information on starting and using Log Loader

4.3.2 Searching Log Repository With Simple Search

To search the Log Repository for diagnostic messages, go to the View Logs > Search Log Repository page, and use the **Available Components** and **Selected Components** boxes to select components. The online help describes the available search and display options for the View Logs > Search Log Repository page.

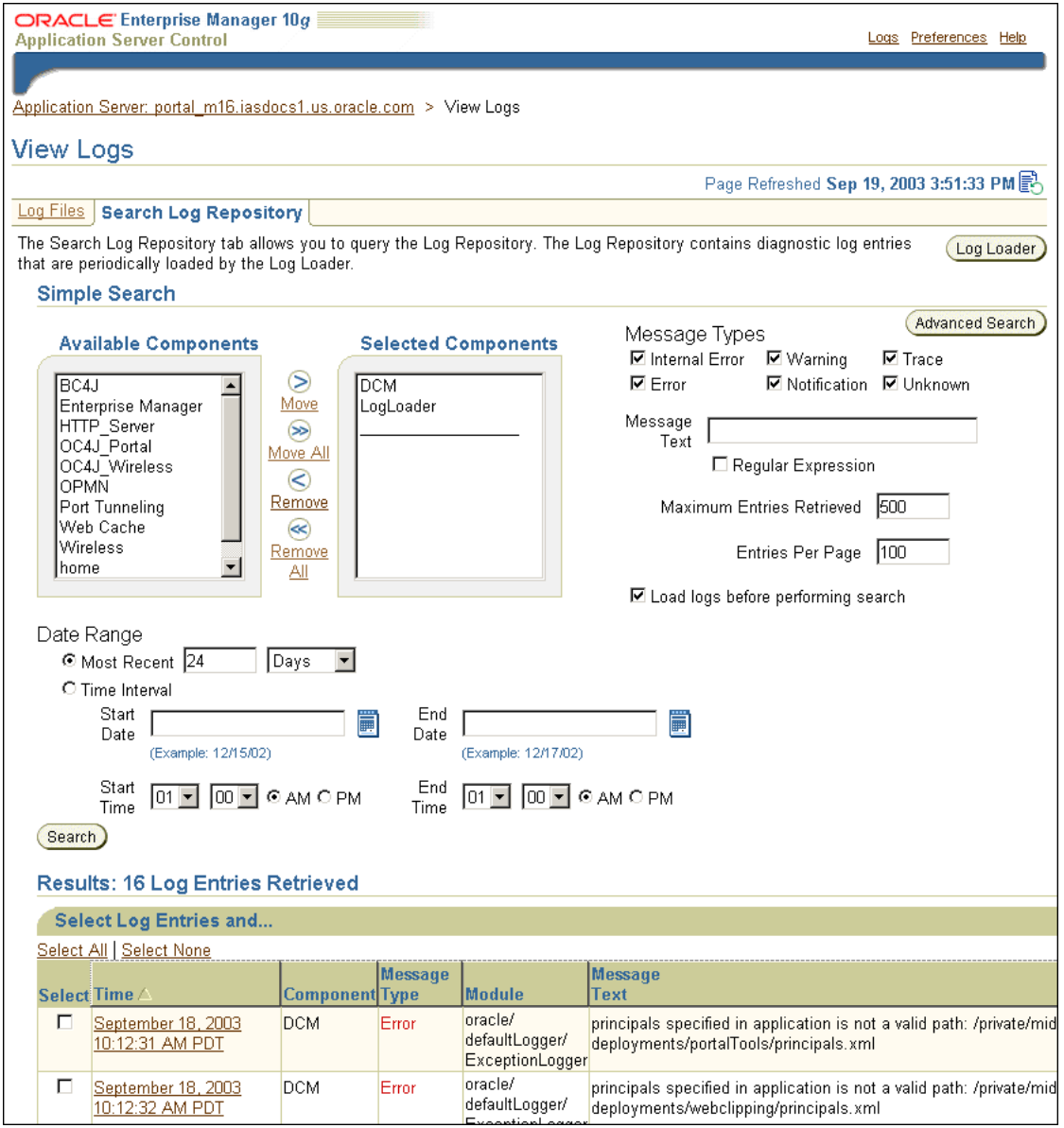
To search for diagnostic log entries in the Log Repository, do the following:

1. Select components from the **Available Components** box (optional). Select components and then use the **Move** or **Move All** button to move the selected components to the **Selected Components** box (some browsers support double clicking to move components between the boxes). This step is optional.
2. Use the default selections, or select the available search and result display options. The online help describes the available search and display options for the View Logs > Search Log Repository page.
3. Select the **Search** button to search for messages in the Log Repository that match the constraints you specify. When the search returns, the Results section shows the matching diagnostic log messages from the Log Repository.

Note: The **Message Type** selection box includes the Unknown option. Some components do not include a message type when the component writes log file entries. These messages are loaded into the Log Repository with Unknown specified as the message type.

See Also: Section 4.3.4, "Viewing Repository Log Entry Details"

Figure 4–3 Search Log Repository Page



4.3.3 Searching Log Repository With Advanced Search

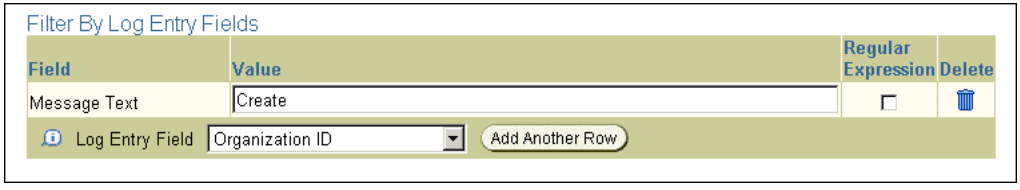
To search the Log Repository for diagnostic messages using advanced search, go to the View Logs > Search Log Repository page, and select the **Advanced Search** button. On the View Logs > Search Log Repository Advanced Search page, use the **Filter By Log Entry Fields** box to select log fields and values to search. The View Logs pages shows the diagnostic log entries with matching field values when you enter after you select the **Search** button.

Figure 4–4 shows the Advanced Search Log Repository **Filter By Log Entry Fields** box.

To display Log Repository entries matching the **Advanced Search** filter, perform the following steps:

1. Use the default selections, or specify search and result date range and message type options by making selections and entering constraints on the View Logs > Search Log Repository Advanced Search page.
2. Select log entries with specified field values using the **Filter by Log Entry Fields** box. Select multiple fields using the **Add Another Row** button. When you specify values for multiple fields, the search only returns results that match all of the specified constraints. The online help describes the available search and display options for the View Logs > Search Log Repository page.
3. Select the **Search** button to search for messages in the Log Repository that match the selection constraints. When the search returns, the Results section shows the matching log entries.

Figure 4–4 Search Log Repository Advanced Search Filter By Log Entry Fields



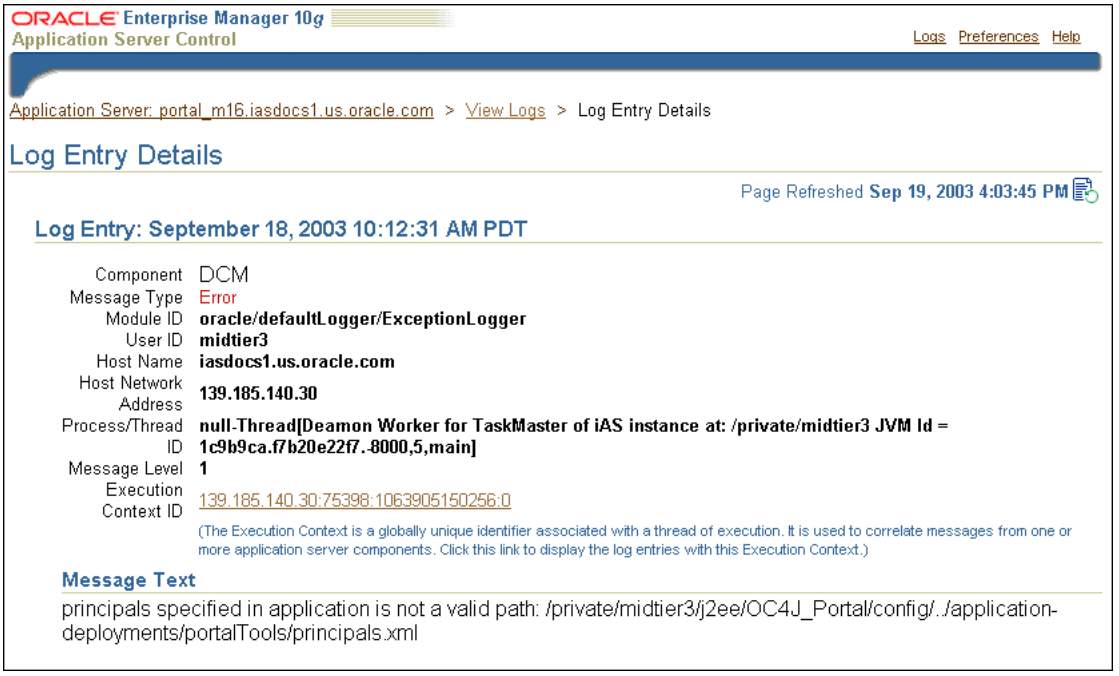
See Also: Section 4.3.4, "Viewing Repository Log Entry Details"

4.3.4 Viewing Repository Log Entry Details

Using either the link shown in the Time field of the Results area on the View Logs page, or by selecting entries in the Select field and then selecting the **View Details** button, you can view a log entry and its associated information, including the Message Type, Component, the Message Text, and optionally the Execution Context ID (ECID).

Figure 4–5 shows a log entry details page.

Figure 4–5 Log Repository Log Entry Details Page



See Also: Section 4.4, "Diagnosing Problems and Correlating Messages" for information on Execution Context IDs

4.3.5 Using Regular Expressions With Log Repository Search

Regular expression matching is applied when the checkbox in the Regular Expression field is selected on the Log Repository Simple Search or Advanced

Search page. On the Simple Search page, the Regular Expression checkbox is under the Message Text field. On the Advanced Search page, the Regular Expression checkbox is in the **Filter by Log Entry Fields** box. Using a regular expression in a search allows you to enter a pattern description that enables you to match strings for a Log Repository search.

The Log Repository search uses the Apache Jakarta regular expression engine which uses "*" for a string of characters, "?" for a single character, and supports boundary matches, including "^" for a match only at the beginning of an entry, and "$" for a match only at the end of an entry, and special characters, including "\t" for Tab, "\n" for newline, "\r" for return, and "\f" for form feed.

> **See Also:** http://jakarta.apache.org/regexp for more information on supported regular expressions

4.4 Diagnosing Problems and Correlating Messages

Generally Administrators and others view log file data to diagnose, monitor, and search for component errors or problems that may cause component errors. Application Server Control supports a unified architecture and provides cross component tools that can assist you in these tasks.

This section covers the following topics:

- Correlating Messages Across Log Files and Components
- Diagnosing Component Problems

4.4.1 Correlating Messages Across Log Files and Components

Certain Oracle Application Server components provide **message correlation** information for diagnostic messages. Message correlation information helps those viewing diagnostic messages determine relationships between messages across components. The Execution Context ID (ECID), is a globally unique identifier associated with a thread of execution. The ECID helps you to use log file entries to correlate messages from one application or across application server components. By searching related messages using the message correlation information, multiple messages can be examined and the component that first generates a problem can be identified (this technique is called **first-fault component isolation**). Message correlation data can help establish a clear path for a diagnostic message across components, within which errors and related behavior can be understood.

When you view an entry on the Log Entry Details page in Application Server Control, if the Execution Context ID field is available, it displays the Execution

Context ID as a link. Selecting the **Execution Context ID** link shows you all the messages with the same execution context ID.

You can use the ECID to track requests as they move through Oracle Application Server.

The ECID takes the following format:

```
request_id, sequence_number
```

The *request_id* is a unique integer that is associated with each request. The *sequence_number* represents the hop number of the request, as it passes through Oracle Application Server (or through the component). For example, OracleAS Web Cache assigns an initial sequence number of 0 to a request (when OracleAS Web Cache handles the request). After that, the sequence number is incremented as the request moves through Oracle Application Server components.

Table 4–2 lists the Oracle Application Server components that provide message correlation information (using an ECID).

Note: Some Oracle Application Server components do not support generating message correlation data. Other Oracle Application Server components support generating message correlation data, but by default do not enable this option.

Table 4–2 Oracle Application Server Components Supporting Message Correlation

Component	Message Correlation Configuration Reference
DCM	DCM supports message correlation.
OC4J	OC4J supports message correlation when ODL logging is enabled and when the property `oracle.dms.transtrace.ecidenabled` is set to the value `true` (by default this is `false`). This property is set on the OC4J command line. See Also: "Configuring Components to Produce ODL Messages and ECIDs" on page 4-29 *Oracle Application Server Containers for J2EE User's Guide* for details on enabling ODL logging in OC4J.

Table 4–2 (Cont.) Oracle Application Server Components Supporting Message Correlation

Component	Message Correlation Configuration Reference
HTTP Server	Oracle HTTP Server supports message correlation. See Also: Section 4.6.5, "Configuring Components to Produce ODL Messages and ECIDs"
Portal	Portal supports message correlation. Portal outputs the ECID with error messages in the Portal Repository Diagnostics log file. See Also: "Diagnosing OracleAS Portal Problems" *Oracle Application Server Portal Configuration Guide.*
Web Cache	Web Cache supports message correlation. See Also: the section, "Oracle-ECID Request-Header Field" in Chapter 2, "Caching Concepts" in the *Oracle Application Server Web Cache Administrator's Guide*

4.4.2 Diagnosing Component Problems

When an Oracle Application Server component has a problem you can isolate and determine the cause of the problem by viewing the diagnostic messages. There are general techniques that can assist you in accomplishing this task. In general, the techniques include the following:

- Search for errors, or warnings, related to the problem
- Correlate the errors across components
- Correlate the errors across a time interval
- Perform component based analysis

Using a Log Repository can make searching for the root cause of a problem much easier. A Log Repository consolidates log file data and allows you use to easily search, correlate, and view log file data that is generated by multiple Oracle Application Server components. A Log Repository correlates cross component information by time, and correlates events that occur in a cascading fashion. Once a problem is isolated to a particular component in the repository, then, if needed, the problem can be further analyzed by examining the component-specific diagnostic files.

See Also: Section 4.5, "Using Oracle Application Server Log Loader"

4.5 Using Oracle Application Server Log Loader

The Oracle Application Server **Log Loader** component works to place messages in the Log Repository. A Log Repository stores diagnostic messages from multiple log files across Oracle Application Server components. After the Log Loader starts, at regular intervals it reads the contents of log files incrementally and stores the contents to the Log Repository.

This section covers the following topics:

- Starting and Stopping Log Loader
- Enabling and Disabling Log Loader
- Updating the Log Configuration
- Setting Log Loader Properties
- Understanding Log Loader Diagnostic Messages

4.5.1 Starting and Stopping Log Loader

You can use the controls on the Application Server Control Log Loader page to start and stop the Log Loader. Starting the Log Loader starts the Oracle Application Server component that periodically updates the Log Repository. Stopping the Log Loader stops the Oracle Application Server component that periodically updates the Log Repository.

Note: By default, when Oracle Application Server is installed, the Log Loader is stopped.

To start the log loader, perform the following steps:

1. Select the Logs link on any Application Server Control page.
2. From the View Logs page select the Search Log Repository link.
3. Select the **Log Loader** button on the view logs page.
4. On the Log Loader page, select the **Start** button.
5. After selecting the **Start** button, on the confirmation page select either, **Cancel**, **Start**, or **Start and Load Existing Logs**. Use the **Cancel** button on this page to cancel, use the **Start** button to start the Log Loader, and use the **Start and Load Existing Logs** button to start and initialize the log repository with the existing

log messages (using **Start and Load Existing Logs** is usually recommended, since this operation may be faster than simply starting the Log Loader).

> **See Also:** Section 4.3, "Searching Diagnostic Messages In A Log Repository"

4.5.2 Enabling and Disabling Log Loader

On the Log Loader page, the **Enable** button enables the Log Loader. By default, when you first install Oracle Application Server, the Log Loader is enabled. Disabling the Log Loader specifies that the Log Loader's own log files are not shown in the component lists on the View logs page.

4.5.3 Updating the Log Configuration

When the Log Loader starts, it loads configuration information about the component log files to use as source for the diagnostic messages that are stored in the Log Repository (this includes information on the location and format of the log files). If the instance is reconfigured after the Log Loader is started, for example when a new component is added, use the **Update Log Configuration** button to update the Log Loader configuration. Updating the log configuration lets the Log Loader reread configuration files to locate and load all the component log files into the Log Repository.

> **See Also:** Section 4.6.4, "Component Diagnostic Log File Registration"

4.5.4 Setting Log Loader Properties

You can set Log Loader properties from the Log Loader page. To navigate to the Log Loader page:

1. Select the Logs link on any Application Server Control page.
2. From the View Logs page select the Search Log Repository link.
3. Select the **Log Loader** button on the view logs page.
4. Select the Log Loader Properties link in the Administration section.The Log Loader Properties page includes fields showing the current values for the Log Loader properties.

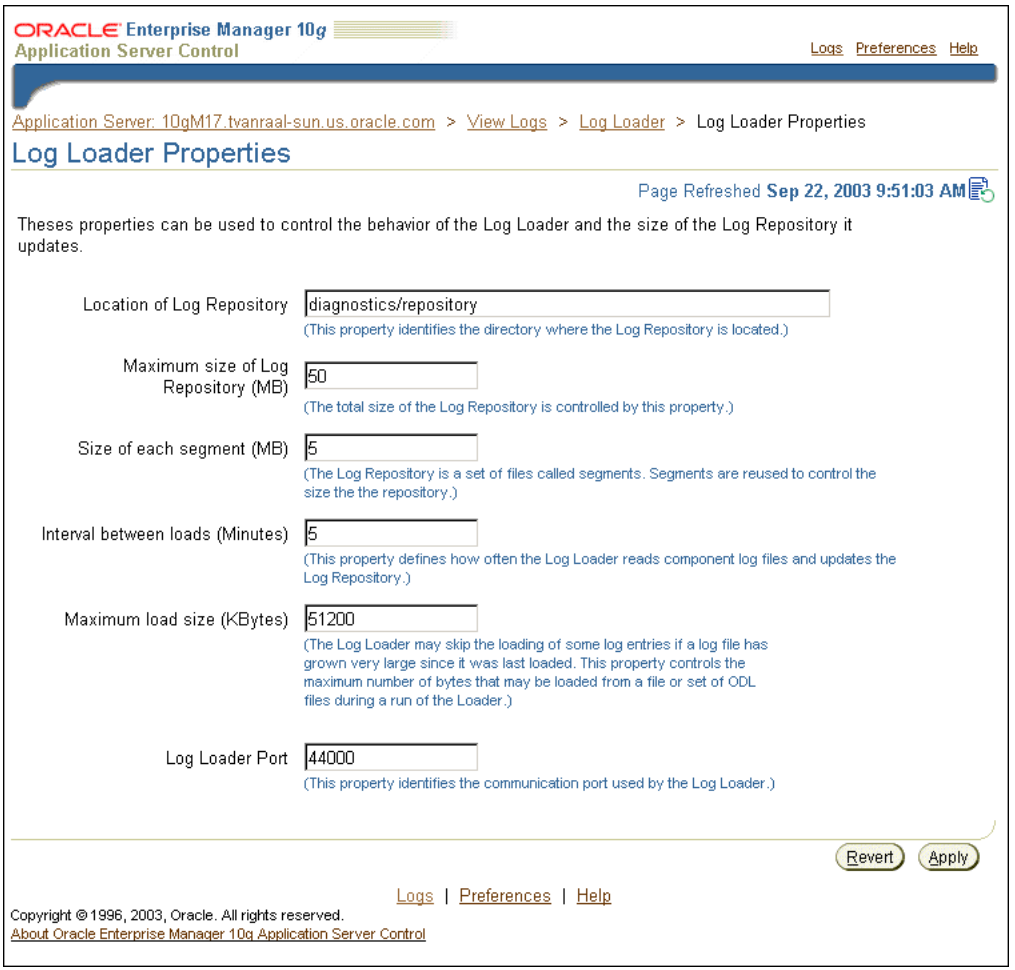
To change the Log Loader properties, perform the following steps:

1. Enter updated values in the appropriate fields on the Log Loader Properties page.
2. Select the **Apply** button to apply the new values.

Figure 4–6 shows the Application Server Control Log Loader Properties page.

The Application Server Control online help includes detailed information on the Log Loader Properties fields.

Figure 4–6 Log Loader Properties Page



4.5.5 Understanding Log Loader Diagnostic Messages

The Log Loader logs its diagnostic messages, including errors to its log file. Diagnostic messages might include errors encountered due to an incorrect configuration, or errors that occur while the Log Loader is reading data from a log file or is writing data to the log repository.

The common Log Loader problems include:

1. Errors in the Log Loader configuration file (`$ORACLE_HOME/diagnostics/config/logloader.xml`). Errors in the configuration file usually prevent the Log Loader from running. Such errors need to be corrected before the Log Loader can work properly.
2. Configuration errors that occur when a component's registration file contains errors (`$ORACLE_HOME/diagnostics/config/registration/*.xml`). Errors in the registration files do not prevent the Log Loader from running but may prevent the contents of certain log files from being loaded in the repository. Typically, there are two common types of registration file errors:
   a. XML syntax errors that prevent the file from being parsed. If such errors are encountered, the Log Loader completely ignores the contents of the file.
   b. A wrong path specified for a configuration file. If the Log Loader cannot find a log file at the specified path, it issues a Warning level diagnostic message. This does not always indicate an error, for example, it is possible that the component that generates that log was not active when the Log Loader started and the log file had not been created yet. The Log Loader continues to look for the log file and starts reading messages when the log file is created.
3. Errors may occur while the Log Loader is reading messages from a log file. If the log file includes contents that cannot be read or parsed, then the Log Loader issues a log message indicating that it cannot read part of the contents of the file. In this case, the Log Loader attempts to recover from the error and continue to read the Log File.
4. Errors may occur when writing messages to the repository (for example, a disk error). This type of error may indicate a problem that may require attention from the system administrator to correct the problem.
5. The Log Loader produces an error message when it skips reading log files because a log file exceeds the currently specified maximum load size. The maximum load size can be specified on the Log Loader properties page.

   In this case the Log Loader logs an error message in the following format:

```
Size of data to be read from log /logfile exceeds threshold of x bytes.
Skipping y_skipped bytes and moving to end of log.
```

This message indicates the size of data to be read exceeds the specified maximum load size *x*, and that the Log Loader is skipping to the end of the log file. The error message provides information on the name of the log file */logfile*, and the number of bytes skipped *y_skipped*.

4.6 Advanced Logging Topics

This section covers the following topics:

- Using the printlogs Tool to View Log Messages
- Understanding ODL Messages and OLD Log Files
- Understanding Log Loader Log File Format Conversion
- Component Diagnostic Log File Registration
- Configuring Components to Produce ODL Messages and ECIDs

4.6.1 Using the printlogs Tool to View Log Messages

The `printlogs` tool is a command-line alternative to Application Server Control for viewing log messages. `printlogs` supports a variety of options for gathering and filtering log messages, and prints the results to standard output in a single format. For example, you can use `printlogs` to:

- Read log messages from the Log Repository or individual log files
- Filter log messages according to timestamp or log field value
- Print log messages in ODL or text format
- Sort log messages by field
- Report the number of log messages of a specified type
- Run in a continuous loop, printing log reports and sleeping for a specified amount of time

> **See Also:** Appendix E, "printlogs Tool Syntax and Usage" for more information

4.6.2 Understanding ODL Messages and OLD Log Files

This section covers the following topics:

- ODL Message Contents
- ODL Log File Naming

4.6.2.1 ODL Message Contents

Using ODL, diagnostic messages are written to log files using XML format and each message includes a HEADER element containing information about the message, optionally a CORRELATION_DATA element containing information to assist in correlating messages across components, and a PAYLOAD element containing the message text including optional arguments and associated values.

Table 4–3 describes the contents of an ODL message header. Table 4–3 includes the optional header fields. For any given component that produces ODL format messages, the optional header fields may not be present in the generated diagnostic messages.

Example 4–1 shows a sample ODL format message that includes the optional CORRELATION_DATA element.

Example 4–1 Sample ODL Message Content

```
MESSAGE>
  <HEADER>
    <TSTZ_ORIGINATING>2002-04-01T18:38:48.058-08:00</TSTZ_ORIGINATING>
    <ORG_ID>oracle.com</ORG_ID>
    <COMPONENT_ID>OHS</COMPONENT_ID>
    <HOSTING_CLIENT_ID>0.0.255.255</HOSTING_CLIENT_ID>
    <MSG_TYPE TYPE="ERROR"></MSG_TYPE>
    <MSG_LEVEL>17</MSG_LEVEL>
    <HOST_ID>test-perf9</HOST_ID>
    <HOST_NWADDR>0.0.255.255</HOST_NWADDR>
    <MODULE_ID>apache_core</MODULE_ID>
    <PROCESS_ID>5713</PROCESS_ID>
  </HEADER>
  <CORRELATION_DATA>
    <EXEC_CONTEXT_ID>
      <UNIQUE_ID>1017715128:255..255.255.88:5713:0:1</UNIQUE_ID>
      <SEQ>1</SEQ>
    </EXEC_CONTEXT_ID>
  </CORRELATION_DATA>
  <PAYLOAD>
```

```
    <MSG_TEXT>File does not exist:
/files/Apache/docs/images/java-apache-project.gif
    </MSG_TEXT>
  </PAYLOAD>
</MESSAGE>
```

Table 4–3 ODL Format Message Header Fields

Header Field Name	Description	Required
COMPONENT_ID	Specifies the product or component ID for the component that originated the message.	Required
HOST_ID	Specifies the DNS host network ID.	Optional
HOST_NWADDR	Specifies the IP or other network address for the originating host.	Optional
HOSTING_CLIENT_ID	Specifies the ID of the client or security group that the message relates to.	Optional
MODULE_ID	Specifies the ID for the module that originated the message.	Optional
MSG_GROUP	Name of the group the message belongs to, for purposes of selecting similar messages.	Optional
MSG_ID	Specifies the message ID. The message ID uniquely identifies the message.	Optional
MSG_LEVEL	Specifies an integer value that qualifies the message type (MSG_TYPE). Lower level values are for higher severity errors. Valid Values: 1 - 32	Optional
MSG_TYPE	Specify the type of the message, which is one of: INTERNAL_ERROR, ERROR, WARNING, NOTIFICATION, TRACE, UNKNOWN. If MSG_TYPE is included, the TYPE attribute is required when MSG_TYPE is included in the message header.	Required
ORG_ID	Specifies the organization ID, for the originating component. This is usually the domain name for the organization.	Optional
PROCESS_ID	Specifies the process ID for the process, or execution unit associated with the message. Java components may use this field to specify the process ID and the thread ID, or only the thread ID.	Optional
TSTZ_NORMALIZED	Timestamp normalized for clock drift across hosts. This field is used when the diagnostic message is copied to a repository in a different hosts.	Optional
TSTZ_ORIGINATING	Timestamp with local timezone. This specifies the date and time when the message was generated.	Required
USER_ID	Specifies the User ID associated with the message.	Optional

4.6.2.2 ODL Log File Naming

Using ODL, Oracle Application Server components write diagnostic log files to a logging directory. Components determine the names for logging directories using a component specific naming convention.

An **ODL log** is a set of log files that includes: the current ODL log file, typically named `log.xml`, and zero or more **ODL Archives (segment files)** that contain older messages. As the log file grows, new information is added to the end of the log file, `log.xml`. Each ODL log can specify a maximum segment size. When the log file reaches the maximum segment size, it is renamed and a new log file, `log.xml` is created (specify the maximum ODL segment size using component-specific configuration options).

Note: Some Oracle Application Server components, in particular the Oracle HTTP Server, do not support the ODL log file naming mechanism that this section describes. In the Oracle HTTP Server, ODL diagnostic messages are written to a file, `log.xml`, that does not have a configurable size limit.

Segment files are created when the ODL log file `log.xml` reaches the maximum segment size. That is, the `log.xml` is renamed to `log`*n*`.xml`, where *n* is an integer, and a new `log.xml` file is created when the component generates new diagnostic messages.

To limit the size of the ODL log, components use a configuration option specifying the maximum size of the logging directory. Whenever the sum of the sizes of all of the files in the directory reaches the maximum, the oldest archive is deleted to keep the total size under the specified limit.

Note: The most recent segment file is never deleted.

For example, when the maximum directory size is reached, with the starting segment file named log9872, the following files could be present in the log file directory:

```
File                        Size

log.xml                     10002
log9872.xml                 15000
log9873.xml                 15000
log9874.xml                 15000
log9875.xml                 15000
log9876.xml                 15000
```

In this case, when log.xml fills up, log9872.xml is removed and log.xml is moved to the new file log9877.xml; new diagnostic messages then are written to a new log.xml.

Using ODL provides the following benefits:

- Limits the total amount of diagnostic information saved
- Older segment files are removed and newer segment files are saved in chronological fashion
- Components can remain active, and do not need to be shutdown, when diagnostic logging files are cleaned

4.6.3 Understanding Log Loader Log File Format Conversion

The Log Loader reads logs in several different formats and it converts the contents of non-ODL logs to ODL format. In most cases, the resulting ODL log record will contain only a timestamp and the message text from the original log entry. Values for other ODL message fields, such as COMPONENT_ID and MODULE_ID can be provided in the log registration file for each log, so that these values are set to all log records parsed from the log. The Log Loader attempts to determine the severity or level of each non-ODL log and generate an appropriate ODL message type. However, in many cases, if the severity or level cannot be determined, the resulting ODL log record will have the message type set to UNKNOWN.

The Log Loader can even read "unformatted" logs, that may not even contain timestamp values. This is the case for several logs in the $ORACLE_HOME/opmn/logs directory which contain redirected output from Oracle Application Server processes managed by Oracle Process Manager and Notification Server. When log entries do not contain a timestamp, the Log Loader

will set the timestamp to the value of the "last known timestamp" for that log. The value of the last known timestamp is determined according to the following rules:

1. The initial value of the last known timestamp is zero. Note that whenever adding a log record to the repository, a zero value timestamp will be converted to the current time.
2. If the Log Loader finds an Oracle Process Manager and Notification Server generated timestamp it will set the last known timestamp with its value.
3. When the Log Loader reaches the end of the log, it sets the last known timestamp with the current time. If the Log Loader is running regularly, such as once every five minutes, this will result in timestamps that are approximate to the actual time the message was written within a five minute range. If the Log Loader is not run frequently, the value of these timestamps could be inaccurate.

Note: The OC4J redirected logs found in the `$ORACLE_HOME/opmn/logs` directory are not treated as "unformatted" logs, since each line in the OC4J logs contains a timestamp. Most other logs in this directory are treated as unformatted logs, and will have timestamps assigned according to the preceding rules.

4.6.4 Component Diagnostic Log File Registration

Application Server Control and the Log Loader read Oracle Application Server component diagnostic registration files to determine names, locations, and additional configuration information about diagnostic log files. The directory `$ORACLE_HOME/diagnostics/config/registration` contains the diagnostic log file registration files.

Oracle Application Server components may have multiple registration files in the configuration registration directory.

The format for the registration files includes a Oracle Application Server component ID, and extension, `.xml`. Table 4–4 lists the Oracle Application Server Components and their associated Component IDs.

Note: Components are responsible for creating the component diagnostic registration files. Normally, Oracle Application Server Administrators should not modify these files.

Table 4–4 Component IDs For Diagnostic Log File Configuration

Component Name	Component ID
BC4J	BC4J
DCM	DCM
Discoverer	DISCOVER
Enterprise Manager	EM
HTTP Server	OHS
Infrastructure Database	RDBMS
Internet Directory	OID
Listener for Infrastructure Database	LISTENER
Log Loader	LOGLOADER
OC4J	OC4J
OPMN	OPMN
Port Tunneling	IASPT
Portal	PORTAL
ProcessConnect	INTEGRAT
Reports	REPORTS
Single Sign-On	SSO
TopLink	TOPLINK
Ultra Search	ULTRSRCH
Universal Installer	OUI
Web Cache	WEBCACHE
Wireless	WIRELESS

4.6.5 Configuring Components to Produce ODL Messages and ECIDs

Table 4–5 lists the Oracle Application Server components that support ODL messages but that generate text messages by default. By making configuration changes, these components can be configured to produce ODL messages and for OC4J, an ECID.

This section covers the following topics:

- Configuring Oracle HTTP Server to Produce ODL Messages
- Configuring OC4J to Produce ODL Messages
- Configuring OC4J to Produce ECIDs

See Table 4–1 for the complete list of Oracle Application Server components that produce ODL messages.

Table 4–5 Oracle Application Server Components with Configuration Options for Supporting ODL

Component	Default Format	ODL Support	Location
HTTP Server	Text	Yes	`$ORACLE_HOME/Apache/Apache/logs`
OC4J *Instance*	Text	Yes	`$ORACLE_HOME/j2ee/`*`instance_name`*`/log` `$ORACLE_HOME/j2ee/application-deployments/`*`application_name`*`/application.log`

4.6.5.1 Configuring Oracle HTTP Server to Produce ODL Messages

To configure the Oracle HTTP Server to produce ODL messages, perform the following steps:

1. Add a directory named `oracle` where the Oracle HTTP Server ODL messages will be stored. The directory should be located at the following location:

   ```
   %ORACLE_HOME/Apache/Apache/logs
   ```

2. Using Application Server Control or the `dcmctl` command line utility, modify the `httpd.conf` file to set the value of the `OraLogMode` and `OraLogSeverity` directives. Using Application Server Control, from the Administration section of the HTTP_Server page select the Advanced Server Properties link. Specify the `OraLogMode` and `OraLogSeverity` directives in `httpd.conf`.

   For example:

   ```
   OraLogMode oracle
   ```

```
OraLogSeverity NOTIFICATION
```

3. Using Application Server Control, restart the HTTP Server.

> **See Also:** *Oracle HTTP Server Administrator's Guide* for details on using the `OraLogMode` and `OraLogSeverity` directives

4.6.5.2 Configuring OC4J to Produce ODL Messages

The supplied configuration files for OC4J include commented out specifications for ODL logging. Enabling ODL logging in OC4J involves uncommenting the ODL configuration options and restarting the associated OC4J instance.

To change the ODL logging configuration for OC4J, use Application Server Control to select the Administration link for the OC4J instance that you want to enable ODL logging. Then, select the Advanced Properties link to show the Advanced Server Properties page. On this page, edit the configuration files and uncomment the lines that contain the `<odl>` element.

> **See Also:** Chapter 3, "Advanced Configuration Development, and Deployment" in *Oracle Application Server Containers for J2EE User's Guide*

4.6.5.3 Configuring OC4J to Produce ECIDs

OC4J supports generating an Execution Context ID (ECID) for its log file entries. You can use the ECID to track requests as they move through Oracle Application Server, or through OC4J. By default ECID generation is disabled in OC4J.

To enable ECID generation in OC4J, set the Java command-line option `-Doracle.dms.transtrace.ecidenabled=true`.

To modify Java command line options using Application Server Control, do the following:

1. Select the Administration link on the OC4J Home Page of the application server instance of interest.
2. Select **Server Properties** in the Instance Properties area.
3. Scroll down to the Multiple VM Configuration section. This section defines the ports and the command line options for OC4J and for the JVM that runs OC4J processes.
4. Under the Command Line Options area, add the following at the end of the Java Options text field:

```
-Doracle.dms.transtrace.ecidenabled=true
```

5. Select the **Apply** button.

Note the following when setting the `oracle.dms.transtrace.ecidenabled` property:

- The default value for `oracle.dms.transtrace.ecidenabled` is `false`.
- The property applies for the entire OC4J instance and it cannot be set to different values for different applications running on OC4J.
- When ODL is enabled for OC4J, and you specify `oracle.dms.transtrace.ecidenabled=false`, OC4J uses an ECID that is generated from within OC4J, rather than receiving the ECID from Oracle HTTP Server. When ODL is enabled for OC4J, all log messages should include an ECID.

> **See Also:** "Advanced Configuration Development, and Deployment" in *Oracle Application Server Containers for J2EE User's Guide*

4.6.6 Limitations and Configuration

The Logs link in Application Server Control gives you an integrated view of many Oracle Application Server component log files. However, certain log files are only available at the component level. Oracle Application Server components use the directory `$ORACLE_HOME/diagnostics/config/registration` to make their log files visible to Application Server Control. Some Oracle Application Server component log files are not exposed through Application Server Control pages.

5

Managing Ports

This chapter describes how to view and change Oracle Application Server port numbers. It contains the following topics:

5.1 About Managing Ports

Many Oracle Application Server components and services use ports. As an administrator, it is important to know the port numbers used by these services, and to ensure that the same port number is not used by two services on your host.

Most port numbers are assigned during installation. Every component and service has an allotted port range, which is the set of port numbers Oracle Application Server attempts to use when assigning a port. Oracle Application Server starts with the lowest number in the range and performs the following checks:

- Is the port used by another Oracle Application Server installation on the host?

  The installation may be up or down at the time; Oracle Application Server can still detect if the port is used.)

- Is the port used by a process that is currently running?

  This could be any process on the host, even a non-Oracle Application Server process.

- Is the port listed in the `/etc/services` files?

If the answer to any of the above questions is yes, Oracle Application Server moves to the next highest port in the allotted port range and continues checking until it finds a free port.

You can override this behavior for some ports, and specify a port number assignment during installation. To do this, you edit a template file called `staticports.ini`, and launch Oracle Universal Installer with special options.

> **See Also:** Appendix C, "Oracle Application Server Port Numbers" for a complete list of allotted port ranges. Refer to *Oracle Application Server 10g Installation Guide* for directions on overriding port assignments during installation with `staticports.ini`.

5.2 Viewing Port Numbers

You can view port numbers in the following ways:

- Immediately after installation, you can view port number assignments in:

  ORACLE_HOME/install/portlist.ini

  If you change a port number, it is not updated in this file, so you can only rely on this file immediately after installation.

- Another file that displays two important ports, the Application Server Control port and the HTTP Server port is:

  ORACLE_HOME/Apache/Apache/setinfo.txt

  Since the Application Server Control port number cannot be changed, this is always a good place to locate the URL for Application Server Control. However, you may change the HTTP Server port after installation, so it is not reliable for that.

- The main way to view port numbers once your installation is up and running is on the Application Server Control Ports Page. You can view the Ports Page by clicking the ports link on the Application Server home page. The Ports Page displays the current port numbers and is updated any time you change a port number. It also contains links to pages that allow you do change port numbers.

Querying the Runtime JServ Port

If you have JServ configured, you can query the runtime port used by JServ with the following URL:

http://*hostname.domain*:*http_port*/oprocmgr-status

5.3 Changing Ports Common to All Middle-Tier Instances

This section provides complete instructions for changing port numbers in middle-tier instances. The instructions explain how to change the port number, and update any other components that might be affected.

> **See Also:** Appendix C, "Oracle Application Server Port Numbers" for more information on changing port numbers

Note: You can change a port number to any number you want, as long as it is an unused port. You do not have to use a port in the allotted port range for the component.

It contains the following topics:

- Changing Oracle Enterprise Manager Ports
- Changing OC4J Ports
- Changing Oracle HTTP Server Ports
- Changing the Web Cache Non-SSL Listener Port (Middle-Tier Installations)
- Changing the Web Cache SSL Listener Port (Middle-Tier Installations)
- Changing the Web Cache Administration Port
- Changing the Web Cache Invalidation Port
- Changing the Web Cache Statistics Port
- Changing the DCM Java Object Cache Port
- Changing the Java Object Cache Port
- Changing the JServ Servlet Engine Port
- Changing the Log Loader Port
- Changing OPMN Ports (ONS Local, Request, and Remote)
- Changing the Oracle HTTP Server Diagnostic Port
- Changing the Port Tunneling Port

5.3.1 Changing Oracle Enterprise Manager Ports

You cannot change Oracle Enterprise Manager ports after installation.

See Also: Appendix C, "Oracle Application Server Port Numbers"

5.3.2 Changing OC4J Ports

This section describes how to change the following OC4J port numbers:

- AJP
- JMS

- RMI
- IIOP
- IIOPS1 (Server only)
- IIOPS2 (Server and client)

By default, Oracle Application Server does not specify a single port number for each OC4J port. Instead, it specifies a port range for each type of OC4J port and that range is the same for all instances on the host. During runtime, each instance is assigned a single free port from the range.

For example, the default AJP range for every OC4J instance on a host is 3301-3400. Each OC4J instance is assigned a single free port from that range for its AJP port.

In order to change an OC4J port number, you typically change the range of port numbers for a service, and then a free port from that range will be assigned.

You can change OC4J port numbers using Application Server Control or manual steps:

- **Using Application Server Control**
  1. Navigate to the Application Server Instance Home Page.
  2. Click **Ports**.
  3. On the Ports Page, locate the OC4J Instance and OC4J port range you would like to change. Click the icon in the Configure column.
  4. On the Server Properties Page, enter the new port range in the appropriate field. Click **Apply**.
  5. On the Confirmation page, click **Yes**, you would like to restart now.
- **Using Manual Steps**
  1. Edit the following file:

     ORACLE_HOME/opmn/conf/opmn.xml

  2. Locate the element for the OC4J instance that contains the port number you would like to change. For example, if you want to change a port number for the `home` instance, locate this element:

     ```
     <process-type id="home" ...>
     ```

  3. Within the OC4J instance element, there is a `port` element for each type of port. For example:

```
<port id="ajp" range="3301-3400"/>
<port id="rmi" range="3201-3300"/>
<port id="jms" range="3701-3800"/>
<port id="iiop" range="3401-3500"/>
<port id="iiops1" range="3501-3600"/>
<port id="iiops2" range="3601-3700"/>
```

Modify the range parameter for the port you would like to change.

4. Save and close the file.
5. Reload OPMN:

   ```
   opmnctl reload
   ```

6. Restart the OC4J instance that contains the port number you changed:

   ```
   opmnctl restartproc process-type=OC4J_instance
   ```

   For example, if you changed a port number in the home instance:

   ```
   opmnctl restartproc process-type=home
   ```

7. Run the following command:

   ```
   dcmctl updateConfig
   ```

5.3.3 Changing Oracle HTTP Server Ports

This section describes how to change the Oracle HTTP Server Listen directive on a middle-tier instance. It contains the following procedures:

- Changing the Oracle HTTP Server Non-SSL Listen Port (with Web Cache)

  Follow this procedure to change the Oracle HTTP Server Listen port on a middle-tier instance. In this procedure, you update the Oracle HTTP Server Listen directive and register the new port number with Web Cache. The Web Cache port and the Oracle HTTP Server Port directive remain unchanged.

- Changing the Oracle HTTP Server SSL Listen Port (with Web Cache)

  Follow this procedure to change the Oracle HTTP Server SSL Listen port on a middle-tier instance. In this procedure, you update the Oracle HTTP Server SSL Listen directive and register the new port number with Web Cache. The Web Cache SSL port and the Oracle HTTP Server SSL Port directive remain unchanged.

- Changing the Oracle HTTP Server Non-SSL Listen Port (No Web Cache)

Follow this procedure on a J2EE and Web Cache installation that does not have Web Cache configured. It involves changing the Listen directive and Port directive with the new port number.

- Changing the Oracle HTTP Server SSL Listen Port (No Web Cache)

  Follow this procedure on a J2EE and Web Cache installation that does not have Web Cache configured. It involves changing the SSL Listen directive and SSL Port directive with the new port number.

5.3.3.1 Changing the Oracle HTTP Server Non-SSL Listen Port (with Web Cache)

This section describes how to change the Oracle HTTP Server non-SSL listen port on an installation that has Web Cache front-ending the Oracle HTTP Server.

Step 1: Modify the Oracle HTTP Server Listen Directive

You can do this using Application Server Control or manual steps:

- **Using the Application Server Control:**

  1. Navigate to the Application Server home page and click **Ports**.
  2. On the Ports Page, locate the Oracle HTTP Server Listen port and click the icon in the Configure column.
  3. On the Server Properties Page, in the Listening Addresses and Ports section, enter the new port number in the Listening Port column. There may be more than one listening port listed. The only way to tell which is the non-SSL listening port is to choose the one with the old non-SSL listening port value.
  4. At the bottom of the page, click **Apply**.
  5. On the Confirmation Page, click **No**, you would not like to restart now.

- **Using Manual Steps:**

  1. Edit the following file:

     ORACLE_HOME/Apache/Apache/conf/httpd.conf

  2. Update the `Listen` directive with the new port number. Do not update the `Port` directive.

     There may be multiple `Listen` directives in this file. Modify the `Listen` directive that is not enclosed in an SSL virtual host container. The easiest

way to locate the proper `Listen` directive is to search the file for the old listen port number.

3. Save and close the file.
4. Run the following command:

```
dcmctl updateConfig -ct ohs
```

Step 2: Enable Oracle HTTP Server to Run as Root for Ports < 1024 on UNIX

Perform this step if you are changing the port to a number < 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Oracle Application Server non-SSL listen port number to a value less than 1024, you must enable Oracle Application Server to run as root, as follows:

1. Log in as root.
2. Run the following commands in the middle-tier Oracle home:

```
cd ORACLE_HOME/Apache/Apache/bin
chown root .apachectl
chmod 6750 .apachectl
```

Step 3: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

```
ORACLE_HOME/sysman/emd/targets.xml
```

2. Update each occurrence of the old Oracle HTTP Server listen port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Oracle HTTP Server listen port, or it may contain many occurrences. The listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Oracle HTTP Server listen port number, and replace them with the new port number. Be sure to update only the Oracle HTTP Server listen port; do not update the Web Cache listener port or any other port numbers.
3. Save and close the file.
4. Reload Application Server Control:

```
ORACLE_HOME/bin/emctl reload
```

Step 4: Update OracleAS Web Cache

1. Using Application Server Control, navigate to the Web Cache home page.
2. In the Administration section, click Web Cache Administration. Log in to Web Cache Administrator.
3. In the navigator frame, select Origin Servers, Sites, and Load Balancing > Origin Servers. The Origin Servers page appears.
4. Select the Oracle HTTP Server port that has HTTP in the Protocol column. Click **Edit Selected**.
5. Enter the new port number in the Port field. Click **Submit**.
6. Click Apply Changes.

Step 5: Restart the Middle-Tier Instance

Restart the middle-tier instance:

```
opmnctl stopall
opmnctl startall
```

5.3.3.2 Changing the Oracle HTTP Server SSL Listen Port (with Web Cache)

This section describes how to change the Oracle HTTP Server non-SSL listen port on an installation that has Web Cache front-ending the Oracle HTTP Server.

Step 1: Modify the Oracle HTTP Server Listen Directive

1. Edit the following file:

   ORACLE_HOME/Apache/Apache/conf/ssl.conf

2. Update the `Listen` directive with the new port number. Do not update the `Port` directive.
3. Save and close the file.
4. Run the following command:

   ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct ohs

Step 2: Enable Oracle HTTP Server to Run as Root for Ports < 1024 on UNIX

Perform this step if you are changing the port to a number < 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Oracle Application

Server SSL listen port number to a value less than 1024, you must enable Oracle Application Server to run as root, as follows:

1. Log in as root.
2. Run the following commands in the middle-tier Oracle home:

```
cd ORACLE_HOME/Apache/Apache/bin
chown root .apachectl
chmod 6750 .apachectl
```

Step 3: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

   ```
   ORACLE_HOME/sysman/emd/targets.xml
   ```

2. Update each occurrence of the old Oracle HTTP Server SSL listen port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Oracle HTTP Server SSL listen port, or it may contain many occurrences. The listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Oracle HTTP Server SSL listen port number, and replace them with the new port number. Be sure to update only the Oracle HTTP Server SSL listen port; do not update the Oracle HTTP Server non-SSL listen port, the Web Cache listener port, or any other port numbers.

3. Save and close the file.
4. Reload the Application Server Control:

   ```
   ORACLE_HOME/bin/emctl reload
   ```

Step 4: Update OracleAS Web Cache

1. Using Application Server Control, navigate to the Web Cache home page.
2. In the Administration section, click Web Cache Administration. Log in to Web Cache Administrator.
3. In the navigator frame, select Origin Servers, Sites, and Load Balancing > Origin Servers.
4. The Origin Servers page appears.

5. Select the Oracle HTTP Server port that has HTTPS in the Protocol column.Click **Edit Selected**.
6. Enter the new port number in the Port field. Click **Submit**.
7. Click Apply Changes.

Step 5: Restart the Middle-Tier Instance

Restart the middle-tier instance:

```
opmnctl stopall
opmnctl startall
```

5.3.3.3 Changing the Oracle HTTP Server Non-SSL Listen Port (No Web Cache)

This section describes how to change the Oracle HTTP Server non-SSL listen port on an installation that does not have Web Cache front-ending the Oracle HTTP Server.

Step 1: Modify the Oracle HTTP Server Listen and Port Directives

You can do this using Application Server Control or manual steps:

- **Using the Application Server Control:**
  1. Navigate to the instance home page and click **Ports**.
  2. On the Ports Page, locate the Oracle HTTP Server Listen port and click the icon in the Configure column.
  3. On the Server Properties Page:
     * Enter the new port number in the Default Port field. This is for the `Port` directive.
     * Enter the new port number in the Listening Port column. This is for the `Listen` directive. There may be more than one listening port listed. The only way to tell which is the non-SSL listen port is to choose the one with the old non-SSL listen port value.
  4. At the bottom of the page, click **Apply**.
  5. On the Confirmation Page, click **No**, you would not like to restart now.
- **Using Manual Steps:**
  1. Edit the following file:

     ORACLE_HOME/Apache/Apache/conf/httpd.conf

2. Update the non-SSL `Listen` and `Port` directives with the new port number. The value for `Listen` and `Port` must be the same port number, for example, to change the listener port to `7779`:

   ```
   Listen 7779
   Port 7779
   ```

   There may be multiple `Listen` and `Port` directives in this file. Modify the `Listen` and `Port` directives that are not enclosed in an SSL virtual host container. The easiest way to locate the proper `Listen` and `Port` directives is to search the file for the old listen port number.

3. Save and close the file.

4. Run the following command:

   ```
   dcmctl updateConfig -ct ohs
   ```

Step 2: Enable Oracle HTTP Server to Run as Root for Ports < 1024 on UNIX

Perform this step if you are changing the port to a number < 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Oracle Application Server non-SSL listen port number to a value less than 1024, you must enable Oracle Application Server to run as root, as follows:

1. Log in as root.

2. Run the following commands in the middle-tier Oracle home:

   ```
   cd ORACLE_HOME/Apache/Apache/bin
   chown root .apachectl
   chmod 6750 .apachectl
   ```

Step 3: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

   ```
   ORACLE_HOME/sysman/emd/targets.xml
   ```

2. Update each occurrence of the old Oracle HTTP Server listen port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Oracle HTTP Server listen port, or it may contain many occurrences. The

listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Oracle HTTP Server listen port number, and replace them with the new port number.

3. Save and close the file.
4. Reload the Application Server Control:

   ```
   ORACLE_HOME/bin/emctl reload
   ```

Step 4: Re-register mod_osso

If you are using Single Sign-On, re-register `mod_osso` with the new port number:

1. Make sure the `LD_LIBRARY_PATH` environment variable contains `$ORACLE_HOME/lib`.
2. Re-register mod_osso with the new port number by running the following command in the middle-tier Oracle home:

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
   -oracle_home_path middle_tier_oracle_home
   -site_name middle_tier_hostname:new_http_port_number
   -config_mod_osso TRUE
   -mod_osso_url mod_osso_url
   -u user
   ```

   Note that *user* is the user that starts Oracle HTTP Server. By default, this is the user that installed Oracle Application Server. If you have changed the Oracle HTTP Server listen port number to a value < 1024, then this user is root.

   For example, if you want to change the Oracle HTTP Server listen port to 7779 on middle-tier host `myhost`:

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
   -oracle_home_path /disk1/oracleas
   -site_name myhost:7779
   -mod_osso_url http://myhost.mydomain:7779
   -u oracle
   ```

   See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering mod_osso.

Step 5: Restart the Middle-Tier Instance

Restart the middle-tier instance:

```
opmnctl stopall
```

```
opmnctl startall
```

5.3.3.4 Changing the Oracle HTTP Server SSL Listen Port (No Web Cache)

This section describes how to change the Oracle HTTP Server SSL listen port on an installation that has Web Cache front-ending the Oracle HTTP Server.

Step 1: Modify the Oracle HTTP Server Listen and Port directives

1. Edit the following file:

   ORACLE_HOME/Apache/Apache/conf/ssl.conf

2. Update the `Listen` and `Port` directives with the new port number. The value for `Listen` and `Port` must be the same port number, for example, to change the listener port to `4445`:

   ```
   Listen 4445
   Port 4445
   ```

3. Save and close the file.
4. Run the following command:

   ```
   dcmctl updateConfig -ct ohs
   ```

Step 2: Enable Oracle HTTP Server to Run as Root for Ports < 1024 on UNIX

Perform this step if you are changing the port to a number < 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Oracle Application Server SSL listen port number to a value less than 1024, you must enable Oracle Application Server to run as root, as follows:

1. Log in as root.
2. Run the following commands in the middle-tier Oracle home:

   ```
   cd ORACLE_HOME/Apache/Apache/bin
   chown root .apachectl
   chmod 6750 .apachectl
   ```

Step 3: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

   ORACLE_HOME/sysman/emd/targets.xml

2. Update each occurrence of the old Oracle HTTP Server SSL listen port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Oracle HTTP Server SSL listen port, or it may contain many occurrences. The listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Oracle HTTP Server SSL listen port number, and replace them with the new port number. Be sure to update only the Oracle HTTP Server SSL listen port; do not update the Oracle HTTP Server non-SSL listen port or any other port numbers.

3. Save and close the file.

4. Reload the Application Server Control:

   ```
   ORACLE_HOME/bin/emctl reload
   ```

Step 4: Re-register mod_osso

If you have registered your SSL virtual host as an SSO partner application, follow these steps to re-register your SSL virtual host:

1. Make sure the `LD_LIBRARY_PATH` environment variable contains `$ORACLE_HOME/lib`.

2. Re-register your SSL virtual host with the new port number by running the following command in the middle-tier Oracle home:

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
   -oracle_home_path middle_tier_oracle_home
   -site_name middle_tier_hostname:new_https_port_number
   -config_mod_osso TRUE
   -mod_osso_url mod_osso_url
   -virtualhost -u user
   ```

   Note that *user* is the user that starts Oracle HTTP Server. By default, this is the user that installed Oracle Application Server. If you have changed the Oracle HTTP Server listen port number to a value < 1024, then this user is root.

   For example, if you want to change the Oracle HTTP Server SSL listen port to 4445 on middle-tier host `myhost`:

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
   -oracle_home_path /disk1/oracleas
   -site_name myhost:4445
   -config_mod_osso TRUE
   ```

```
-mod_osso_url https://myhost.mydomain:4445
-virtualhost -u oracle
```

See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering `mod_osso`

Step 5: Restart the Middle-Tier Instance

Restart the middle-tier instance:

```
opmnctl stopall
opmnctl startall
```

5.3.4 Changing the Web Cache Non-SSL Listener Port (Middle-Tier Installations)

This section describes how to change the Web Cache non-SSL listener port. It involves changing the Web Cache port number and updating other components in the middle tier with the new port number.

Step 1: Change the Web Cache Non-SSL Listener Port

1. Using the Application Server Control, navigate to the Web Cache home page.
2. In the Administration section, click Web Cache Administration. Log in to Web Cache Administrator.
3. In the navigator frame, select Ports > Listen Ports. The Listen Ports page appears.
4. Select the port appropriate port that has HTTP in the Protocol column. Click **Edit Selected**.
5. Enter the new port number in the Port field. Click **Submit**.
6. Click **Apply Changes**. It is not necessary to restart Web Cache at this time since you are going to restart the entire instance at the end of this procedure.

Step 2: Change the Web Cache Logical Site Port

If the Web Cache non-SSL listener port is the same as the logical site port, update the logical site port as follows:

1. In Web Cache Manager, in the navigator frame, select Origin Servers, Sites, and Load Balancing > Site Definitions.
2. On the Site Definitions page, locate the appropriate site using the old port number. If there is no site using the old port number, then the Web Cache listener and site do not share the same port number. Skip to Step 3: Enable Web Cache to Run as Root for Ports < 1024 on UNIX.
3. Select the appropriate site with the old port number. Click **Edit Site**.
4. In the Edit Site dialog box, enter the new port number. Click **Submit**.
5. In the navigator frame, select Origin Servers, Sites, and Load Balancing > Site-to-Server Mapping.
6. On the Site-to-Server Mapping page, you may see one or more mappings using the old port number. For each site:
   a. Select the site and click **Edit Selected**.

b. In the Edit / Add Site-to-Server Mapping dialog box, change the Port Number field to the new port number. **Click Submit**.

7. Click **Apply Changes**.

Step 3: Enable Web Cache to Run as Root for Ports < 1024 on UNIX

Perform this step if you are changing the port to a number < 1024.

By default, Web Cache runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Web Cache non-SSL listener port number to a value less than 1024, you must enable Web Cache to run as root, as follows:

1. Log in as the user that installed Oracle Application Server and stop Web Cache:

   ```
   opmnctl stopproc ias-component=WebCache
   ```

2. Log in as root.

3. Run the following command in the middle-tier Oracle home:

   ORACLE_HOME/webcache/bin/webcache_setuser.sh setroot *userID*

   Where *userid* is the current user Web Cache is running under. This is usually the user that installed Oracle Application Server. This user is listed on the Process Identity screen in Web Cache Manager.

4. Log in as the user that installed Oracle Application Server and start Web Cache:

   ```
   opmnctl startproc ias-component=WebCache
   ```

Step 4: Update the Oracle HTTP Server Port directive

1. Edit the following file:

   ORACLE_HOME/Apache/Apache/conf/httpd.conf

2. Update the `Port` directive with the new port number. Do not modify the `Listen` directive. The Web Cache port must equal the Oracle HTTP Server Port directive.

3. Save the file.

4. Run the following command:

   ```
   dcmctl updateConfig -ct ohs
   ```

Step 5: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

   ORACLE_HOME/sysman/emd/targets.xml

2. Update each occurrence of the old Web Cache listener port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Web Cache listener port, or it may contain many occurrences. The listener port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Web Cache listener port number, and replace them with the new port number.

3. Save and close the file.

4. Reload the Application Server Control:

   ORACLE_HOME/bin/emctl reload

Step 6: Update mod_osso

1. Make sure the LD_LIBRARY_PATH environment variable contains $ORACLE_HOME/lib.

2. Re-register mod_osso with the new port number by running the following command in the middle-tier Oracle home:

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
   -oracle_home_path middle_tier_oracle_home
   -site_name middle_tier_hostname:new_http_port_number
   -config_mod_osso TRUE
   -mod_osso_url mod_osso_url
   -u user
   ```

   Note that *user* is the user that starts Oracle HTTP Server. By default, this is the user that installed Oracle Application Server. If you have changed the Oracle HTTP Server listen port number to a value < 1024, then this user is root.

   For example, if you want to change the Web Cache listener port to 7779 on middle-tier host myhost:

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
   -oracle_home_path /disk1/oracleas
   -site_name myhost:7779
   -config_mod_osso TRUE
   ```

```
-mod_osso_url http://myhost.mydomain:7779
-u oracle
```

See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering `mod_osso`

Step 7: Update OracleAS Portal

If you have OracleAS Portal configured, update Portal with the new listener port number.

1. Using the Application Server Control, navigate to the Portal home page.
2. In the Administration section, click Portal Web Cache Settings.
   - If Listening Port SSL Enabled is set to No, update the Listening Port field with the new port number. Click **OK**.
   - If Listening Port SSL Enabled is set to Yes, you do not need to update anything on this page. Click **Cancel**.

Step 8: Update Web Providers with OracleAS Portal

If you are using Web Providers with OracleAS Portal, you must update them as follows (note that locally hosted Web Providers run on the same middle-tier instance as OracleAS Portal):

1. Log in to OracleAS Portal as the administrator (for example, PORTAL).
2. Click the Administrator tab.
3. Click the Portlets sub-tab.
4. Repeat this step for all locally hosted Web Providers registered in your Portal:
   a. In the Remote Providers portlet, enter the provider name (for example, WEBCLIPPING) in the Name field. Click Edit.
   b. Click the Connection tab.
   c. In the URL field, update the port to the new port number. Click OK.

Step 9: Update OracleAS Wireless

If you have OracleAS Wireless configured, update Wireless with the new port number:

1. Re-register Wireless with SSO by running the following command on the middle-tier host:

```
ORACLE_HOME/wireless/bin/reRegisterSSO.sh new_wireless_url oracle_home
administrator_dn
```

new_wireless_url: Wireless HTTP URL with the new Web Cache listener port.

oracle_home: Middle-tier Oracle home whose Web Cache port you are changing.

administrator_dn: OID administrator.

For example, if you have changed the Web Cache listener port to 7779 on the middle-tier installation in /home/oracle on host myhost:

```
ORACLE_HOME/wireless/bin/reRegisterSSO.sh http://myhost:7779/ptg/rm
/home/oracle cn=orcladmin
```

2. Update the Wireless HTTP configuration information:
   a. Navigate to the Wireless home page on Application Server Control.
   b. Select the Site Administration link.
   c. In the General Configuration section, select the HTTP, HTTPS Configuration link.
   d. In the URL section, update each URL that contains the non-SSL Web Cache listener port with the new port number.
   e. Click **OK**.
3. Update the instance URLs:
   a. Navigate to the Wireless home page on the Application Server Control.
   b. In the Instance Configuration Section, select the Instance URLs link.
   c. On the Instance URLs page:
      – If the Use the Wireless Site URLs radio button is selected, you do not need to make any changes to this page.
      – If the Use the WIreless Instance URLs radio button is selected, update each URL that contains the non-SSL Web Cache listener port with the new port number.
   d. Click **OK**.

Step 10: Update OracleAS Discoverer

If you have OracleAS Discoverer configured, and you are using the non-SSL port for the URL of the Discoverer Portlet Provider, edit the URL of the Discoverer Portlet Provider to use the new port number.

> **See Also:** Refer to the instructions on "How to edit Discoverer Portlet Provider" in *Oracle Application Server Discoverer Configuration Guide*.

Step 11: Update OracleAS Reports Services

You do not need to make any configuration changes to Reports Service to reflect the change. However, if you have built any Web pages that contain links to the middle-tier Reports Service, you need to update those Web pages with the new port number.

Step 12: Restart the Middle-Tier Instance

Restart the middle-tier instance:

```
opmnctl stopall
opmnctl startall
```

5.3.5 Changing the Web Cache SSL Listener Port (Middle-Tier Installations)

This section describes how to change the Web Cache SSL listener port. It involves changing the Web Cache port number and updating other components in the middle tier with the new port number.

Step 1: Change the Web Cache SSL Listener Port

1. Using the Application Server Control, navigate to the Web Cache home page.
2. In the Administration section, click Web Cache Administration. Log in to Web Cache Administrator.
3. In the navigator frame, select Ports > Listen Ports. The Listen Ports page appears.
4. Select the port appropriate port that has HTTPS in the Protocol column. Click **Edit Selected**.
5. Enter the new port number in the Port field. Click **Submit**.
6. Click **Apply Changes**. It is not necessary to restart Web Cache at this time since you are going to restart the entire instance at the end of this procedure.

Step 2: Change the Web Cache Logical Site Port

If the Web Cache SSL listener port is the same as the logical site port, update the logical site port as follows:

1. In Web Cache Manager, in the navigator frame, select Origin Servers, Sites, and Load Balancing > Site Definitions.
2. On the Site Definitions page, locate the appropriate site using the old port number. If there is no site using the old port number, then the Web Cache listener and site do not share the same port number. Skip to Step 3: Enable Web Cache to Run as Root for Ports < 1024 on UNIX.
3. Select the appropriate site with the old port number. Click **Edit Site**.
4. In the Edit Site dialog box, enter the new port number. Click **Submit**.
5. In the navigator frame, select Origin Servers, Sites, and Load Balancing > Site-to-Server Mapping.
6. On the Site-to-Server Mapping page, you may see one or more mappings using the old port number. For each site:
   a. Select the site and click **Edit Selected**.
   b. In the Edit / Add Site-to-Server Mapping dialog box, change the Port Number field to the new port number. **Click Submit**.
7. Click **Apply Changes**.

Step 3: Enable Web Cache to Run as Root for Ports < 1024 on UNIX

By default, Web Cache runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Web Cache SSL listener port number to a value less than 1024, you must enable Web Cache to run as root, as follows:

1. Log in as the user that installed Oracle Application Server and stop Web Cache:

   ```
   opmnctl stopproc ias-component=WebCache
   ```

2. Log in as root.
3. Run the following command in the middle-tier Oracle home:

   ```
   ORACLE_HOME/webcache/bin/webcache_setuser.sh setroot userID
   ```

Where *userid* is the current user Web Cache is running under. This is usually the user that installed Oracle Application Server. This user is listed on the Process Identity screen in Web Cache Manager.

4. Log in as the user that installed Oracle Application Server and start Web Cache:

   ```
   opmnctl startproc ias-component=WebCache
   ```

Step 4: Update the Oracle HTTP Server Port directive

1. Edit the following file:

   ORACLE_HOME/Apache/Apache/conf/ssl.conf

2. Update the SSL `Port` directive with the new port number. Do not modify the `Listen` directive. The Web Cache SSL port must equal the Oracle HTTP Server SSL Port directive.
3. Save the file.
4. Run the following command:

   ```
   dcmctl updateConfig -ct ohs
   ```

Step 5: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

   ORACLE_HOME/sysman/emd/targets.xml

2. Update each occurrence of the old Web Cache SSL listener port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Web Cache SSL listener port, or it may contain many occurrences. The listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Web Cache SSL listener port number, and replace them with the new port number. Be sure to update only the Web Cache SSL listener port; do not update any other port numbers.

3. Save and close the file.
4. Reload the Application Server Control:

   ORACLE_HOME/bin/emctl reload

Step 6: Update mod_osso

If you have registered your SSL virtual host as an SSO partner application, follow these steps to re-register your SSL virtual host:

1. Make sure the `LD_LIBRARY_PATH` environment variable contains `$ORACLE_HOME/lib`.
2. Re-register `mod_osso` with the new port number by running the following command in the middle-tier Oracle home:

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path middle_tier_oracle_home
-site_name middle_tier_hostname:new_https_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-virtualhost -u user
```

   Note that *user* is the user that starts Oracle HTTP Server. By default, this is the user that installed Oracle Application Server. If you have changed the Oracle HTTP Server listen port number to a value < 1024, then this user is root.

   For example, if you want to change the Web Cache SSL listen port to 4445 on middle-tier host `myhost`:

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path /disk1/oracleas
-site_name myhost:4445
-config_mod_osso TRUE
-mod_osso_url https://myhost.mydomain:4445
-virtualhost -u oracle
```

   See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering `mod_osso`

Step 7: Update OracleAS Portal

If you have OracleAS Portal configured, update Portal with the new SSL listener port number.

1. Using the Application Server Control, navigate to the Portal home page.
2. In the Administration section, click Portal Web Cache Settings.
   - If Listening Port SSL Enabled is set to Yes, update the Listening Port field with the new port number. Click **OK**.

- If Listening Port SSL Enabled is set to No, you do not need to update anything on this page. Click **Cancel**.

3. Update the following file to use the new port number:

   ORACLE_HOME/Apache/modplsql/conf/dads.conf

4. Run the following command:

   ```
   dcmctl updateConfig
   ```

5. Update the `httpsports` parameter in the following file:

   ORACLE_HOME/j2ee/OC4J_Portal/applications/portal/portal/WEB-INF/web.xml

Step 8: Update Wireless

If you have Wireless configured, update Wireless with the new port number:

1. Re-register Wireless with SSO by running the following command on the middle-tier host:

   ORACLE_HOME/wireless/bin/reRegisterSSO.sh *new_wireless_url oracle_home administrator_dn*

   new_wireless_url: Wireless HTTPS URL with the new Web Cache SSL listener port.

   oracle_home: Middle-tier Oracle home whose Web Cache port you are changing.

   administrator_dn: OID administrator.

   For example, if you have changed the Web Cache SSL listener port to `80` on the middle-tier installation in `/home/oracle` on host `myhost`:

   ORACLE_HOME/wireless/bin/reRegisterSSO.sh https://myhost:80/ptg/rm /home/oracle cn=orcladmin

2. Update the Wireless HTTPS configuration information:

   a. Navigate to the Wireless home page on the Application Server Control.

   b. Select the Site Administration link.

   c. In the General Configuration section, select the HTTP, HTTPS Configuration link.

   d. In the URL section, update each URL that contains the SSL Web Cache listener port with the new port number.

e. Click **OK**.

3. Update the instance URLs:

   a. Navigate to the Wireless home page on the Application Server Control.

   b. In the Instance Configuration Section, select the Instance URLs link.

   c. On the Instance URLs page:

      – If the Use the Wireless Site URLs radio button is selected, you do not need to make any changes to this page.

      – If the Use the WIreless Instance URLs radio button is selected, update each URL that contains the SSL Web Cache listener port with the new port number.

   d. Click **OK**.

Step 9: Update OracleAS Discoverer

If you have OracleAS Discoverer configured, and you are using the SSL port for the URL of the Discoverer Portlet Provider, edit the URL of the Discoverer Portlet Provider to use the new port number.

> **See Also:** Refer to the instructions on "How to edit Discoverer Portlet Provider" in *Oracle Application Server Discoverer Configuration Guide*.

Step 10: Update OracleAS Reports Services

You do not need to make any configuration changes to Reports Services to reflect the change. However, if you have built any Web pages that contain links to the middle-tier Reports Service, you need to update those Web pages with the new port number.

Step 11: Restart the Middle-Tier Instance

Restart the middle-tier instance:

```
opmnctl stopall
opmnctl startall
```

5.3.6 Changing the Web Cache Administration Port

To change the Web Cache administration port on any installation type:

Step 1: Change the Web Cache Administration Port

1. Navigate to the Web Cache Manager using the following URL:

   `http://web_cache_hostname:current_web_cache_admin_port/webcacheadmin`

   For example:

   `http://web_cache_hostname:4000/webcacheadmin`

2. Log in to the Web Cache Manager as `ias_admin` or `administrator`.
3. In the navigator frame, select Ports > Operations Ports. The Operations Ports page appears.
4. Select the cache for which to modify the administration port. Click **Edit Selected**.
5. In the ADMINISTRATION row, change the Port Number field. Click **Submit**.
6. Click **Apply Changes**.
7. Exit out of the Web Cache Manager.
8. Restart Web Cache

   Note that you must restart from the command-line; do not use the Web Cache Manager to restart. You can restart in either of the following ways:

   - The preferred method is to restart your Web Cache server as follows:

     `ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=WebCache`

   - If you do not want to restart the Web Cache server, you can restart only the Web Cache Manager:

     `ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=WebCacheAdmin`

     If you choose this method, Web Cache will operate properly, however, Web Cache Manager will display the following message until you restart the entire Web Cache server: "Restart Web Cache to make configuration changes take effect."

Step 2: Update Application Server Control

Update the Application Server Control with the new Web Cache administration port number as follows:

1. Edit the following file:

ORACLE_HOME/sysman/emd/targets.xml

2. In the target type `oracle_webcache`, update the `AdminPort` property with the new port number.
3. Save and close the file.
4. Reload Oracle Enterprise Manager Application Server Control:

   ORACLE_HOME/bin/emctl reload

Step 3: Update OracleAS Portal

If the Web Cache is front-ending Portal, update Portal with the new administration port number:

1. Using the Application Server Control, navigate to the Portal home page.
2. In the Administration section, click Portal Web Cache Settings.
3. Update the Administration Port field with the new port number. Click **OK**.

5.3.7 Changing the Web Cache Invalidation Port

To change the Web Cache invalidation port on any installation type:

Step 1: Change the Web Cache Invalidation Port

1. Using the Application Server Control, navigate to the Web Cache home page.
   a. In the Administration section, click Web Cache Administration. Log in to Web Cache Administrator.
   b. In the navigator frame, select Ports > Operations Ports. The Operations Ports page appears.
   c. Select the cache for which to modify the invalidation port. Click **Edit Selected**.
   d. In the INVALIDATION row, change the Port Number field. Click **Submit**.
   e. Click **Apply Changes**.
   f. Click **Restart**.

Step 2: Update OracleAS Portal

If the Web Cache is front-ending Portal, update Portal with the new invalidation port number.

1. Using the Application Server Control, navigate to the Portal home page.
2. In the Administration section, click Portal Web Cache Settings.
3. Update the Invalidation Port field with the new port number. Click **OK**.

5.3.8 Changing the Web Cache Statistics Port

To change the Web Cache statistics port on any installation type:

1. Using the Application Server Control, navigate to the Web Cache home page.
2. In the Administration section, click Web Cache Administration. Log in to Web Cache Administrator.
3. In the navigator frame, select Ports > Operations Ports. The Operations Ports page appears.
4. Select the cache for which to modify the statistics port. Click **Edit Selected**.
5. In the STATISTICS row, change the Port Number field. Click **Submit**.
6. Click **Apply Changes**.
7. Click **Restart**.

5.3.9 Changing the DCM Java Object Cache Port

This section describes how to change the DCM Java Object Cache port number in any installation type. To change the DCM Java Object Cache port number:

1. Edit the following file:

   ORACLE_HOME/dcm/config/dcmCache.xml

2. Under the <communication> element, update the discovery-port parameter in the <coordinator> element with the new port number. For example:

   ```
   <coordinator discovery-port="7110" original="true" />
   ```

3. Save the file.
4. In every instance in the farm, stop Application Server Control and stop the DCM daemon:

   ```
   emctl stop iasconsole
   opmnctl stopproc ias-component=dcm-daemon
   ```

It is important that you make sure all Application Server Control instances and DCM daemons in the farm are stopped before you proceed to the next step.

5. In every instance in the farm, start the DCM daemon and Application Server Control:

```
opmnctl startproc ias-component=dcm-daemon
emctl start iasconsole
```

5.3.10 Changing the Java Object Cache Port

This section describes how to change the Java Object Cache port number in any installation type. To change the Java Object Cache port number:

1. Edit the following file:

   ORACLE_HOME/javacache/admin/javacache.xml

2. Under the `<communication>` element, update the `discovery-port` parameter in the `<coordinator>` element with the new port number. For example:

```
<coordinator discovery-port="7010" />
```

3. Save the file.
4. Restart all OC4J instances which contain J2EE applications that use JavaCache:

```
dcmctl restart -co OC4J_INSTANCE
```

5.3.11 Changing the JServ Servlet Engine Port

This section describes how to change the JServ Servlet Engine port number in any installation type. To change the JServ Servlet Engine port:

1. Edit the following file:

   ORACLE_HOME/Apache/Jserv/etc/jserv.properties

2. Update the `port` parameter with the new port number.
3. Save the file.
4. Restart Oracle HTTP Server:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl startproc ias-component=HTTP_Server
```

5.3.12 Changing the Log Loader Port

This section describes how to change the Log Loader port on any installation type. To change the Log Loader port:

1. Stop the Log Loader:
   a. In Application Server Control, navigate to the Application Server home page for the instance whose Log Loader port you would like to change.
   b. Click **Logs** in the upper-right corner.
   c. On the View Logs page, click **Search Log Repository**.
   d. On the View Logs page, click the **Log Loader** button.
   e. On the Log Loader page, click the **Stop** button.
2. Change the Log Loader port number:
   a. On the Log Loader page, in the Administration section, click **Log Loader Properties**.
   b. On the Log Loader Properties page, enter the new port number in the Log Loader Port field.
   c. Click **Apply**.
3. Start the Log Loader:
   a. At the top of the Log Loader Properties page, click **Log Loader** to get back to the Log Loader page.
   b. On the Log Loader page, click the **Start** button.

5.3.13 Changing OPMN Ports (ONS Local, Request, and Remote)

This section describes how to change any of the following port numbers:

- ONS Local port
- ONS Request port
- ONS Remote port

You can change ONS port using Application Server Control or manual steps:

- **Using Application Server Control**:
  1. Navigate to the Application Server home page and click **Process Management**.

2. On the Process Management page, modify the `local`, `remote`, or `request` parameter, as desired, in the `<port>` element. For example:

   ```
   <port local="6101" remote="6201" request="6004"/>
   ```

3. At the bottom of the page, click **Apply**.
4. Restart OPMN and OPMN-managed processes:

   ```
   opmnctl stopall
   opmnctl startall
   ```

- **Using Manual Steps:**

1. Edit the following file:

   ORACLE_HOME`/opmn/conf/opmn.xml`

2. Under the `<notification-server>` element, modify the `local`, `remote`, or `request` parameter, as desired, in the `<port>` element. For example:

   ```
   <port local="6101" remote="6201" request="6004"/>
   ```

3. Reload and restart OPMN and OPMN-managed processes:

   ```
   opmnctl reload
   opmnctl stopall
   opmnctl startall
   ```

5.3.14 Changing the Oracle HTTP Server Diagnostic Port

This section describes how to change the Oracle HTTP Server Diagnostics port number in any installation type. To change the Oracle HTTP Server Diagnostics port number:

1. Edit the following file:

   ORACLE_HOME`/Apache/Apache/conf/dms.conf`

2. Change the old port number to the new port number everywhere it appears in the file. This includes the `Listen` directive, `OpmnHostPort` directive, `Redirect` directive, and the Virtual Host.
3. Save the file.
4. Restart Oracle HTTP Server:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl startproc ias-component=HTTP_Server
```

5.3.15 Changing the Port Tunneling Port

This section describes how to change the Port Tunneling port on any installation type. To change the Port Tunneling port number:

1. Edit the following file:

   ORACLE_HOME/opmn/conf/opmn.xml

2. Under the <ias-component id="IASPT"> element, update the range parameter in the <port> element with the new range. For example:

   ```
   <port id="ajp" range="7501-7503"/>
   ```

   Note that the port number range specified in opmn.xml overrides any port number specified in iaspt.conf. So you only need to update the port number in opmn.xml.

3. Restart OPMN:

   ```
   opmnctl reload
   opmnctl stopall
   opmnctl startall
   ```

5.4 Changing Portal and Wireless Ports

This section contains the following topics:

- Changing OracleAS Portal Ports
- Changing OracleAS Wireless Ports

5.4.1 Changing OracleAS Portal Ports

OracleAS Portal uses the Web Cache HTTP server port on the instance.

> **See Also:** Section 5.3.4, "Changing the Web Cache Non-SSL Listener Port (Middle-Tier Installations)"

5.4.2 Changing OracleAS Wireless Ports

OracleAS Wireless uses the Web Cache HTTP server port on the instance.

See Also: Section 5.3.4, "Changing the Web Cache Non-SSL Listener Port (Middle-Tier Installations)"

5.5 Changing Business Intelligence and Forms Ports

This section contains the following topics:

- Changing OracleAS Discoverer Ports
- Changing OracleAS Forms Services Ports
- Changing the OracleAS Reports Services SQL*Net Port

5.5.1 Changing OracleAS Discoverer Ports

The OracleAS Discoverer OSAgent port cannot be changed after installation. Other OracleAS Discoverer services use the Web Cache HTTP server port on the instance.

See Also: Section 5.3.4, "Changing the Web Cache Non-SSL Listener Port (Middle-Tier Installations)"

5.5.2 Changing OracleAS Forms Services Ports

OracleAS Forms Services uses the Web Cache HTTP server port on the instance.

See Also: Section 5.3.4, "Changing the Web Cache Non-SSL Listener Port (Middle-Tier Installations)"

5.5.3 Changing the OracleAS Reports Services SQL*Net Port

To change the Reports Services SQL*Net port number:

1. On the Reports Services host, edit the `tnsnames.ora` file. The default location is:

   ORACLE_HOME`/network/admin/tnsnames.ora`

   In the `REP_`*HOSTNAME* entry, update the `PORT` parameter with the new port number.

2. On all client hosts, edit the `tnsnames.ora` file. In the `REP_`*HOSTNAME* entry, update the `PORT` parameter with the new port number.

5.6 Changing Infrastructure Ports

This section contains the following topics:

5.6.1 Changing the Metadata Repository Net Listener Port

First, determine if it is necessary to change the Metadata Repository listener port number. If you are concerned about the fact that you have another database on your host using the same port, it is possible that the Metadata Repository and the other database can use the same port.

The following are guidelines for port usage by multiple databases on the same host:

- Multiple Oracle9i databases can share the same Net listener port. So, if the other databases on your host are Oracle9i databases, the Metadata Repository can all use port 1521 as the Net listener port. There is no need to change the port number.
- If the other databases on your system are Oracle8i databases running Oracle Net8 listener, then the Metadata Repository must use a different port. They cannot share the same port.

Note: If you want to run two listeners that use the same key value on one host, refer to Section 5.6.1.1, "Changing the KEY value for an IPC Listener"

If you determine that you would like to change the Metadata Repository Listener Port, follow the steps in this section. A Metadata Repository may be used in several different ways. Use the following table to determine the steps that are required for changing your type of Metadata Repository:

If the Metadata Repository is used as follows:	Follow these steps to change its Net Listener port:
■ Identity Management Repository, Product Metadata Repository, and Management (DCM) Repository ■ Registered with OID	Step 1: Make Sure OID and SSO Are Running Step 2: Change the Metadata Repository Net Listener Port Step 3: Update Oracle Internet Directory Step 4: Update Single Sign-On Step 5: Update OracleAS Certificate Authority Step 6: Update Application Server Control Step 8: Update the Middle-Tier Instances
■ Identity Management Repository only ■ Registered with OID	Step 1: Make Sure OID and SSO Are Running Step 2: Change the Metadata Repository Net Listener Port Step 3: Update Oracle Internet Directory Step 4: Update Single Sign-On Step 5: Update OracleAS Certificate Authority Step 6: Update Application Server Control
■ Product Metadata and Management (DCM) Repository ■ Registered with OID	Step 1: Make Sure OID and SSO Are Running Step 2: Change the Metadata Repository Net Listener Port Step 3: Update Oracle Internet Directory Step 8: Update the Middle-Tier Instances
■ Management (DCM) Repository only ■ Not registered with OID	Step 2: Change the Metadata Repository Net Listener Port Step 7: Update DCM Schema Information

Step 1: Make Sure OID and SSO Are Running

If the Metadata Repository is registered with OID, make sure that the Identity Management instance (SSO and OID) is up and running before you proceed.

Step 2: Change the Metadata Repository Net Listener Port

On the Metadata Repository host:

1. Make sure your `ORACLE_HOME` environment variable and `ORACLE_SID` are set.
2. Stop the Metadata Repository listener:

   ```
   lscnrctl stop
   ```

3. Edit the following file:

ORACLE_HOME/network/admin/listener.ora

Under the LISTENER entry, update the value for PORT.

4. Edit the tnsnames.ora file. The default location is:

   ORACLE_HOME/network/admin/tnsnames.ora

   Update the PORT value in each entry that applies to the Metadata Repository.

5. Start the Metadata Repository listener:

   ```
   lsnrctl start
   ```

Step 3: Update Oracle Internet Directory

On the Identity Management host, update OID with the new Net Listener port number:

1. Start Oracle Directory Manager:

   ORACLE_HOME/bin/oidadmin

2. Log in to Oracle Directory Manager.
3. In the System Objects frame:
   a. Expand **Entry Management**.
   b. Expand **cn=Oracle Context**.
   c. Select the DBName for the Metadata Repository. For example, if the DBName is the default, asdb, select **cn=ASDB**.
4. On the Properties tab, update the PORT parameter in the orclnetdescstring field with the new port number.
5. Click **Apply**.

Step 4: Update Single Sign-On

On the SSO host:

1. Make sure the LD_LIBRARY_PATH environment variable contains $ORACLE_HOME/lib.
2. Update Single-Sign on with the new repository port number by running the following command in the SSO Oracle home:

   ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoca.jar reassoc -repos $ORACLE_HOME

Step 5: Update OracleAS Certificate Authority

If the Identity Management installation has OracleAS Certificate Authority:

1. Launch the OracleAS Certificate Authority management GUI:

   `https://`*`infrastructure_hostname`*`:`*`http_ssl_port`*`/oca/admin`

   Where *`http_ssl_port`* is the HTTP SSL listener port.

2. Select the Configuration Management tab.
3. Select the General sub-tab.
4. Under Database Settings, update the Database Connect String with the new port number.

Step 6: Update Application Server Control

Update Application Server Control with the new port number:

1. In the Identity Management Oracle home, edit the following file:

   `ORACLE_HOME``/sysman/emd/targets.xml`

2. Update the old Metadata Repository port number with the new port number.

   Locate the `oracle_ldap` target and update the `PORT` parameter in the `ConnectDescriptor` value with the new port number. The easiest way to find this is to search the file for the old port number.

3. Save and close the file.
4. Reload Application Server Control:

   `ORACLE_HOME``/bin/emctl reload`

Step 7: Update DCM Schema Information

In each middle-tier Oracle home uses the Metadata Repository for its Management (DCM) schema:

1. Edit the following file:

   `ORACLE_HOME``/config/iasschema.xml`

2. Locate the `<SchemaConfigData>` entry for the `DCM` schema.
3. In this entry, update the `<DBConnect>` entry with the new port number.
4. Save and close the file.

5. Restart the DCM daemon:

```
opmnctl restartproc ias-component=dcm-daemon
```

Step 8: Update the Middle-Tier Instances

In each middle-tier Oracle home that uses the Metadata Repository, update the following file with the new Net Listener port number:

ORACLE_HOME/network/admin/tnsnames.ora

5.6.1.1 Changing the KEY value for an IPC Listener

It is not possible to run two listeners at the same time that are configured to use the same KEY value in their IPC protocol address. By default, the OracleAS Metadata Repository listener has its IPC KEY value set to EXTPROC. Hence, if your computer has another IPC listener that uses the EXTPROC key, you should configure the Metadata Repository listener to use some other key value such as EXTPROC1.

To change the KEY value of an IPC listener:

1. Stop the listener:

   ORACLE_HOME/bin/lsnrctl stop

2. Edit the listener.ora and tnsnames.ora files. In each file, change the line that says:

   ```
   (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC))
   ```

   to something like:

   ```
   (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
   ```

3. Restart the listener:

   ORACLE_HOME/bin/lsnrctl start

5.6.2 Changing Oracle Internet Directory Ports

This section describes how to change the Oracle Internet Directory port on an Identity Management installation. When you change this port number, you must update any middle-tier instances that use the Identity Management installation.

The following procedures contain complete instructions for updating the Oracle Internet Directory port number on Identity Management, including updating other components in the Infrastructure and updating the middle-tier instances that use the port:

- Changing the Oracle Internet Directory Non-SSL Port
- Changing the Oracle Internet Directory SSL Port

5.6.2.1 Changing the Oracle Internet Directory Non-SSL Port

This procedure describes how to change the Oracle Internet Directory non-SSL port on an Identity Management installation. Review all steps before you begin.

Step 1: Prepare the Middle-Tier Instances

Follow this step only if the Identity Management installation is being used by middle-tier instances. On each middle-tier instance that uses Identity Management, stop the middle-tier instance as follows:

1. On the Application Server home page of Application Server Control, click **Stop All**.
2. Leave Application Server Control running.

It is important that you leave Application Server Control running in each of the middle-tier instances while you perform this procedure.

Step 2: Prepare the Infrastructure Instances

1. Make sure that Identity Management and its associated Metadata Repository are up and running on the Infrastructure whose port number you are changing.
2. If any middle-tier instances use different Metadata Repositories for their product metadata and DCM repositories, make sure those are up. In short, make sure all Metadata Repositories in your environment are up.

Step 3: Change the Oracle Internet Directory port

1. On the Oracle Internet Directory host:
   a. Create a file named `mod.ldif` with the following contents (you can create the file in any directory):

```
dn:cn=configset0, cn=osdldapd, cn=subconfigsubentry
changetype:modify
replace:orclnonsslport
orclnonsslport:new_port_number
```

   b. Run the following command:

```
ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w password -p oid_port -f
mod.ldif
```

c. On the Oracle Internet Directory host, restart OID:

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

2. Perform this step in the Oracle Internet Directory Oracle home. If you have Metadata Repositories installed in other Oracle homes that are registered with this Oracle Internet Directory, perform this step in each of those Oracle homes as well.

   a. Edit the following file:

   ORACLE_HOME/network/admin/ldap.ora

   Modify the following line to contain the new non-SSL port number:

   DIRECTORY_SERVERS=(myhost.myco.com:*non_ssl_port*:*ssl_port*)

   Save and close the file.

   b. Edit the following file:

   ORACLE_HOME/config/ias.properties

   Change the value of `OIDport` to the new non-SSL port number.

   Save and close the file.

3. Perform this step in the SSO Oracle home:

   a. Make sure the `LD_LIBRARY_PATH` environment variable contains `$ORACLE_HOME/lib`.

   b. Run the following command in the SSO Oracle home:

   ```
   ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoca.jar reassoc
   -repos $ORACLE_HOME
   ```

Step 4: Reconfigure OracleAS Certificate Authority

Follow this step if you are using OCA:

1. If OCA is running in a different Oracle home, do the following step in the OCA Oracle home:

   a. Edit the following file:

   ORACLE_HOME/config/ias.properties

a. Change the value of `OIDport` to the new non-SSL port number.

b. Save and close the file.

2. Update OCA with the new OID port number by running the following command in the OCA Oracle home:

```
ORACLE_HOME/oca/bin/ocactl changesecurity -server_auth_port port_number
```

Where *port_number* is the OCA Server Authentication Virtual Host (SSL) port; the default is `4400`.

See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for more information

Step 5: Restart the Identity Management Instance

Restart the Identity Management instance:

```
emctl stop iasconsole
opmnctl stopall
opmnctl startall
emctl start iasconsole
```

Step 6: Update the Middle-Tier Instances to Use the New Port Number

On each middle-tier instance that uses the Identity Management installation, run the Change Identity Management Services wizard and start the instance:

1. On Application Server Control, navigate to the Application Server home page for the middle-tier instance.
2. Click the Infrastructure link.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the new Identity Management information (the new port number).
5. When the wizard is finished, navigate to the Application Server Home Page and start the middle-tier instance by clicking **Start All**.

5.6.2.2 Changing the Oracle Internet Directory SSL Port

This procedure describes how to change the Oracle Internet Directory SSL port on an Identity Management installation. Review all steps before you begin.

Step 1: Prepare the Middle-Tier Instances

Follow this step only if the Identity Management installation is being used by middle-tier instances. On each middle-tier instance that uses Identity Management, stop the middle-tier instance as follows:

1. On the Application Server home page of Application Server Control, click **Stop All**.
2. Leave Application Server Control running.

It is important that you leave Application Server Control running in each of the middle-tier instances while you perform this procedure.

Step 2: Prepare the Infrastructure Instances

1. Make sure that Identity Management and its associated Metadata Repository are up and running on the Infrastructure whose port number you are changing.
2. If any middle-tier instances use different Metadata Repositories for their product metadata and DCM repositories, make sure those are up. In short, make sure all Metadata Repositories in your environment are up.

Step 3: Change the Oracle Internet Directory port

1. On the Oracle Internet Directory host:
   a. Create a file named `mod.ldif` with the following contents (you can create the file in any directory):

      ```
      dn:cn=configset0, cn=osdldapd, cn=subconfigsubentry
      changetype:modify
      replace:orclsslport
      orclsslport:new_ssl_port_number
      ```

   b. Run the following command:

      ```
      ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w password -p oid_port -f
      mod.ldif
      ```

   c. On the Oracle Internet Directory host, restart OID:

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

2. Perform this step in the Oracle Internet Directory Oracle home. If you have Metadata Repositories installed in other Oracle homes that are registered with

this Oracle Internet Directory, perform this step in each of those Oracle homes as well.

a. Edit the following file:

ORACLE_HOME/network/admin/ldap.ora

Modify the following line to contain the new SSL port number:

```
DIRECTORY_SERVERS=(myhost.myco.com:non_ssl_port:ssl_port)
```

Save and close the file.

b. Edit the following file:

ORACLE_HOME/config/ias.properties

Change the value of `OIDsslport` to the new SSL port number.

Save and close the file.

3. Perform this step in the SSO Oracle home:

a. Make sure the `LD_LIBRARY_PATH` environment variable contains `$ORACLE_HOME/lib`.

b. Run the following command in the SSO Oracle home:

```
ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoca.jar reassoc
-repos $ORACLE_HOME
```

Step 4: Reconfigure OracleAS Certificate Authority

Follow this step if you are using OCA:

1. If OCA is running in a different Oracle home, perform the following step in the OCA Oracle home:

a. Edit the following file:

ORACLE_HOME/config/ias.properties

a. Change the value of `OIDsslport` to the new SSL port number.

b. Save and close the file.

2. Update OCA with the new OID port number by running the following command in the OCA Oracle home:

ORACLE_HOME/oca/bin/ocactl changesecurity -server_auth_port *port_number*

Where *port_number* is the OCA Server Authentication Virtual Host (SSL) port; the default is 4400.

> **See Also:** *Oracle Application Server Certificate Authority Administrator's Guide* for more information

Step 5: Restart the Identity Management Instance

Restart the Identity Management instance:

```
emctl stop iasconsole
opmnctl stopall
opmnctl startall
emctl start iasconsole
```

Step 6: Update the Middle-Tier Instances to Use the New Port Number

On each middle-tier instance that uses the Identity Management installation, run the Change Identity Management Services wizard and start the instance:

1. On Application Server Control, navigate to the Application Server home page for the middle-tier instance.
2. Click the Infrastructure link.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the new Identity Management information (the new port number).
5. When the wizard is finished, navigate to the Instance Home Page and start your instance by clicking **Start All**.

5.6.3 Changing the HTTP Server (SSO) Port on Identity Management

This section describes how to change the Oracle HTTP Server listen port on an Identity Management installation. When you change this port number, you also effectively change the Single Sign-On (SSO) port number. This means you must update any middle-tier instances that use the Single Sign-On port.

The following procedures contain complete instructions for updating the Oracle HTTP Server port number on Identity Management, including updating other components in the Infrastructure and updating the middle-tier instances that use the port:

- Changing the Oracle HTTP Server Non-SSL Listen Port on Identity Management

- Changing the Oracle HTTP Server SSL Listen Port on Identity Management

5.6.3.1 Changing the Oracle HTTP Server Non-SSL Listen Port on Identity Management

This procedure describes how to change the non-SSL listen port on an Identity Management installation. When you do this, you must update both the Listen and Port directives with the new port number.

Step 1: Prepare the Middle-Tier Instances

Follow this step only if the Identity Management installation is being used by middle-tier instances. On each middle-tier instance that uses Identity Management, stop the middle-tier instance as follows:

1. On the Application Server home page of Application Server Control, click **Stop All**.
2. Leave Application Server Control running.

It is important that you leave Application Server Control running in each of the middle-tier instances while you perform this procedure.

Step 2: Prepare the Infrastructure Instances

1. Make sure that Identity Management and its associated Metadata Repository are up and running on the Infrastructure whose port number you are changing.
2. If any middle-tier instances use different Metadata Repositories for their product metadata and DCM repositories, make sure those are up. In short, make sure all Metadata Repositories in your environment are up.

Step 3: Modify the Oracle HTTP Server Listen and Port Directives

Change both the Listen and Port directive to the new port number. You can perform this step using Application Server Control or manual steps.

- **Using the Application Server Control:**
  1. Navigate to the Application Server home page and click **Ports**.
  2. On the Ports Page, locate the Oracle HTTP Server Listen port and click the icon in the Configure column.
  3. On the Server Properties Page:
     * Enter the new port number in the Default Port field. This is for the `Port` directive.

* Enter the new port number in the Listening Port column. This is for the `Listen` directive. There may be more than one listening port listed. The only way to tell which is the non-SSL listen port is to choose the one with the old non-SSL listen port value.

4. At the bottom of the page, click **Apply**.
5. On the Confirmation Page, click **No**, you would not like to restart now.

- **Using Manual Steps:**

1. Edit the following file:

   ORACLE_HOME`/Apache/Apache/conf/httpd.conf`

2. Update the non-SSL `Listen` and `Port` directives with the new port number. The value for `Listen` and `Port` must be the same port number, for example, to change the listener port to `7779`:

   ```
   Listen 7779
   Port 7779
   ```

   There may be multiple `Listen` and `Port` directives in this file. Modify the `Listen` and `Port` directives that are not enclosed in an SSL virtual host container. The easiest way to locate the proper `Listen` and `Port` directives is to search the file for the old port number.

3. Save and close the file.
4. Run the following command:

   ```
   dcmctl updateConfig -ct ohs
   ```

Step 4: Enable Oracle HTTP Server to Run as Root for Ports < 1024 on UNIX

Perform this step if you are changing the port to a value less than 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Oracle Application Server non-SSL listen port number to a value less than 1024, you must enable Oracle HTTP Server to run as root, as follows:

1. Log in as root.
2. Run the following commands in the middle-tier Oracle home:

   ```
   cd ORACLE_HOME/Apache/Apache/bin
   chown root .apachectl
   chmod 6750 .apachectl
   ```

Step 5: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

   ORACLE_HOME/sysman/emd/targets.xml

2. Update each occurrence of the old Oracle HTTP Server listen port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Oracle HTTP Server listen port, or it may contain many occurrences. The listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Oracle HTTP Server listen port number, and replace them with the new port number.

3. Save and close the file.

4. Reload Application Server Control:

   ORACLE_HOME/bin/emctl reload

Step 6: Update Single Sign-On

Perform this step if SSO is configured to use the non-SSL Oracle HTTP Server listen port in the installation where you are changing the port.

1. Make sure the LD_LIBRARY_PATH environment variable contains $ORACLE_HOME/lib.

2. Run the following command in the SSO Oracle home:

   ORACLE_HOME/sso/bin/ssocfg.sh http *hostname new_port_number*

   Where:

   hostname is the host on which SSO is running

   new_port_number is the new non-SSL Oracle HTTP Server listen port number

Step 7: Re-register mod_osso

Re-register mod_osso as follows:

1. Make sure the LD_LIBRARY_PATH environment variable contains $ORACLE_HOME/lib.

2. Re-register mod_osso to take care of the default partner applications by running the following command in the Identity Management Oracle home:

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path middle_tier_oracle_home
-site_name middle_tier_hostname:new_http_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-u user
```

Note that *user* is the user that starts Oracle HTTP Server. By default, this is the user that installed Oracle Application Server. If you have changed the Oracle HTTP Server listen port number to a value < 1024, then this user is `root`.

For example, if you want to change the Oracle HTTP Server listen port to 7779 on host `myhost`:

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path /disk1/oracleas
-site_name myhost:7779
-config_mod_osso TRUE
-mod_osso_url http://myhost.mydomain:7779
-u oracle
```

3. If you have configured or modified any additional partner applications, you must also re-register those.

   See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering `mod_osso`.

Step 8: Update DAS

If you have DAS configured, and DAS uses the non-SSL port number, follow these steps to update the DAS URL entry in Oracle Internet Directory.

Note: You can find out what port DAS uses with the following command:

```
ORACLE_HOME/bin/ldapsearch -h oid_host -p oid_port -D "cn=orcladmin"
-w "password" -b "cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext"
-s base "objectclass=*" orcldasurlbase
```

1. Create a file named `mod.ldif` with the following contents (you can create the file in any directory):

   ```
   dn:cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
   changetype:modify
   replace:orcldasurlbase
   orcldasurlbase:http://hostname:new_http_port_number/
   ```

Note the slash at the end of the `orcldasurlbase` URL.

2. Run the following command:

```
ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w password -p oid_port -f
mod.ldif
```

3. Refresh the OID cache in your applications:
   a. Log in to the Portal.
   b. Click on the global settings link.
   c. Click the OID / DAS tab.
   d. Check the refresh OID cache settings and click Apply.

Step 9: Update Oracle Application Server Certificate Authority

If you are using OracleAS Certificate Authority:

1. Re-register OCA with the SSO server by running the following command in the OCA Oracle home:

```
ORACLE_HOME/oca/bin/ocactl changesecurity -server_auth_port port_number
```

   Where *port_number* is the OCA Server Authentication Virtual Host (SSL) port; the default is `4400`.

   See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for more information

2. If OCA is located in a different Oracle home than the SSO server, restart Oracle HTTP Server and the `oca` instance in the OCA Oracle home:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl stopproc process-type=oca
opmnctl startproc ias-component=HTTP_Server
opmnctl startproc process-type=oca
```

Step 10: Restart the Identity Management Instance:

Restart the Identity Management instance:

```
opmnctl stopall
opmnctl startall
```

Step 11: Restart OracleAS Certificate Authority

If OCA is configured in this instance, restart it:

```
ORACLE_HOME/oca/bin/ocactl start
```

Step 12: Update the Middle-Tier Instances to Use the New Port Number

On each middle-tier instance that uses the Identity Management installation, run the Change Identity Management Services wizard and start the instance:

1. On Application Server Control, navigate to the Application Server home page for the middle-tier instance.
2. Click the Infrastructure link.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the new Identity Management information (the new port number).
5. When the wizard is finished, navigate to the Application Server Home Page and start the middle-tier instance by clicking **Start All**.

5.6.3.2 Changing the Oracle HTTP Server SSL Listen Port on Identity Management

This procedure describes how to change the SSL listen port on an Identity Management installation. When you do this, you must update both the SSL Listen and SSL Port directives with the new port number.

Step 1: Prepare the Middle-Tier Instances

Follow this step only if the Identity Management installation is being used by middle-tier instances. On each middle-tier instance that uses Identity Management, stop the middle-tier instance as follows:

1. On the Application Server home page of Application Server Control, click **Stop All**.
2. Leave Application Server Control running.

It is important that you leave Application Server Control running in each of the middle-tier instances while you perform this procedure.

Step 2: Prepare the Infrastructure Instances

1. Make sure that Identity Management and its associated Metadata Repository are up and running on the Infrastructure whose port number you are changing.

2. If any middle-tier instances use different Metadata Repositories for their product metadata and DCM repositories, make sure those are up. In short, make sure all Metadata Repositories in your environment are up.

Step 3: Modify the Oracle HTTP Server SSL Listen and SSL Port Directives

Change both the SSL Listen and SSL Port directives to the new port number. You must do this using manual steps.

1. Edit the following file:

   ORACLE_HOME/Apache/Apache/conf/ssl.conf

2. Update the SSL `Listen` and SSL `Port` directives with the new port number. The value for `Listen` and `Port` must be the same port number, for example, to change the listener port to `4445`:

   ```
   Listen 4445
   Port 4445
   ```

3. Save and close the file.

4. Run the following command:

   ```
   dcmctl updateConfig -ct ohs
   ```

Step 4: Enable Oracle HTTP Server to Run as Root for Ports < 1024 on UNIX

Perform this step if you are changing the port to a value less than 1024.

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Application Server). On UNIX systems, if you change the Oracle Application Server non-SSL listen port number to a value less than 1024, you must enable Oracle HTTP Server to run as root, as follows:

1. Log in as root.

2. Run the following commands in the middle-tier Oracle home:

   ```
   cd ORACLE_HOME/Apache/Apache/bin
   chown root .apachectl
   chmod 6750 .apachectl
   ```

Step 5: Update Application Server Control

Update Application Server Control with the new port number:

1. Edit the following file:

```
ORACLE_HOME/sysman/emd/targets.xml
```

2. Update each occurrence of the old Oracle HTTP Server SSL listen port number with the new port number.

   Depending on your configuration, this file may not contain any occurrences of the Oracle HTTP Server SSL listen port, or it may contain many occurrences. The listen port may occur as a parameter on its own, or it may be part of a URL. The easiest way to edit this file is to search for all occurrences of the old Oracle HTTP Server SSL listen port number, and replace them with the new port number. Be sure to update only the Oracle HTTP Server SSL listen port; do not update the Oracle HTTP Server non-SSL listen port or any other port numbers.

3. Save and close the file.

4. Reload Application Server Control:

   ```
   ORACLE_HOME/bin/emctl reload
   ```

Step 6: Update Single Sign-On

Perform this step if SSO is configured to use the non-SSL Oracle HTTP Server listen port in the installation where you are changing the port.

1. Make sure the `LD_LIBRARY_PATH` environment variable contains `$ORACLE_HOME/lib`.

2. If SSO is configured to use the SSL Oracle HTTP Server listen port in the installation where the listen port is being changed, run the following command in the SSO Oracle home:

   ```
   ORACLE_HOME/sso/bin/ssocfg.sh https hostname new_port_number
   ```

   Where:

   `hostname` is the host on which SSO is running

   `new_port_number` is the new SSL Oracle HTTP Server listen port number

Step 7: Re-register mod_osso

Re-register `mod_osso` as follows:

1. Make sure the `LD_LIBRARY_PATH` environment variable contains `$ORACLE_HOME/lib`.

2. Re-register `mod_osso` to take care of the default partner applications by running the following command in the Identity Management Oracle home:

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path middle_tier_oracle_home
-site_name middle_tier_hostname:new_https_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-virtualhost -u user
```

Note that *user* is the user that starts Oracle HTTP Server. By default, this is the user that installed Oracle Application Server. If you have changed the Oracle HTTP Server listen port number to a value < 1024, then this user is root.

For example, if you want to change the Oracle HTTP Server listen port to 4445 on host myhost:

```
$ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
-oracle_home_path /disk1/oracleas
-site_name myhost:4445
-config_mod_osso TRUE
-mod_osso_url https://myhost.mydomain:4445
-virtualhost -u oracle
```

3. If you have configured or modified any additional partner applications, you must also re-register those.

   See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for more information on registering mod_osso.

Step 8: Update DAS

If you have DAS configured, and DAS uses the SSL port number, update the DAS URL entry in Oracle Internet Directory.

Note: You can find out what port DAS uses with the following command:

```
ORACLE_HOME/bin/ldapsearch -h oid_host -p oid_port -D "cn=orcladmin"
-w "password" -b "cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext"
-s base "objectclass=*" orcldasurlbase
```

1. Create a file named mod.ldif with the following contents (you can create the file in any directory):

```
dn:cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
changetype:modify
replace:orcldasurlbase
orcldasurlbase:https://hostname:new_https_port_number/
```

Note the slash at the end of the orcldasurlbase URL.

2. Run the following command:

```
ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w password -p oid_port -f
mod.ldif
```

3. Refresh the OID cache in your applications:
   a. Log in to the Portal.
   b. Click on the global settings link.
   c. Click the OID / DAS tab.
   d. Check the refresh OID cache settings and click Apply.

Step 9: Update Oracle Application Server Certificate Authority

If you are using OracleAS Certificate Authority:

1. Re-register OCA with the SSO server by running the following command in the OCA Oracle home:

```
ORACLE_HOME/oca/bin/ocactl changesecurity -server_auth_port port_number
```

   Where *port_number* is the OCA Server Authentication Virtual Host (SSL) port; the default is 4400.

   See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for more information

2. If OCA is located in a different Oracle home from the SSO server, restart Oracle HTTP Server and the oca instance in the OCA Oracle home:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl stopproc process-type=oca
opmnctl startproc ias-component=HTTP_Server
opmnctl startproc process-type=oca
```

Step 10: Restart the Identity Management Instance

Restart the Identity Management instance:

```
opmnctl stopall
opmnctl startall
```

Step 11: Restart OracleAS Certificate Authority

If OCA is configured in this instance, restart it:

```
ORACLE_HOME/oca/bin/ocactl start
```

Step 12: Update the Middle-Tier Instances to Use the New Port Number

On each middle-tier instance that uses the Identity Management installation, run the Change Identity Management Services wizard and start the instance:

1. On Application Server Control, navigate to the Application Server home page for the middle-tier instance.
2. Click the Infrastructure link.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the new Identity Management information (the new port number).
5. When the wizard is finished, navigate to the Application Server Home Page and start the middle-tier instance by clicking **Start All**.

5.6.4 Changing OracleAS Certificate Authority Ports

This section describes how to change the following port numbers:

- OracleAS Certificate Authority Server Authentication Virtual Host (SSL)
- OracleAS Certificate Authority Mutual Authentication Virtual Host (SSL)

To change either of these port numbers:

1. Edit the following file in the Oracle home of the Infrastructure that contains OracleAS Certificate Authority:

   ```
   ORACLE_HOME/Apache/Apache/conf/ocm_apache.conf
   ```

   a. Modify the Server or Mutual port, or both. Note that each port number is listed in the file in two places:

      – As a `Listen` directive

      – As a default virtual host

      The easiest way to find these is to search for the old port number.

   b. Save and close the file.

   c. Run the following command:

```
dcmctl updateConfig -ct ohs
```

2. Run the following command:

   ```
   sqlplus oca/oca_admin_password @$ORACLE_HOME/oca/sql/ocaportchg
   ```

   a. Enter the Server Authentication Only port when prompted. If you do not want to change this port number, enter the old port number.

   b. Enter the Mutual Authentication port when prompted. If you do not want to change this port number, enter the old port number.

3. Re-register OCA with the SSO server by running the following command in the OCA Oracle home:

   ```
   ORACLE_HOME/oca/bin/ocactl changesecurity -server_auth_port port_number
   ```

   Where *port_number* is the OCA Server Authentication Virtual Host (SSL) port; the default is 4400.

   See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for more information

4. Restart Oracle HTTP Server:

   ```
   opmnctl restartproc type=ohs
   ```

5. Restart the OCA OC4J instance:

   ```
   opmnctl restartproc type=oc4j instancename=oca
   ```

6. Start Oracle Application Server Certificate Authority:

   ```
   ORACLE_HOME/oca/bin/ocactl start
   ```

6

Managing an OracleAS Metadata Repository

This chapter provides information on managing an OracleAS Metadata Repository.

It contains the following topics:

6.1 Frequently Asked Questions About the Metadata Repository

The OracleAS Metadata Repository is an Oracle9*i* database and can be managed using standard database procedures and tools. However, there are some considerations for managing the Metadata Repository within the Oracle Application Server environment. This section answers frequently asked questions about managing the Metadata Repository.

- **What is a Metadata Repository?**

  A Metadata Repository is an Oracle9*i* Release 1 Enterprise Edition database. It is pre-seeded with schemas to support Oracle Application Server components and services.

  > **See Also:** Appendix D, "Metadata Repository Schemas" for information on the schemas that are pre-seeded in the Metadata Repository

- **When is a Metadata Repository required?**

  A Metadata Repository is required by the following installations:

  - An Identity Management installation requires a Metadata Repository for Identity Management schemas
  - A J2EE and Web Cache installation that is part of an OracleAS Cluster Managed using a Database Repository requires a Metadata Repository for the Management (DCM) schema
  - A Portal and Wireless installation requires a Metadata Repository for Product Metadata schemas
  - A Business Intelligence and Forms installation requires a Metadata Repository for Product Metadata schemas

- **How can I obtain a Metadata Repository?**

  You can obtain a Metadata Repository in either of the following ways:

  - You can install a Metadata Repository as part of an Infrastructure installation with Oracle Universal Installer. This installs the Metadata Repository from scratch.
  - You can install a Metadata Repository into an existing Oracle9*i* database using the Oracle Application Server Repository Creation Assistant (OracleAS RepCA).

See Also: *Oracle Application Server 10g Installation Guide*

- **Must the Metadata Repository be registered with Oracle Internet Directory?**

  It depends on what type of installation is using the Metadata Repository.

  A Metadata Repository must be registered with Oracle Internet Directory for the following installations:

  – Identity Management—the Metadata Repository must be registered with the Oracle Internet Directory within the Identity Management installation

  – Portal and Wireless—the Metadata Repository must be registered with the Oracle Internet Directory within the Identity Management installation used by the Portal and Wireless installation

  – Business Intelligence and Forms—the Metadata Repository must be registered with the Oracle Internet Directory within the Identity Management installation used by the Business Intelligence and Forms installation

  You have the option of registering the Metadata Repository with Oracle Internet Directory for a J2EE and Web Cache using OracleAS Single Sign-On—you may register the Metadata Repository with the Oracle Internet Directory in the Identity Management used by J2EE and Web Cache, or, you may use a free-standing Metadata Repository. Either one will allow you to use OracleAS Clusters Managed using a Database Repository.

- **Are there any tools for managing the Metadata Repository?**

  You can use Oracle Enterprise Manager, refer to Section 2.5, "Managing the OracleAS Metadata Repository Database".

- **Can I use the Metadata Repository to deploy applications?**

  No. The Metadata Repository is not intended for deploying applications.

- **Can a Metadata Repository coexist on a host with other databases?**

  Yes. As long as each database has a unique SID and global database identifier. The databases may be able to share a Net listener as follows:

  – Multiple Oracle9*i* databases can share the same Net listener port. So, if the other databases on your host are Oracle9*i* databases, the Metadata Repository can use the same Net listener port (for example. 1521) as the other databases.

  - If the other databases on your system are Oracle8*i* databases running Oracle Net8 listener, then the Metadata Repository must use a different port for its Net listener.

- **Can I change the character set of the Metadata Repository?**

  Yes. Follow the instructions for changing the character set in the database documentation, then refer to Section 6.3, "Changing the Character Set of the Metadata Repository" for updates you need to make to Oracle Application Server.

- **Can I tune the Metadata Repository?**

  Yes, you can apply database tuning strategies to the Metadata Repository.

  One important point to be aware of is that the processes and sessions parameters in the Oracle `init$SID.ora` configuration file should be tuned to allow the Metadata Repository to handle the maximum number of database sessions used by Oracle Application Server 10*g* middle-tier installations, or other middle-tier installations accessing the Metadata Repository.

  The primary consumers of database sessions are OracleAS Portal and OracleAS Wireless. An `init$SID.ora` setting of processes=150 should support four middle-tier installations that include these components. Note that an OracleAS Portal best practice recommendation is to relocate the Portal instance out of the Infrastructure, which would reduce the database connections requirement.

  > **See Also:** *Oracle Application Server 10g Performance Guide* for a detailed description of the database connection usage of `mod_plsql` in an OracleAS Portal installation

- **Can I change Metadata Repository schema passwords?**

  Yes. However, you must make sure to use the correct procedure. Some schemas store their passwords in Oracle Internet Directory and you must change their passwords using Application Server Control so the password is updated in Oracle Internet Directory and the database.

  > **See Also:** Section 6.2, "Changing Schema Passwords"

- **Can I delete schemas from the Metadata Repository that I am not using?**

  No. You should never delete any of the schemas that come with the Metadata Repository.

- **Can I rename or relocated Metadata Repository datafiles after installation?**

Yes.

See Also: Section 6.4, "Renaming and Relocating Datafiles"

- **Can I configure my Metadata Repository for high availability?**

  Yes. Oracle Application Server offers several high availability options for the Metadata Repository, including:

  – Oracle Application Server Cold Failover Cluster
  – Oracle Application Server Active Failover Cluster (Limited Release)
  – Oracle Application Server Disaster Recovery

  See Also: *Oracle Application Server 10g High Availability Guide*

- **Can I enable archive logging on the Metadata Repository?**

  Yes. This is part of the Oracle-recommended backup and recovery strategy.

  See Also: Section 13.2.1, "Enabling ARCHIVELOG Mode"

- **How can I backup and recover the Metadata Repository?**

  Oracle provides a backup and recovery strategy for your entire Oracle Application Server environment, including the Metadata Repository.

  See Also: Part IV, "Backup and Recovery"

6.2 Changing Schema Passwords

The method for changing schemas passwords in the Metadata Repository varies by schema. Some schemas store their passwords in Oracle Internet Directory; you must change their passwords using Application Server Control so that both Oracle Internet Directory and the database are updated. Other schemas do not store their passwords in Oracle Internet Directory; you can change their passwords in the database using SQL*Plus. A few schemas require special steps for changing their passwords.

Table 6–1 lists the appropriate method for change each Metadata Repository schema.

Table 6–1 Methods for Changing Metadata Repository Schema Passwords

Schema	Method for Changing Password
DCM	If the Metadata Repository is registered with Oracle Internet Directory, you must change the password in two places: ■ Use SQL*Plus to change the password directly in the database. Refer to Section 6.2.2, "Changing Schema Passwords Using SQL*Plus". ■ Manually change the password in Oracle Internet Directory. Refer to Section 6.2.3, "Viewing and Changing Schema Passwords in Oracle Internet Directory". If the Metadata Repository is not registered with Oracle Internet Directory, you only need to change the password directly in the database using SQL*Plus.
DISCOVERER5	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
DSGATEWAY	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
IP	You must change the password in two places: ■ Use SQL*Plus to change the password directly in the database. Refer to Section 6.2.2, "Changing Schema Passwords Using SQL*Plus". ■ Manually change the password in Oracle Internet Directory. Refer to Section 6.2.3, "Viewing and Changing Schema Passwords in Oracle Internet Directory".
OCA	This schema requires special steps. Refer to *Oracle Application Server Certificate Authority Administrator's Guide* for advanced topics in administration.
ODS	This schema requires special steps. Refer to *Oracle Internet Directory Administrator's Guide* for information on resetting the default password for the database.
ORAOCA_PUBLIC	This schema requires special steps. Refer to *Oracle Application Server Certificate Authority Administrator's Guide* for advanced topics in administration.

ORASSO	Use Application Server Control. Navigate to the Home Page for the Infrastructure (Identity Management) installation and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
	After you change the password, restart Oracle HTTP Server:
	`opmnctl stopproc ias-component=HTTP_Server`
	`opmnctl startproc ias-component=HTTP_Server`

ORASSO_DS	Use Application Server Control. Navigate to the Home Page for the Infrastructure (Identity Management) installation and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".

Table 6–1 (Cont.) Methods for Changing Metadata Repository Schema Passwords

Schema	Method for Changing Password
ORASSO_PA	Use Application Server Control. Navigate to the Home Page for the Infrastructure (Identity Management) installation and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
ORASSO_PS	Use Application Server Control. Navigate to the Home Page for the Infrastructure (Identity Management) installation and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control". Changing the ORASSO_PS password requires that the database link from all Portal schemas to the ORASSO_PS schema be recreated. To do this, run the following command for each affected Portal instance: `ORACLE_HOME/portal/conf/ptlconfig -dad dad_name -site` Refer to *Oracle Application Server Portal Configuration Guide*.
ORASSO_PUBLIC	Use Application Server Control. Navigate to the Home Page for the Infrastructure (Identity Management) installation and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
OWF_MGR	You must change the password in two places: ■ Use SQL*Plus to change the password directly in the database. Refer to Section 6.2.2, "Changing Schema Passwords Using SQL*Plus". ■ Manually change the password in Oracle Internet Directory. Refer to Section 6.2.3, "Viewing and Changing Schema Passwords in Oracle Internet Directory".

PORTAL	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
	
	After you change the password, restart Oracle HTTP Server:
	
	`opmnctl stopproc ias-component=HTTP_Server`
	`opmnctl startproc ias-component=HTTP_Server`

PORTAL_APP	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
PORTAL_DEMO	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
PORTAL_PUBLIC	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".

Table 6–1 (Cont.) Methods for Changing Metadata Repository Schema Passwords

Schema	Method for Changing Password
SCOTT	Use SQL*Plus to change the password directly in the database. Refer to Section 6.2.2, "Changing Schema Passwords Using SQL*Plus".
SYS	Use SQL*Plus to change the password directly in the database. Refer to Section 6.2.2, "Changing Schema Passwords Using SQL*Plus".
SYSTEM	Use SQL*Plus to change the password directly in the database. Refer to Section 6.2.2, "Changing Schema Passwords Using SQL*Plus".
UDDISYS	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
WCRSYS	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
WIRELESS	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
WK_TEST	Use SQL*Plus to change the password directly in the database. Refer to Section 6.2.2, "Changing Schema Passwords Using SQL*Plus".
WKPROXY	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".
WKSYS	Use Application Server Control. Navigate to the Home Page for the middle-tier instance that uses this schema and follow the instructions in Section 6.2.1, "Changing Schema Passwords Using Application Server Control".

6.2.1 Changing Schema Passwords Using Application Server Control

Some schemas store their passwords in Oracle Internet Directory. You must change their passwords using Application Server Control so the password is updated in both the database and Oracle Internet Directory.

To change a schema password using Application Server Control:

1. Depending on the schema, navigate to the home page for the middle-tier instance or the Infrastructure. Refer to Table 6–1 to determine which home page to use.
2. On the home page, click **Infrastructure**.
3. On the Infrastructure page, click **Change Schema Password**.

4. On the Change Schema Password page, select the radio button for the schema. Enter the new password in the Password and Confirm Password fields. Click **OK**.

6.2.2 Changing Schema Passwords Using SQL*Plus

You can change some schema passwords directly in the database using SQL*Plus. To do so, connect to the database as a user with SYSDBA privileges and issue the following command:

```
SQL> ALTER USER schema identified by new_password;
```

For example, to change the SCOTT schema password to "abc123":

```
SQL> ALTER USER SCOTT IDENTIFIED BY abc123;
```

6.2.3 Viewing and Changing Schema Passwords in Oracle Internet Directory

A few schemas (DCM, IP, OWF_MGR) require you to manually update the password in the Metadata Repository and in Oracle Internet Directory. You can use this procedure to change these passwords and to view any schema password in Oracle Internet Directory.

1. Start Oracle Directory Manager with the following command:

   ORACLE_HOME/bin/oidadmin

2. Log in to Oracle Directory Manager as the orcladmin user.
3. In the System Objects frame, expand **Entry Management**, expand **cn=OracleContext**, expand **cn=Products**, expand **cn=IAS**, expand **cn=IAS Infrastructure Databases**, and expand the orclReferenceName for the Metadata Repository.
4. Select the OrclResourceName entry for the schema whose password you want to change.
5. In the Properties tab, you can view and update the password in the orclpasswordattribute field.
6. Click Apply.

6.3 Changing the Character Set of the Metadata Repository

To configure the middle-tier and infrastructure to work with the metadata repository after its character set has been changed:

1. Modify the character set of all Database Access Descriptors (DADs) accessing the metadata repository to the new database character set.
   a. Using Application Server Control, navigate to the middle-tier instance home page.
   b. In the System Components section, click HTTP_Server.
   c. On the HTTP_Server home page, click Administration.
   d. On the HTTP_Server Administration page, select "PL/SQL Properties". This opens the `mod_plsql` Services page.
   e. Scroll to the DADs section and click the name of the DAD that you want to configure. This opens the Edit DAD page.
   f. In the NLS Language field, type in a NLS_LANG value whose character set is the same as the new character set for the metadata repository.
   g. Click OK.
   h. Repeat steps e to g for all DADs accessing the Metadata Repository.
2. Reconfigure the Ultra Search index, using the two SQL scripts provided for this purpose: `wk0prefcheck.sql` and `wk0idxcheck.sql` under `$ORACLE_HOME/ultrasearch/admin`.
   - `wk0prefcheck.sql` is invoked under `wksys` to reconfigure default cache character set and index preference.
   - `wk0idxcheck.sql` is needed for reconfiguring instance(s) created before database character set change, e.g., the default instance. This script must be invoked by the instance owner and `wk0prefcheck.sql` must be run first as it depends on reconfigured default settings generated by `wk0prefcheck.sql`.
   - Running `wk0idxcheck.sql` will also drop and recreate the Oracle Text index used by Ultra Search. So if there are already data source indexed then user must force recrawl all of the data sources.
   - Note that `wk0idxcheck.sql` must be run once for each instance. So if there are two instances "inst1" and "inst2" owned by "owner1" and "owner2"

respectively then wk0idxcheck.sql should be run twice; once by "owner1" and once by "owner2".

6.4 Renaming and Relocating Datafiles

When you install a Metadata Repository, you can choose the location for its datafiles. The default location is *ORACLE_HOME*/oradata/*SID*. After installation, you may want to relocate datafiles to a different directory. For example, you may want to move them to a directory on a filesystem with more space. Or, you may want to move them to a directory on a different disk for performance reasons. Another thing you may want to do is keep the datafiles in the same directory, but rename them.

This section provides a procedure for renaming or relocating datafiles. You can use this procedure on one or more datafiles, and the datafiles may be in multiple tablespaces.

This procedure applies to:

- The datafiles associated with Oracle Application Server schemas and tablespaces.

  See Also: Appendix D, "Metadata Repository Schemas"

- The following standard Oracle database datafiles:
  - drsys01.dbf
  - system01.dbf
  - temp01.dbf
  - users01.dbf

The following example shows how to relocate two datafiles in two different tablespaces, as follows:

- Relocate the oca.dbf datafile in the OCATS tablespace from /infra_home/oradata/asdb/oca.dbf to /new_directory/oca.dbf
- Relocate the dcm.dbf datafile in the DCM schema from /infra_home/oradata/asdb/dcm.dbf to /new_directory/dcm.dbf

Before you start the procedure:

- Make sure you have a complete cold backup of the Metadata Repository

- Connect to the Metadata Repository as a user with administrator privileges. You must have the ALTER DATABASE system privilege to relocate datafiles.
- Read through the entire procedure before you start.

The procedure is as follows:

1. Verify the location of your datafiles.

   You can verify the location of datafiles in a particular tablespace by querying the data dictionary view DBA_DATA_FILES.

   For example, to query the location of datafiles in the OCATS and DCM tablespaces:

```
SQL> SELECT FILE_NAME, BYTES FROM DBA_DATA_FILES
WHERE TABLESPACE_NAME = 'OCATS' OR TABLESPACE_NAME = 'DCM';

FILE_NAME                                          BYTES
---------------------------------------------------------
/infra_home/oradata/asdb/oca.dbf                78643200
/infra_home/oradata/asdb/dcm.dbf                96993280
```

2. Shut down all middle-tier instances that use the Metadata Repository.
3. Stop the Infrastructure that contains the Metadata Repository, then start a Metadata Repository instance and mount the database without opening it, as follows:

   a. Stop Application Server Control and OPMN-managed processes:

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
```

   b. Leave the Metadata Repository listener running.

   c. Stop the Metadata Repository instance:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> SHUTDOWN
```

   d. Start a Metadata Repository instance and mount the database without opening it:

```
SQL> STARTUP MOUNT
```

4. Move the datafiles to their new location using the operating system. For example:

```
(UNIX)
mv /infra_home/oradata/asdb/oca.dbf /new_directory/oca.dbf
mv /infra_home/oradata/asdb/dcm.dbf /new_directory/dcm.dbf

(Windows)
rename C:\infra_home\oradata\asdb\oca.dbf D:\new_directory\oca.dbf
rename C:\infra_home\oradata\asdb\dcm.dbf D:\new_directory\dcm.dbf
```

Note: You can execute an operating system command to copy a file by using the SQL*Plus HOST command.

5. Use ALTER DATABASE to rename the file pointers in the database's control file.

```
SQL> ALTER DATABASE
RENAME FILE       '/infra_home/oradata/asdb/oca.dbf',
                  '/infra_home/oradata/asdb/dcm.dbf'
TO                '/new_directory/oca.dbf',
                  '/new_directory/dcm.dbf';
```

   The new files must already exist; this statement does not create the files. Also, always provide complete filenames (including their full paths) to properly identify the old and new datafiles. In particular, specify the old datafile name exactly as it appears in the DBA_DATA_FILES view of the data dictionary.

6. Shut down the Metadata Repository, then perform a normal startup of the Infrastructure:

   a. Leave the Metadata Repository listener running.

   b. Shut down the Metadata Repository

      ```
      SQL> SHUTDOWN
      ```

   c. Start the Metadata Repository:

      ```
      SQL> STARTUP
      ```

   d. Start OPMN-managed processes and Application Server Control:

      ```
      ORACLE_HOME/opmn/bin/opmnctl startall
      ORACLE_HOME/bin/emctl start iasconsole
      ```

7. Start the middle-tier instances that use the Infrastructure.

8. Verify the new location of your datafiles.

```
SQL> SELECT FILE_NAME, BYTES FROM DBA_DATA_FILES
WHERE TABLESPACE_NAME = 'OCATS' OR TABLESPACE_NAME = 'DCM';

FILE_NAME                                          BYTES
---------------------------------------------------------
/new_directory/oca.dbf                             78643200
/new_directory/dcm.dbf                             96993280
```

9. Perform a complete cold backup of the Metadata Repository. After making any structural changes to a database, always perform an immediate and complete backup.

6.5 Specifying Segment Space Management When Creating Tablespaces

When you create a locally managed tablespace using the CREATE TABLESPACE statement, the SEGMENT SPACE MANAGEMENT clause allows you to specify how free and used space within a segment is to be managed. Your choices are:

- MANUAL—specifies that you want to use free lists for managing free space within segments. This is the default.
- AUTO—specifies that you want to use bitmaps to manage the free space within segments.

Most tablespaces in the Metadata Repository are created using MANUAL mode, with the following exceptions, which use AUTO mode:

- OLTS_ATTRSTORE
- OLTS_CT_STORE
- OLTS_DEFAULT

Therefore, it is important to follow these rules if you create a tablespace in preparation for importing a tablespace from a Metadata Repository:

- If you are creating the OLTS_ATTRSTORE, OLTS_CT_STORE, or OLTS_DEFAULT tablespace, include the SEGMENT SPACE MANAGEMENT AUTO clause in the creation statement.

  For example, to create the OLTS_DEFAULT tablespace of size 10M:

```
create tablespace OLTS_DEFAULT datafile
  'gdefault1_oid.dbf' size 10M
```

```
  reuse autoextend ON
  EXTENT MANAGEMENT LOCAL AUTOALLOCATE SEGMENT SPACE MANAGEMENT AUTO;
```

- If you are creating any other tablespaces, do not specify `SEGMENT SPACE MANAGEMENT AUTO`.

See Also: *Oracle9i Database Administrator's Guide*

Part III

Advanced Administration

This part describes advanced administration tasks that involve reconfiguring Oracle Application Server.

It contains the following chapters:

- Reconfiguring Application Server Instances
- Changing Infrastructure Services
- Changing Network Configurations
- Management Considerations for Recommended Topologies

7

Reconfiguring Application Server Instances

When you install Oracle Application Server, you choose an installation type and the components you would like to configure. For J2EE and Web Cache installations, you choose if you would like to use Infrastructure Services. After installation, you may want make some changes. You may want to add or delete components, or even change the installation type. Or, you may want to start using Infrastructure Services with your J2EE and Web Cache installation. This chapter describes how to make these types of changes.

It contains the following topics:

7.1 Expanding a Middle-Tier Installation

There are three types of middle-tier installations. The types are ordered in that each contains all of the components in the previous installation type, plus additional components. The installation types, in order from lowest to highest are:

- J2EE and Web Cache
- Portal and Wireless (Includes all components in J2EE and Web Cache)
- Business Intelligence and Forms (Includes all components in J2EE and Web Cache, Portal and Wireless)

When you install Oracle Application Server, you choose an installation type based on the components you require at the time. You may decide later that you would like to use additional components that are available in a higher installation type. For example, you may install a J2EE and Web Cache, and then decide later that you would like to use OracleAS Portal.

To accomplish this, you can expand your application server installation by installing a higher installation type in the same Oracle home using Oracle Universal Installer. Options for expanding a middle-tier installation are shown in Table 7–1.

Table 7–1 Options for Expanding a Middle-Tier Installation

You can expand this type of installation:	To this type of installation:	Result
J2EE and Web Cache	Portal and Wireless	■ If Web Cache is not already configured, it is automatically configured ■ You are given the option of configuring Portal and Wireless
J2EE and Web Cache	Business Intelligence and Forms	■ If Web Cache is not already configured, it is automatically configured ■ You are given the option of configuring Portal, Wireless, Discoverer, Forms, Reports, and Personalization
Portal and Wireless	Business Intelligence and Forms	■ You are given the option of configuring Discoverer, Forms, Reports, and Personalization

When you expand an installation:

- All of your current configured components are maintained

- The disk files for the additional components in the higher installation type are installed in your Oracle home
- You are given the option of configuring any of the additional components in the higher installation type

Additional Notes

- You cannot reduce an installation by installing a lower installation type in the same Oracle home. For example, you cannot install a J2EE and Web Cache installation in an Oracle home that contains a Portal and Wireless installation. If you would like to exclude certain components from your installation, you can disable them. Refer to Section 3.4, "Enabling and Disabling Components" for more information.
- You can only expand middle-tier installations; you cannot expand an Infrastructure installation.

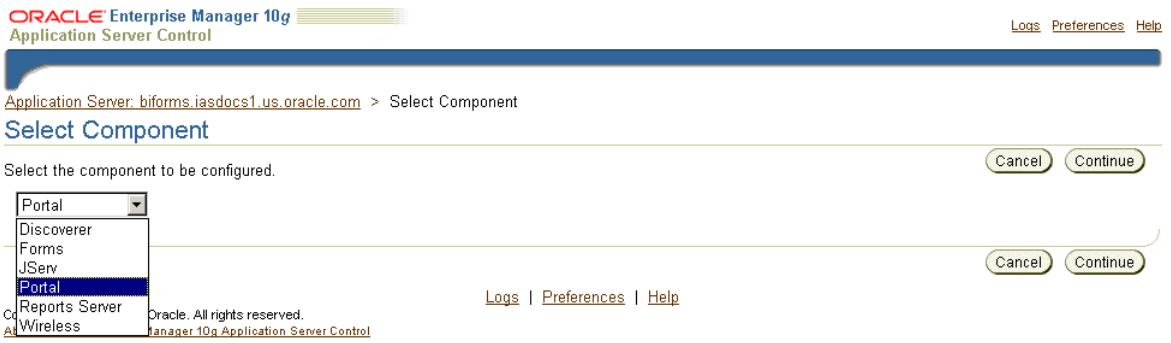
> **See Also:** *Oracle Application Server 10g Installation Guide* for complete instructions on expanding a middle-tier installation

7.2 Configuring Additional Components After Installation

When you install Oracle Application Server you are allowed to select the components you would like to configure. You may decide later you would like to configure one of the components you did not select during installation. For example, if you install J2EE and Web Cache and do not choose to configure Web Cache, you can configure Web Cache after installation.

You can configure components after installation using the Configure Component Page in Oracle Enterprise Manager Application Server Control, shown in Figure 7–1.

Figure 7–1 Configuring Component Page in Application Server Control



In addition to using Application Server Control to configure a component, there may be other information, manual steps, and verification steps you should be aware of. This section provides complete instructions for configuring and verifying components.

Table 7–2 lists which components can be configured after installation and provides pointers to the instructions.

Table 7–2 Components That Can Be Configured After Installation

You can configure this component after installation:	In these Installation Types:	For instructions, refer to:
JServ	J2EE and Web Cache Portal and Wireless Business Intelligence and Forms Infrastructure[1]	Section 7.2.1, "Configuring JServ After Installation"
Web Cache	2EE and Web Cache	Section 7.2.2, "Configuring Web Cache After Installation"
Portal	Portal and Wireless Business Intelligence and Forms	Section 7.2.3, "Configuring Portal After Installation"
Wireless	Portal and Wireless Business Intelligence and Forms	Section 7.2.4, "Configuring Wireless After Installation"

Table 7–2 (Cont.) Components That Can Be Configured After Installation

You can configure this component after installation:	In these Installation Types:	For instructions, refer to:
Discoverer	Business Intelligence and Forms	Section 7.2.5, "Configuring Discoverer After Installation"
Forms	Business Intelligence and Forms	Section 7.2.6, "Configuring Forms After Installation"
Reports Services	Business Intelligence and Forms	Section 7.2.7, "Configuring Reports After Installation"
Single Sign-On (SSO)	Infrastructure	Section 7.2.8, "Configuring Single Sign-On (SSO) After Installation"
Delegated Administration Service (DAS)	Infrastructure	Section 7.2.9, "Configuring Delegated Administration Service (DAS) After Installation"
Directory Integration and Provisioning (DIP)	Infrastructure	Section 7.2.10, "Configuring Directory Integration and Provisioning (DIP) After Installation"

[1] Configuring JServ in an Infrastructure is not recommended since applications are not deployed in the Infrastructure.

7.2.1 Configuring JServ After Installation

It is recommended that you use Oracle Application Server Containers for J2EE (OC4J) for your servlet environment—it is the default configuration for Oracle Application Server. However, you may want or need to use JServ in your Oracle Application Server installation. This section describes how to configure JServ after installation.

Things to Know Before You Start

During installation, Oracle Application Server assigns a port number to JServ. It writes the port number into the JServ configuration files, but leaves the lines commented out. So, even though JServ is not enabled, it does have a port number assigned to it.

You can find the port number by looking in the following file:

ORACLE_HOME`/install/portlist.ini`

It is listed as:

`Oracle HTTP Server Jserv port =` *`port_number`*

When you configure JServ, you will edit the configuration files. You can use the port number that was assigned, or choose a different port number. Just make sure to use a unique port number.

Configuring JServ

To configure JServ, you must perform manual steps and configure it in Application Server Control.

1. Perform manual steps to enable JServ.

   At a minimum, you must:

   a. Edit the following file:

      ORACLE_HOME/Apache/Apache/conf/httpd.conf

   b. Uncomment the following line (remove #):

      #include "*ORACLE_HOME*/Apache/Jserv/etc/jserv.conf"

   c. Save and close the file.

   There are additional directives and options you can manually configure for JServ.

   See Also: Refer to the `mod_jserv` section in *Oracle HTTP Server Administrator's Guide* for more details

2. Configure JServ in Application Server Control

   This step enables Application Server Control to display JServ as a configured component, and allows you to use the JServ Home Pages.

   a. Use Application Server Control to navigate to the Application Server home page for the instance in which you would like to configure JServ.

   b. On the Application Server home page, in the System Components section, click **Configure Component**.

   c. On the Select Component page, select **JServ** in the dropdown menu. Click **Continue**.

   d. On the Login page, in the Administration Password field, enter the `ias_admin` password. Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. Restart Oracle HTTP Server:

   ```
   ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=HTTP_Server
   ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=HTTP_Server
   ```

3. On the Application Server home page, verify that JServ is listed in the System Components section with an up status. It may take a few minutes for the JServ status and metrics to show up on Application Server Control.
4. Verify JServ is working by accessing the JServ demo at the following URL:

   ```
   http://hostname.domain:port_number/servlets/IsItWorking
   ```

   Where *hostname.domain* is the JServ host and *port_number* is the HTTP port number for the instance (default 7777).

   See Also: *Oracle HTTP Server Administrator's Guide* for more information on using JServ

7.2.2 Configuring Web Cache After Installation

This section describes how to configure Web Cache after installation.

Things to Know Before You Start

During installation, port numbers were reserved for Web Cache services. You can find the port numbers in the following file:

```
ORACLE_HOME/install/portlist.ini
```

They are listed as:

```
Web Cache HTTP Listen port = port_number
Web Cache HTTP Listen (SSL) port = port_number
Web Cache Administration port = port_number
Web Cache Invalidation port = port_number
Web Cache Statistics port = port_number
```

These port numbers will be used when you configure Web Cache. If you would like to use different port numbers, you can change them after you configure Web Cache.

Configuring Web Cache

1. Use Application Server Control to navigate to the Application Server home page for the instance in which you would like to configure Web Cache.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Web Cache** in the dropdown menu. Click **Continue**.
4. On the Login page, in the Administration Password field, enter the `ias_admin` password. Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. Verify that Web Cache is listed in the System Components section. It will have a down status. Select the checkbox next to Web Cache and click **Start**.
3. Verify that Web Cache shows an up status. Click the "Web Cache" instance and verify that the Web Cache Home Page is displayed.
4. On the Web Cache Home Page, in the Administration, click **Web Cache Administration**.
5. You can log in to the Web Cache Manager as either the `ias_admin` or `administrator` user. The password for both users is the `ias_admin` password you supplied during installation. If you have changed the `ias_admin` password since installation, you must still supply the original `ias_admin` password.

> **See Also:** *Oracle Application Server Web Cache Administrator's Guide* for a list of basic setup and configuration tasks

7.2.3 Configuring Portal After Installation

This section describes how to configure Portal after installation.

Configuring Portal

1. Use Application Server Control to navigate to the Application Server home page for the instance in which you would like to configure Portal.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Portal** in the dropdown menu. Click **Continue**.
4. On the Login page, in the Administration Password field, enter the `ias_admin` password. Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. Verify that OC4J_Portal and Portal:portal are listed in the System Components section. OC4J_Portal will have a down status and Portal:portal will have no status. Select the checkbox next to OC4J_Portal and click **Start**.
3. Verify that OC4J_Portal and Portal:portal have an up status. Click the OC4J_Portal instance and verify that the OC4J_Portal Page is displayed. Click the Portal:portal instance and verify that the Portal page is displayed.
4. If you perform this step, Portal is going write configuration entries into the Metadata Repository. This is fine if this is the first instance of Portal to use the Metadata Repository. However, if you already have Portal instances using the Metadata Repository, you should not perform this step, because you will overwrite the existing Portal configuration entries in the Metadata Repository.

   If this is the first instance of Portal to use the Metadata Repository, run the following command in the middle-tier Oracle home to write Portal configuration entries into the Metadata Repository:

   ```
   ORACLE_HOME/portal/conf/ptlconfig -dad portal
   ```

5. Verify that you can access Portal at the following URL:

   ```
   http://hostname.domain:port/pls/portal
   ```

Where *hostname.domain* is the Portal host and *port* is the Web Cache HTTP port number for the instance (default 7777).

You can log in to Portal as `portal`. Use the `ias_admin` password you supplied during middle-tier installation. If you have changed the `ias_admin` password, you must still supply the original `ias_admin` password.

> **See Also:** *Oracle Application Server Portal Configuration Guide* for more information on configuring and using Portal

7.2.4 Configuring Wireless After Installation

This section describes how to configure Wireless after installation.

Configuring Wireless

1. Use Application Server Control to navigate to the Application Server home page for the instance in which you would like to configure Wireless.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Wireless** in the dropdown menu. Click **Continue**.
4. On the Login page:
   - User Name: Enter `cn=orcladmin`, or the distinguished name of a user in the `iASAdmins` group.
   - Password: Enter the password for the user.
   - The SSL Only check box indicates if Wireless is enabled to access Oracle Internet Directory in SSL-mode only. It is grayed out because you cannot change this feature in this operation.

   Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. Verify that OC4J_Wireless and Wireless are listed in the System Components section. OC4J_Wireless and Wireless will have a down status. Select the checkboxes next to OC4J_Wireless and Wireless, and click **Start**.

3. Verify that OC4J_Wireless and Wireless have an up status. Click the OC4J_Wireless instance and verify that the OC4J_Wireless Page is displayed. Click the Wireless instance and verify that the Wireless page is displayed.
4. Verify that you can access Wireless at the following URL:

   `http://`*`hostname.domain`*`:`*`port`*`/webtool/login.uix`

   Where *`hostname.domain`* is the Wireless host and *`port`* is the Web Cache HTTP port number for the instance (default 7777).

   You can log in as `orcladmin` with the `orcladmin` password.

   See Also: *Oracle Application Server Wireless Administrator's Guide* for more information on configuring and using Wireless

7.2.5 Configuring Discoverer After Installation

This section describes how to configure Discoverer after installation.

Things to Know Before You Start

During installation, a port number was reserved for Discoverer. You can find the port number in the following file:

`ORACLE_HOME``/install/portlist.ini`

It is listed as:

`Discoverer OSAgent Port = `*`port_number`*

This port number will be used when you configure Discoverer. You cannot change the port number.

Configuring Discoverer

1. Use Application Server Control to navigate to the Application Server home page for the instance in which you would like to configure Discoverer.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Discoverer** in the dropdown menu. Click **Continue**.
4. On the Login page, in the Administration Password field, enter the `ias_admin` password. Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. If you did not have an OC4J_BI_Forms instance before, you will have one now. The OC4J_BI_Forms instance will have a down status. You will also have a Discoverer instance with a down status. Select the checkboxes next to OC4J_BI_forms and Discoverer, and click **Start**.
3. Verify that OC4J_BI_Forms and Discoverer have an up status. Click the OC4J_BI_Forms instance and verify that the OC4J_BI_Forms page is displayed. Click the Discoverer instance and verify that the Discoverer page is displayed.
4. Check that Discoverer services are up.

   For all of these URLs, *`hostname.domeain`* is the host Discoverer is on and *`port`* is the Web Cache HTTP port number (default 7777).

   a. Discoverer Viewer:

      `http://`*`hostname.domain`*`:`*`port`*`/discoverer/viewer`

   b. Discoverer Plus:

      `http://`*`hostname.domain`*`:`*`port`*`/discoverer/plus`

   c. Discoverer Portlet Provider:

      `http://`*`hostname.domain`*`:`*`port`*`/discoverer/portletprovider`

      See Also: *Oracle Application Server Discoverer Configuration Guide* for additional steps for configuring Discoverer, including installing Discoverer workbooks and End User Layer (EUL) into each database that contains data to be analyzed

7.2.6 Configuring Forms After Installation

This section describes how to configure Forms after installation.

Configuring Forms

1. Use Application Server Control to navigate to the Application Server home page for the instance in which you would like to configure Forms.
2. On the Application Server home page, in the System Components section, click **Configure Component**.

3. On the Select Component page, select **Forms** in the dropdown menu. Click **Continue**.
4. On the Login page:
   - User Name: Enter `cn=orcladmin`, or the distinguished name of a user in the `iASAdmins` group.
   - Password: Enter the password for the user.
   - The SSL Only check box indicates if Forms is enabled to access Oracle Internet Directory in SSL-mode only. It is grayed out because you cannot change this feature in this operation.

   Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. If you did not have an OC4J_BI_Forms instance before, you will have one now. The OC4J_BI_Forms instance will have a down status. You will also have a Forms instance with a down status. Select the checkbox next to OC4J_BI_Forms and click **Start**.
3. Verify that OC4J_BI_Forms and Forms have an up status. Click the OC4J_BI_Forms instance and verify that the OC4J_BI_Forms page is displayed. Click the Forms instance and verify that the Forms page is displayed.
4. Verify that you can access Forms at the following URL:

   `http://`*`hostname.domain`*`:`*`port`*`/forms90/f90servlet/admin`

   Where *`hostname.domain`* is the Forms host and *`port`* is the Web Cache HTTP port number (default 7777).

   Try to access the links on this page to verify that the Forms servlet is available.
5. Refer to the Forms online help for more information on configuring Forms. Specifically, note that if you would like to manage Forms runtime processes through Application Server Control, the entry "em_mode" in the default section of the Forms Web Configuration must be set to the value "1" (the default is "0"). Also, in order to view Forms trace output, the entry for "allow_debug" in that section should be set to "true".

See Also: *Oracle Application Server Forms Services Deployment Guide* for more information

7.2.7 Configuring Reports After Installation

This section describes how to configure Reports after installation.

Things to Know Before You Start

During installation, port numbers were reserved for Reports services. You can find the port numbers in the following file:

ORACLE_HOME/install/portlist.ini

They are listed as:

```
Reports Services SQL*Net port = port_number
Reports Services Visigenics CORBA port = port_number
```

These port numbers will be used when you configure Reports. If you would like to use a different SQL*Net port number, you can change it after you configure Reports. You cannot change the Visigenics CORBA port number.

Configuring Reports

1. Use Application Server Control to navigate to the Application Server home page for the instance in which you would like to configure Reports.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Reports Server** in the dropdown menu. Click **Continue**.
4. On the Login page:
   - User Name: Enter `cn=orcladmin`, or the distinguished name of a user in the `iASAdmins` group.
   - Password: Enter the password for the user.
   - The SSL Only check box indicates if Reports is enabled to access Oracle Internet Directory in SSL-mode only. It is grayed out because you cannot change this feature in this operation.

   Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. If you did not have an OC4J_BI_Forms instance before, you will have one now. The OC4J_BI_Forms instance will have a down status. You will also have a Reports Server:rep_*server* instance with a down status. Select the checkboxes next to OC4J_BI_forms and Reports Server: rep_*server* and click **Start**.
3. Verify that OC4J_BI_Forms and Reports Server: rep_*server* have an up status. Click the OC4J_BI_Forms instance and verify that the OC4J_BI_Forms page is displayed. Click the Reports Server: rep_*server* instance and verify that the Reports page is displayed.
4. Specify your outgoing mail server.
   a. Edit the following file:

      ORACLE_HOME/reports/conf/rep_*server*.conf

   b. Uncomment the `pluginParam name="mailServer"` element and update it with the outgoing mail server name. For example, change the following line:

      ```
      <!--pluginParam name="mailServer">%MAILSERVER_NAME%</pluginParam-->
      ```

      To:

      ```
      <pluginParam name="mailServer">smtpserver.myco.com</pluginParam>
      ```

   c. Save and close the file.
5. Verify that Reports is running with the following URL:

   `http://`*`hostname.domain`*`:`*`port`*`/reports/rwservlet/getserverinfo`

   Where *`hostname.domain`* is the Reports host and *`port`* is the Web Cache HTTP port number.

   You can log in as `orcladmin` with the `orcladmin` password.

   See Also: *Oracle Application Server Reports Services Publishing Reports to the Web* for more information on configuring and using Reports

7.2.8 Configuring Single Sign-On (SSO) After Installation

This section describes how to configure SSO after installation.

Configuring SSO

1. Use Application Server Control to navigate to the Application Server home page for the Infrastructure instance in which you would like to configure SSO.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Single Sign-On Server** in the dropdown menu. Click **Continue**.
4. On the Login page:
   - User Name: Enter `cn=orcladmin`, or the distinguished name of a user in the `iASAdmins` group.
   - Password: Enter the password for the user.
   - The SSL Only check box indicates if SSO is enabled to access Oracle Internet Directory in SSL-mode only. It is grayed out because you cannot change this feature in this operation.

   Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. If you did not have an OC4J_SECURITY instance before, you will have one now. The OC4J_SECURITY instance will have a down status. You will also have a Single Sign-On:orasso instance with a down status. Select the checkbox next to OC4J_SECURITY nd click **Start**.

   Note: You cannot start the Single Sign-On:orasso instance. This feature is started and stopped when you start and stop HTTP_Server and OC4J_SECURITY.
3. Verify that OC4J_SECURITY has an up status.

   Note: The Single Sign-On:orasso status may be displayed as down. This is normal. The metrics should be updated approximately five minutes after configuration.
4. Verify that you can access SSO at the following URL:

   `http://`*`hostname.domain`*`:`*`port`*`/pls/orasso`

Where *hostname.domain* is the host SSO is installed on and *port* is the Infrastructure HTTP Server port (default 7777).

You can log in as `orcladmin` with the `orcladmin` password.

> **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide* for more information on configuring and using SSO

7.2.9 Configuring Delegated Administration Service (DAS) After Installation

This section describes how to configure DAS after installation.

Things to Know Before You Start

When you configure DAS after installation using Application Server Control, the following happens:

- The URL for DAS is set up
- The appropriate privileges are created
- DAS services are deployed in the OC4J_SECURITY instance

Configuring DAS

1. Use Application Server Control to navigate to the Application Server home page for the Infrastructure instance in which you would like to configure DAS.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Delegated Administration Service** in the dropdown menu. Click **Continue**.
4. On the Login page:
   - User Name: Enter `cn=orcladmin`
   - Password: Enter the password for the user.
   - The SSL Only check box indicates if DAS is enabled to access Oracle Internet Directory in SSL-mode only. It is grayed out because you cannot change this feature in this operation.

   Click **Finish**.

Post-Configuration Tasks

1. When the configuration is finished, click **OK**. The Application Server home page will appear.
2. If you did not have an OC4J_SECURITY instance before, you will have one now. The OC4J_SECURITY instance will have a down status. Select the checkbox next to OC4J_SECURITY and click **Start**.
3. Verify that DAS is running by navigating to the following URL:

   `http://hostname.domain:port/oiddas`

   Where *`hostname.domain`* is the host DAS is installed on and *`port`* is the Infrastructure HTTP Server port (default 7777).

   See Also: *Oracle Internet Directory Administrator's Guide* for more information on configuring and using DAS

7.2.10 Configuring Directory Integration and Provisioning (DIP) After Installation

This section describes how to configure DIP after installation.

Configuring DIP

1. Use Application Server Control to navigate to the Application Server home page for the Infrastructure instance in which you would like to configure DIP.
2. On the Application Server home page, in the System Components section, click **Configure Component**.
3. On the Select Component page, select **Directory Integration and Provisioning** in the dropdown menu. Click **Continue**.
4. On the Login page:
   - User Name: Enter `cn=orcladmin`
   - Password: Enter the password for the user.
   - The SSL Only check box indicates if DIP is enabled to access Oracle Internet Directory in SSL-mode only. It is grayed out because you cannot change this feature in this operation.

   Click **Finish**.
5. When the configuration is finished, click **OK**. The Application Server home page will appear.

See Also: *Oracle Internet Directory Administrator's Guide* for more information on configuring and using DIP

7.3 Deconfiguring Components

You can configure components at the following times:

- During installation, by selecting the component on the Select Configuration Options screen on Oracle Universal Installer
- After installation, using the Configure Component page on Application Server Control
- When expanding an installation, by selecting the component on the Select Configuration Options screen on Oracle Universal Installer

Once you have configured a component, you cannot deconfigure it. An alternative is to disable the component, which prevents it from starting when you start your application server instance. It also removes the component from the System Components list on Application Server Control, and from the `opmnctl status` output.

See Also: Section 3.4, "Enabling and Disabling Components"

7.4 Deleting OC4J Instances

Guidelines for deleting OC4J instances are as follows:

- You cannot delete OC4J instances that were created by Oracle Application Server during installation.

  These include `home`, `OC4J_BI_Forms`, `OC4J_Portal`, `OC4J_Wireless`, `OC4J_SECURITY`, and `oca`. An alternative is to disable an OC4J instance, which prevents it from starting when your start your application server instance. It also removes the component from the System Components list on Application Server Control, and from the `opmnctl status` output.

  See Also: Section 3.4, "Enabling and Disabling Components"

- You can delete OC4J instances that were created by a user after installation.

  Deleting these instances removes all applications deployed to the instance. You can delete an OC4J instance using `dcmctl` or Application Server Control.

  To delete an OC4J instance using `dcmctl`:

```
ORACLE_HOME/dcm/bin/dcmctl removeComponent -co OC4J_instance_name
```

For example:

```
ORACLE_HOME/dcm/bin/dcmctl removeComponent -co OC4J_myapps
```

To delete an OC4J instance using Application Server Control:

1. Use Application Server Control to navigate to the Application Server home page for the instance that contains the OC4J instance.
2. In the System Components section, select the checkbox for the OC4J instance and click **Delete OC4J Instance**.

7.5 Configuring J2EE and Web Cache to Use Infrastructure Services

When you install a J2EE and Web Cache instance, you have the option of using the following Infrastructure Services:

- Identity Management

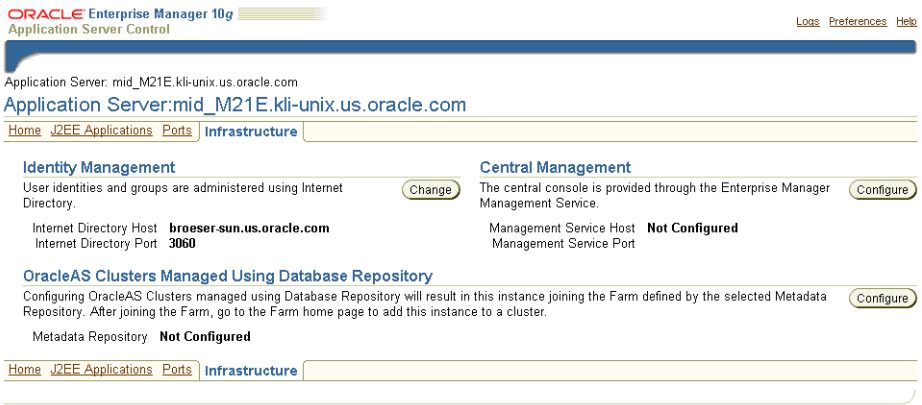
  This enables the J2EE and Web Cache instance to use Single Sign-On services.

- OracleAS Clusters Managed Using Database Repository

  This adds the J2EE and Web Cache instance to the farm of a specified Metadata Repository, thus enabling it to join an OracleAS Cluster Managed using a Database Repository.

If you did not choose the above options during installation, you can configure them after installation using the Infrastructure Page on Oracle Enterprise Manager Application Server Control, shown in Figure 7–2.

Figure 7–2 Application Server Control Infrastructure Page



This section contains the following procedures for configuring a J2EE and Web Cache instance to use Infrastructure services:

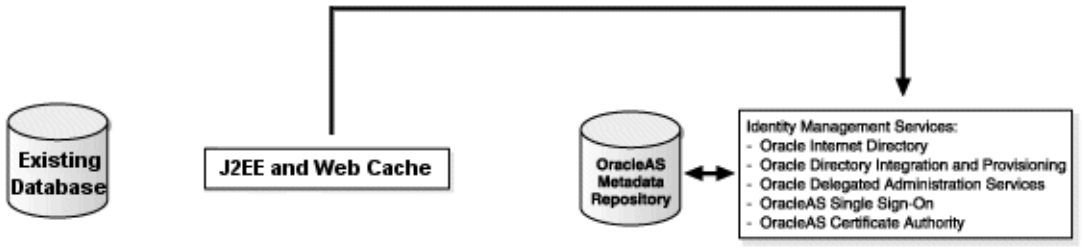
- To configure a J2EE and Web Cache instance to use Identity Management, refer to Section 7.5.1, "Using Identity Management".
- To configure a J2EE and Web Cache instance to use an OracleAS Metadata Repository, refer to Section 7.5.2, "Using an OracleAS Metadata Repository with Identity Management". Note that the instance must already use Identity Management.

- To configure a J2EE and Web Cache instance to use an Existing Database (a Metadata Repository that is not registered with OID), refer to Section 7.5.3, "Using an Existing Database". Note that the instance may or may not use Identity Management.
- If you have an Identity Management and OracleAS Metadata Repository, and would like to configure a J2EE and Web Cache instance to use the Metadata Repository only, you can follow the instructions in Section 7.5.4, "Using an OracleAS Metadata Repository without Identity Management". However, Oracle strongly recommends that you do not do this, but instead configure the instance to use Identity Management and then configure the instance to use the Metadata Repository using the instructions in Section 7.5.2, "Using an OracleAS Metadata Repository with Identity Management".

7.5.1 Using Identity Management

This section describes how to configure a J2EE and Web Cache instance to use Identity Management, as shown in Figure 7–3.

Figure 7–3 J2EE and Web Cache Using Identity Management



Before You Start

- Make sure the Identity Management instance is up.
- Make sure you know the Oracle Internet Directory host and port numbers.
- Make sure you know the password for `cn=orcladmin`, or another user that is a member of the `iASAdmins` group.

Procedure

1. Using Application Server Control, navigate to the Appilcation Server home page for the J2EE and Web Cache instance.
2. Click **Infrastructure**.
3. On the Infrastructure page, in the Identity Management section, click **Configure**.
4. On the Internet Directory page:
   - Host: Enter the fully-qualified name of the OID host.
   - Port: If you do not check "Use only SSL connections with Internet Directory", enter the non-SSL OID port number. Otherwise, enter the SSL OID port number.
   - Use only SSL connections with Internet Directory: By default, some middle-tier components connect to OID using non-SSL connections. If you want components to only connect to OID using SSL, check this box and make sure you entered the SSL OID port number in the Port field.

   Click **Next**.
5. On the Login page:
   - User Name: Enter `cn=orcladmin`, or the distinguished name of a user in the `iASAdmins` group.
   - Password: Enter the password for the user.

   Click **Next**.
6. On the Validation page, you will receive informational messages regarding the validation of this operation. If you receive any error message, follow the instructions for investigating them. Otherwise, if the operation is valid, click **Finish**.
7. When the operation is finished, you must restart the components in the J2EE and Web Cache instance.
   a. Click **Home** to navigate back to the J2EE and Web Cache Home Page.
   b. Click **Start All**.

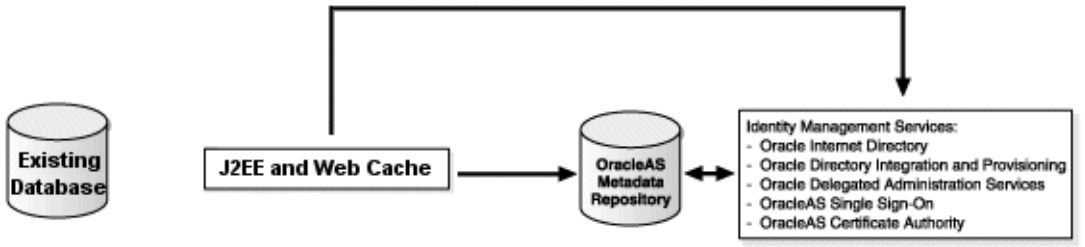
Your J2EE and Web Cache instance is now configured to use Identity Management services.

See Also: *Oracle Identity Management Concepts and Deployment Planning Guide* for more information

7.5.2 Using an OracleAS Metadata Repository with Identity Management

This section describes how to configure a J2EE and Web Cache instance to use an OracleAS Metadata Repository for OracleAS Clusters. This procedure requires that the J2EE and Web Cache instance is already using Identity Management, and the OracleAS Metadata Repository is registered with that Identity Management, as shown in Figure 7–4.

Figure 7–4 J2EE and Web Cache Using an OracleAS Metadata Repository (with Identity Management)



Before You Start

- Make sure the OracleAS Metadata Repository is up
- Make sure the Identity Management instance is up
- Make sure you know the password for `cn=orcladmin`, or another user that is a member of the `iASAdmins` group

Procedure

1. Using Application Server Control, navigate to the Appilcation Server home page for the J2EE and Web Cache instance.
2. Click **Infrastructure**.
3. On the Infrastructure page, in the OracleAS Clusters Managed Using Database Repository section, click **Configure**.
4. On the Source page, choose **OracleAS Metadata Repository**.

   Click **Next**.

5. On the Internet Directory page:

   - User Name: Enter `cn=orcladmin` or the distinguished name of a user in the `iASAdmins` group.
   - Password: Enter the password for the user.

   You will notice that "Use Only SSL connections with Internet Directory" is grayed out. This is because you cannot specify this option in this operation.

   Click **Next**.

6. On the Location page, select the OracleAS Metadata Repository you would like to use from the Repository dropdown list. The Default Schema is always DCM.

   Click **Next**.

7. On the Validation page, you will receive informational messages regarding the validation of this operation. If you receive any error message, follow the instructions for investigating them. Otherwise, if the repository you specified is valid, click **Finish**.

8. When the operation is finished, you must restart the components in the J2EE and Web Cache instance.

   a. Click **Home** to navigate back to the Application Server home page.

   b. Click **Start All**.

Your J2EE and Web Cache instance is now in the OracleAS Metadata Repository's farm and can join an OracleAS Cluster in that farm.

> **See Also:** *Oracle Application Server 10g High Availability Guide* for information on creating and using OracleAS Clusters

7.5.3 Using an Existing Database

This section describes how to configure a J2EE and Web Cache instance to use an Existing Database (a Metadata Repository that is not registered with OID) for OracleAS Clusters. The J2EE and Web Cache may use Identity Management, as shown in Figure 7–5, or it may not, as shown in Figure 7–6.

Figure 7–5 J2EE and Web Cache Using an Existing Database (with Identity Management)

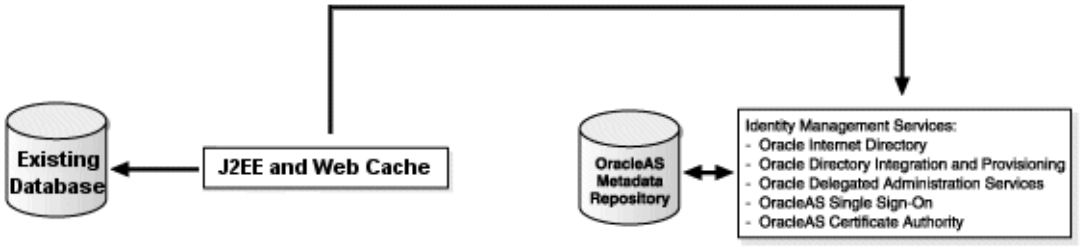


Figure 7–6 J2EE and Web Cache Using an Existing Database (without Identity Management)

Before You Start

- Make sure the Existing Database is up
- Make sure you know the Net listener port and the service name for the Existing Database. These are listed in the entry for the Existing Database in the following file:

  EXISTING_DB_ORACLE_HOME/network/admin/tnsnames.ora

- Make sure the DCM schema in the database is unlocked and that you know the password.

  If you have just installed the Existing Database and have not used the DCM schema yet, the DCM schema is locked and the password is expired. You must unlock it and set a new password as follows (be sure to set the ORACLE_HOME and ORACLE_SID environment variables first):

  ```
  ORACLE_HOME/bin/sqlplus "sys/SYS_PASSWORD as sysdba"
  SQL> alter user dcm identified by NEW_PASSWORD account unlock;
  ```

Procedure

1. Using Application Server Control, navigate to the Application Server home page for the J2EE and Web Cache instance.
2. Click **Infrastructure**.
3. On the Infrastructure page, in the OracleAS Clusters Managed Using Database Repository section, click **Configure**.
4. On the Source page, choose **Existing Database**. (Note: If the OracleAS Metadata Repository option is grayed out, it is because the J2EE and Web Cache instance is not using Identity Management).

   Click **Next**.
5. On the Login page, fill in the following fields:
   - User Name: `DCM`
   - Password: Enter the `DCM` schema password
   - Hostname and Port: Enter the hostname and Net listener port for the Existing Database. For example: `myhost:1521`.
   - Service Name: Enter the service name for the Existing Database. For example, `asdb.myco.com`.

   Click **Next**.
6. On the Validation page, you will receive informational messages regarding the validation of this operation. If you receive any error message, follow the instructions for investigating them. Otherwise, if the operation is valid, click **Finish**.
7. When the operation is finished, you must restart the components in the J2EE and Web Cache instance.
   a. Click **Home** to navigate back to the Application Server home page.
   b. Click **Start All**.

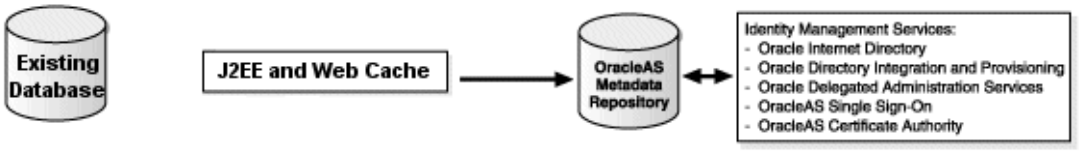
Your J2EE and Web Cache instance is now in the Existing Database's farm and can join an OracleAS Cluster in that farm.

7.5.4 Using an OracleAS Metadata Repository without Identity Management

This section describes how to configure a J2EE and Web Cache instance to use an OracleAS Metadata Repository for OracleAS Clusters. This procedure requires that

the J2EE and Web Cache instance is not using Identity Management, as shown in Figure 7–7.

Figure 7–7 J2EE and Web Cache Using an OracleAS Metadata Repository (without Identity Management)



Cauton: This configuration is not recommended. Instead Oracle recommends that you register the J2EE and Web Cache with Identity Management (see Section 7.5.1, "Using Identity Management") and then configure it to use the OracleAS Metadata Repository (see Section 7.5.2, "Using an OracleAS Metadata Repository with Identity Management").

Before You Start

- Make sure the OracleAS Metadata Repository is up
- Make sure you know the DCM schema password. If you do not know the password, you can obtain it from Oracle Internet Directory:

  ```
  ORACLE_HOME/bin/ldapsearch -h oid_host -p oid_port -D cn=orcladmin -w
  orcladmin_password -b "orclresourcename=DCM,
  orclreferencename=global_db_name, cn=ias infrastructure databases, cn=ias,
  cn=products, cn=oraclecontext" -s base "objectclass=*" orclpasswordattribute
  ```

  oid_host is the hostname of the Oracle Internet Directory the OracleAS Metadata Repository is registered with.

  oid_port is the non-SSL Oracle Internet Directory port number.

  global_db_name is the entry name for the OracleAS Metadata Repository in *ORACLE_HOME*/network/admin/tnsnames.ora. For example, asdb.myco.com.

- Make sure the Identity Management instance that the OracleAS Metadata Repository is registered with is up
- Make sure you know the password for `cn=orcladmin`, or another user that is a member of the `iASAdmins` group

Procedure

1. Using Application Server Control, navigate to the Application Server home page for the J2EE and Web Cache instance.
2. Click **Infrastructure**.
3. On the Infrastructure page, in the OracleAS Clusters Managed Using Database Repository section, click **Configure**.
4. On the Source page, choose **Existing Database**. (Note: The OracleAS Metadata Repository option is grayed out because the J2EE and Web Cache instance is not using Identity Management).

   Click **Next**.
5. On the Login page, fill in the following fields:
   - User Name: `DCM`
   - Password: Enter the `DCM` schema password
   - Hostname and Port: Enter the hostname and Net listener port for the Existing Database. For example: `myhost:1521`.
   - Service Name: Enter the service name for the Metadata Repository. For example, `asdb.myco.com`.

   Click **Next**.
6. On the Validation page, you will receive informational messages regarding the validation of this operation. If you receive any error message, follow the instructions for investigating them. Otherwise, if the operation is valid, click **Finish**.
7. When the operation is finished, you must restart the components in the J2EE and Web Cache instance.
   a. Click **Home** to navigate back to the Application Server home page.
   b. Click **Start All**.

Your J2EE and Web Cache instance is now in the OracleAS Metadata Repository's farm and can join an OracleAS Cluster in that farm.

8

Changing Infrastructure Services

This chapter provides procedures for changing the Infrastructure Services used by a middle-tier instance.

It contains the following topics:

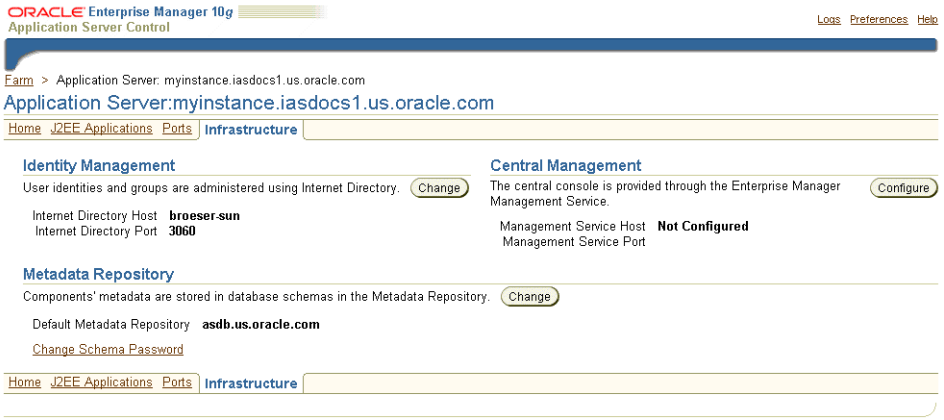
8.1 Overview of Procedures for Changing Infrastructure Services

Most middle-tier instances use Infrastructure Services, such as Identity Management Services and the Metadata Repository. These services are usually assigned during installation.

After installation, you may want to change the Infrastructure Services used by a middle-tier instance. For example, you may want to use an Identity Management Service on a different host. Or, you may want to use a different Metadata Repository.

You can change Infrastructure services using the Infrastructure Page on Oracle Enterprise Manager Application Server Control, shown in figure Figure 8–1. Notice that the page allows you to change the Identity Management or the Metadata Repository used by a middle-tier instance.

Figure 8–1 Application Server Control Infrastructure Page



You must change Infrastructure Services when you change any of the following:

- The HTTP Server (SSO) port number on an Identity Management installation
- The Oracle Internet Directory non-SSL or SSL port number
- The Oracle Internet Directory Mode (Dual-mode or SSL)
- The host that Identity Management or the OracleAS Metadata Repository resides on

You cannot simply use the wizard to change from one Infrastructure service to another. You must first perform manual tasks in order to create and prepare the new

Infrastructure service. This chapter provides the following supported procedures for changing Infrastructure services:

- Changing the OID or HTTP (SSO) Ports on Identity Management

  Use this procedure if you need to change the OID or HTTP listener ports on an Identity Management installation. In addition to changing the port numbers, you must update middle-tier instances with the new port information, which requires changing Infrastructure services.

- Changing Oracle Internet Directory from Dual Mode to SSL Mode

  Use this procedure if you would like to change the Oracle Internet Directory mode from non-SSL to SSL. In addition to changing the mode, you must update middle-tier instances with the new mode, which requires changing Infrastructure services.

- Moving Identity Management to a New Host

  Use this procedure if you would like to move your Identity Management installation, and its associated Metadata Repository, to a new host. After you perform the move, you must update middle-tier instances with the new host information for Identity Management, which requires changing Infrastructure services.

- Changing from a Test to a Production Environment

  This procedure describes how to set up an environment that allows you to develop and test applications in a test environment, then move them into a production environment.

- Changing the Metadata Repository Used by a Middle-Tier Instance

  Use this procedure if you would like to move the Metadata Repository used for product metadata by middle-tier instances to a new host.

8.2 Changing the OID or HTTP (SSO) Ports on Identity Management

If you would like to change the Oracle Internet Directory non-SSL or SSL port on an Identity Management installation, refer to Section 5.6.2, "Changing Oracle Internet Directory Ports".

If you would like to change the Oracle HTTP Server non-SSL or SSL listen port on an Identity Management installation, which effectively changes the SSO port, refer to Section 5.6.3, "Changing the HTTP Server (SSO) Port on Identity Management".

8.3 Changing Oracle Internet Directory from Dual Mode to SSL Mode

When you install Identity Management, you are asked to choose a mode for Oracle Internet Directory. The default mode is dual mode, which allows some components to access Oracle Internet Directory using non-SSL connections. During the installation, you can choose SSL mode, which specifies that all components must use SSL when connecting to the directory.

If you did not choose SSL mode during the installation, and would like to change to SSL mode after installation, you can follow the procedure in this section. It includes changing the mode of the Oracle Internet Directory, and updating middle-tier instances to use the new mode.

Task 1: Change the Oracle Internet Directory Mode

Perform this task on the Infrastructure that contains Oracle Internet Directory.

1. Create a file named `mod.ldif` that contains the following lines:

```
dn:cn=configset0,cn=osdldapd,cn=subconfigsubentry
changetype:modify
replace:orclsslenable
orclsslenable:1
```

2. Run the following command:

```
ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w orcladmin_passwd -p oid_port
-v -f mod.ldif
```

   oid_port is the non-SSL OID port. This is listed as `OIDport` in *ORACLE_HOME*`/config/ias.properties`.

3. Edit the following file:

   ORACLE_HOME`/network/admin/ldap.ora`

   a. Modify the following line to remove the non-SSL port number:

      `DIRECTORY_SERVERS=(`*myhost.myco.com*`::`*sslport*`)`

   b. Save and close the file.

4. Edit the following file:

   ORACLE_HOME`/config/ias.properties`

   a. Change the SSLOnly parameter as follows:

```
SSLOnly=true
```

b. Save and close the file.

5. Reconfigure SSO to communicate to OID in SSL mode:

a. Obtain the ORASSO schema password:

```
ORACLE_HOME/bin/ldapsearch -p oid_port -h hostname -D "cn=orcladmin" -w
orcladmin_password -b "orclresourcename=orasso,
orclreferencename=global_db_name, cn=ias infrastructure databases,
cn=ias, cn=products, cn=oraclecontext" -s base "objectclass=*"
orclpasswordattribute
```

oid_port is the non-SSL OID port. This is listed as `OIDport` in *ORACLE_HOME*`/config/ias.properties`.

global_db_name is the name of the entry for the Metadata Repository in *ORACLE_HOME*`/network/admin/tnsnames.ora`. For example: `asdb.myco.com`.

This command prints the ORASSO password in a line like the following:

```
orclpasswordattribute=LAetjdQ5
```

b. Change to the following directory:

```
cd ORACLE_HOME/sso/admin/plsql/sso
```

c. Run the following command:

```
sqlplus orasso/orasso_password @ssooconf.sql
```

Where ***orasso_password*** is the ORASSO schema password you obtained in the previous step.

The following prompts appear:

* Enter value for new_oid_host:

  Press return to move through this and similar attributes you do not need to change, and enter the new value for the attributes that have changed. When you reach the following prompt:

* Enter value for new_ldapusessl:

  Enter Y in this field, then press return. A message appears indicating that the value new_ldapusessl has been updated.

6. Restart the instance that contains Oracle Internet Directory.

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

Task 2: Change Middle-Tier Instances to Use SSL Mode

In each middle-tier instance, run the Change Identity Management wizard and restart the instance:

1. On Application Server Control, navigate to the Instance Home Page for the middle-tier instance.
2. Click **Infrastructure**.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. On the Internet Directory page:
   - Host: Enter the fully-qualified name of the OID host.
   - Port: Enter the SSL OID port number.
   - Use only SSL connections with Internet Directory: Check this box.

   Click **Next**.
5. On the Login page:
   - User Name: Enter `cn=orcladmin`, or the distinguished name of a user in the `iASAdmins` group.
   - Password: Enter the password for the user.

   Click **Next**.
6. On the Validation page, you will receive informational messages regarding the validation of this operation. If you receive any error message, follow the instructions for investigating them. Otherwise, if the operation is valid, click **Finish**.
7. When the operation is finished, you must restart the components in the middle-tier instance.
   a. Click **Home** to navigate back to the Instance Home Page.
   b. Click **Start All**.

8.4 Moving Identity Management to a New Host

This section provides a procedure for moving Identity Management to a new host. This procedure involves creating a replica (or copy) of the original Identity Management on a different host, along with its own new Metadata Repository, and then changing the middle-tier instance to use the new Identity Management.

Note: You cannot simply change a middle-tier instance from one Identity Management to another. The new Identity Management must be a replica of the original, created using the instructions in this procedure.

8.4.1 Sample Uses for this Procedure

The following are sample uses for this procedure:

- You have an existing Identity Management and associated Metadata Repository that is used by one or more middle-tier instances. Your organization intends to replace the current Identity Management host with a new system. You can use this procedure to create a replica of the Identity Management, along with its own Metadata Repository, and change your middle-tier instances to use the new Identity Management. You can then retire the original host.
- You would like to create a failover environment for your Identity Management. You can use this procedure to create a replica of the current Identity Management, along with its own Metadata Repository. You can keep the replica running so it stays in sync with the original Identity Management. You can perform regular exports of data in the original Metadata Repository and save them. In the event that you lose the original Identity Management, you can import the data to the new Metadata Repository, and change your middle-tier instances to use the new Identity Management. Refer to Section 8.4.5, "Strategy for Performing Failover with this Procedure" for more information.

8.4.2 Assumptions and Restrictions

- For both the original and new installations, the Identity Management and Metadata Repository can exist in the same Oracle home, or in separate Oracle homes (same or different host). If they are in separate Oracle homes, perform the operations on each in their own Oracle home.
- For both the original and new installations, the Identity Management components (SSO, OID, DAS, and DIP) may exist in the same Oracle home, or

may exist in separate Oracle homes (same or different host). If they exist in separate Oracle homes, perform the operations on each in their own Oracle home.

- The Metadata Repository used by middle-tier instances for product metadata is not affected by this procedure.
  - If the middle-tier instances use product metadata in the same Metadata Repository that the original Identity Management uses, they will continue to use that Metadata Repository after they have changed to the new Identity Management. If you want, you can change them to use a different Metadata Repository after you have finished moving Identity Management. Refer to Section 8.6, "Changing the Metadata Repository Used by a Middle-Tier Instance".
  - If the middle-tier instances use a separate Metadata Repository for product metadata, they will continue to use that Metadata Repository after they have changed to the new Identity Management.
- This procedure does not take OracleAS Certificate Authority into consideration.

  See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for information on updating OracleAS Certificate Authority when changing Identity Management services

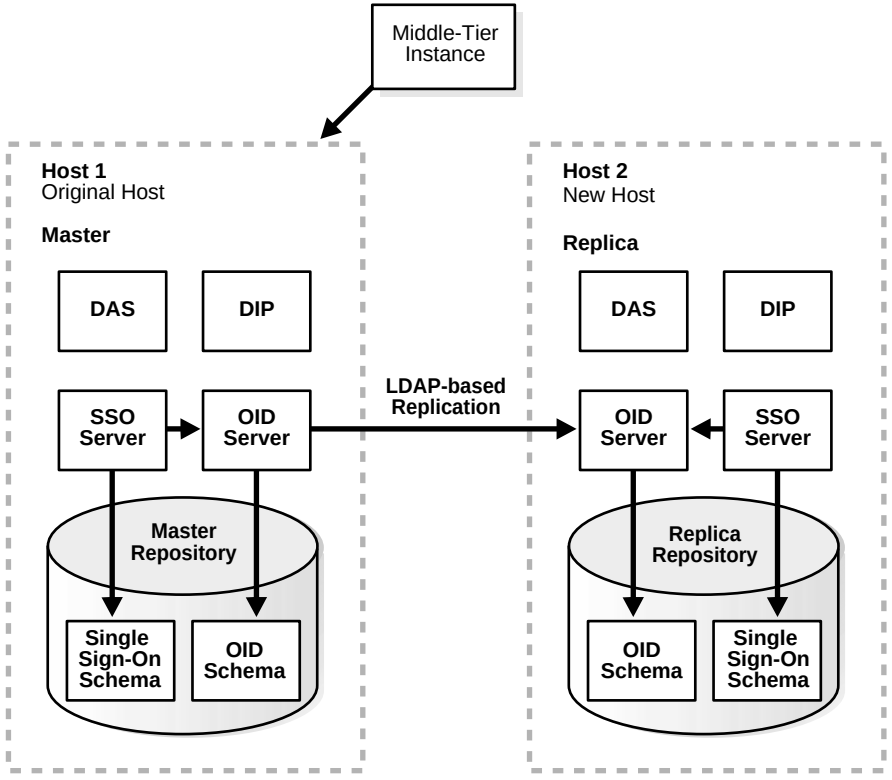
8.4.3 Overview

An overview of the procedure is as follows:

1. You have an original Identity Management (also called the Master) used by one or more middle-tier instances. The Identity Management has a Metadata Repository. You install and setup a new Identity Management (also called the Replica). This Identity Management has its own Metadata Repository. The Oracle Internet Directory in the new Identity Management is an LDAP-based Replica of the original OID. Replication takes place constantly from the original OID to the new OID.

   Figure 8–2 shows a sample of this setup.

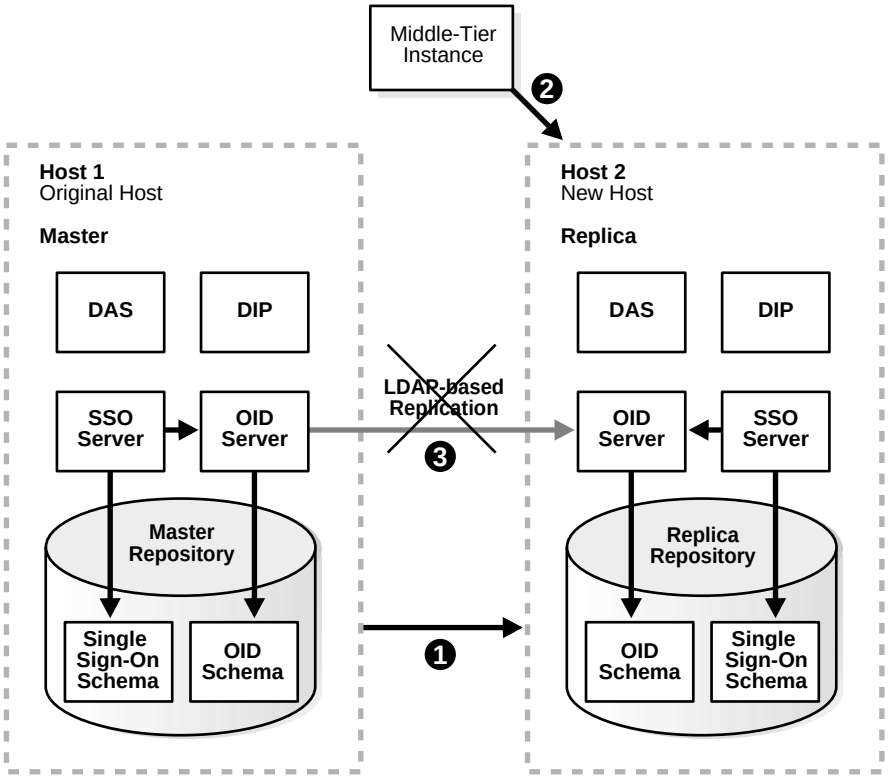
Figure 8–2 Original Host (Master) and New Host (Replica)



2. You perform the following steps to change to the new Identity Management. The steps are shown in Figure 8–3.

   - Step 1: Migrate SSO and DIP data from the original Metadata Repository (Master) to the new Metadata Repository (Replica)
   - Step 2: Change the middle-tier instances to use the new Metadata Repository.
   - Step 3: Stop the LDAP-based replication.

Figure 8–3 Changing from Original to New Identity Management



8.4.4 Procedure

This procedure contains the following tasks:

- Task 1: Install and Set Up the New Identity Management and Metadata Repository
- Task 2: Migrate SSO and DIP Data
- Task 3: Change Middle-Tier Instances to the New Identity Management
- Task 4: Stop Replication

Task 1: Install and Set Up the New Identity Management and Metadata Repository

In this task, you install and set up the new Identity Management and its associated Metadata Repository. The new Identity Management is an LDAP-based replica of the original Identity Management.

1. Read Section F.1, "About LDAP-based Replicas" to learn about LDAP-based Replicas and how they are used for this procedure.
2. Follow the procedure in Section F.2, "Installing and Setting Up an LDAP-based Replica" to install and set up the new Identity Management and Metadata Repository.

Task 2: Migrate SSO and DIP Data

In this task, you migrate the SSO and DIP data from the original Metadata Repository to the new Metadata Repository.

Follow the procedure in Section F.3, "Migrating SSO and DIP Data". The source for the migration is the original Metadata Repository (Master) and the target for the migration is the new Metadata Repository (Replica).

Task 3: Change Middle-Tier Instances to the New Identity Management

In each middle-tier instance, run the Change Identity Management wizard and restart the instance:

1. On Application Server Control, navigate to the Instance Home Page for the middle-tier instance.
2. Click **Infrastructure**.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the new Identity Management information.
5. When the wizard is finished, navigate to the Instance Home Page and start your instance by clicking **Start All**.

If you have a problem changing the middle-tier instances to the new host, check to make sure replication is running and try again.

Task 4: Stop Replication

Stop the replication between the original Identity Management and the new Identity Management (replica) by running the following command in the new Identity Management Oracle home:

```
ORACLE_HOME/bin/oidctl connect=global_db_name server=oidrepld instance=1
flags='-p oid_port' stop
```

global_db_name is the global db name of the new Identity Management. (This is referred to as *replica_db_name* in Section F.2.)

oid_port is the non-SSL OID port in the new Identity Management. (This is referred to as *replica_oid_port* in Section F.2.)

8.4.5 Strategy for Performing Failover with this Procedure

As mentioned in Section 8.4.1, "Sample Uses for this Procedure", you can modify this procedure to perform failover for Identity Management. This enables you to move your middle-tier instances to the new Identity Management in case the original is lost.

To perform failover:

1. Install and set up the new Identity Management as described in Task 1: Install and Set Up the New Identity Management and Metadata Repository.
2. Export SSO and DIP data on a regular basis from the original Metadata Repository. You do not need to import the data into the new Metadata Repository. You only need to export the data and copy the files to the new Metadata Repository Host. Refer to Section F.3, "Migrating SSO and DIP Data".
3. If you lose the original Identity Management:
   a. Stop replication. Refer to Task 4: Stop Replication.
   b. Import your most recent copy of the SSO and DIP data into the new Identity Management repository. Refer to Section F.3, "Migrating SSO and DIP Data".
   c. Change the middle-tier instances to use the new Identity Management. Refer to Task 3: Change Middle-Tier Instances to the New Identity Management.

8.5 Changing from a Test to a Production Environment

This section provides a procedure for changing from a test to production environment. This allows you to have a test environment for your applications, and then move your test applications and, optionally, test data into your production environment.

8.5.1 Sample Uses for this Procedure

The following are sample uses for this procedure:

- You have a production environment, and would like to create a test environment for developing and testing your applications. You would then like to roll out these applications to your production environment.
- You have a Oracle9*i*AS Release 2 (9.0.2/9.0.3) production environment, and would like to create an Oracle Application Server 10*g* (9.0.4) test environment to test your applications before upgrading.

  See Also: *Oracle Application Server 10g Upgrading to 10g (9.0.4)* for compatibility rules for different versions of Oracle9*i*AS and Oracle Application Server

8.5.2 Overview

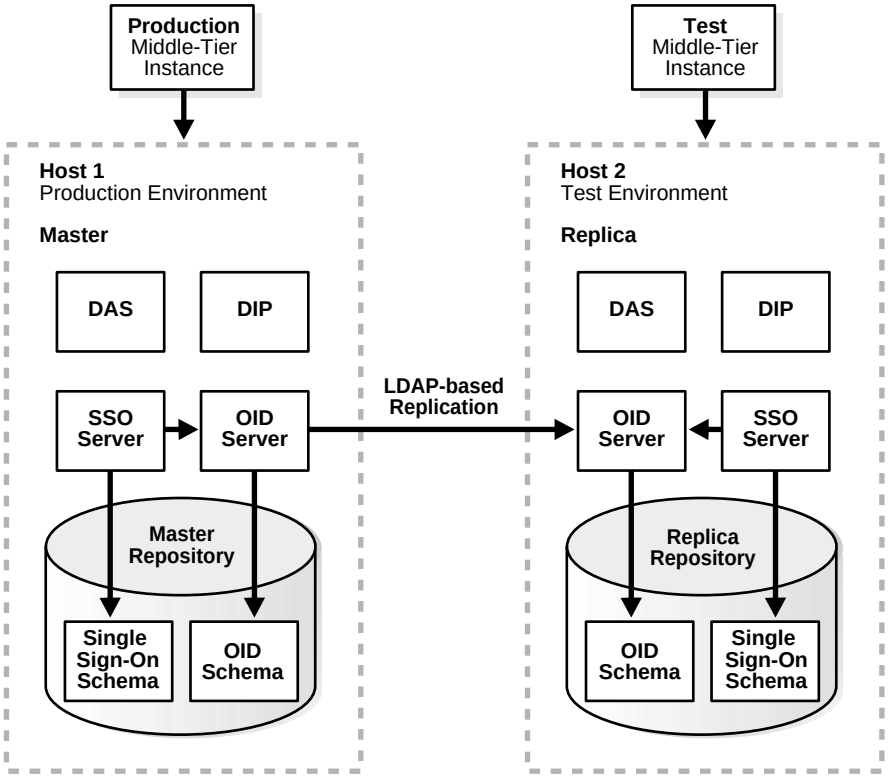
An overview of the procedure is as follows:

1. You have an existing production environment that includes middle-tier instances, an Identity Management installation with a Metadata Repository, and one or more Metadata Repositories used for product metadata.

   You create a test environment by installing and setting up a replica (or copy) of the production Identity Management. This Identity Management has its own Metadata Repository. The Oracle Internet Directory in the test Identity Management is an LDAP-based Replica of the production OID. Replication takes place constantly from the production OID to the test OID.This replica has its own Metadata Repository. You then install test middle-tier instances to use the test Identity Management. These middle-tier instances use a separate Metadata Repository for their product metadata. You can develop and test your applications in the test environment.

   Figure 8–4 shows a sample production and test environment.

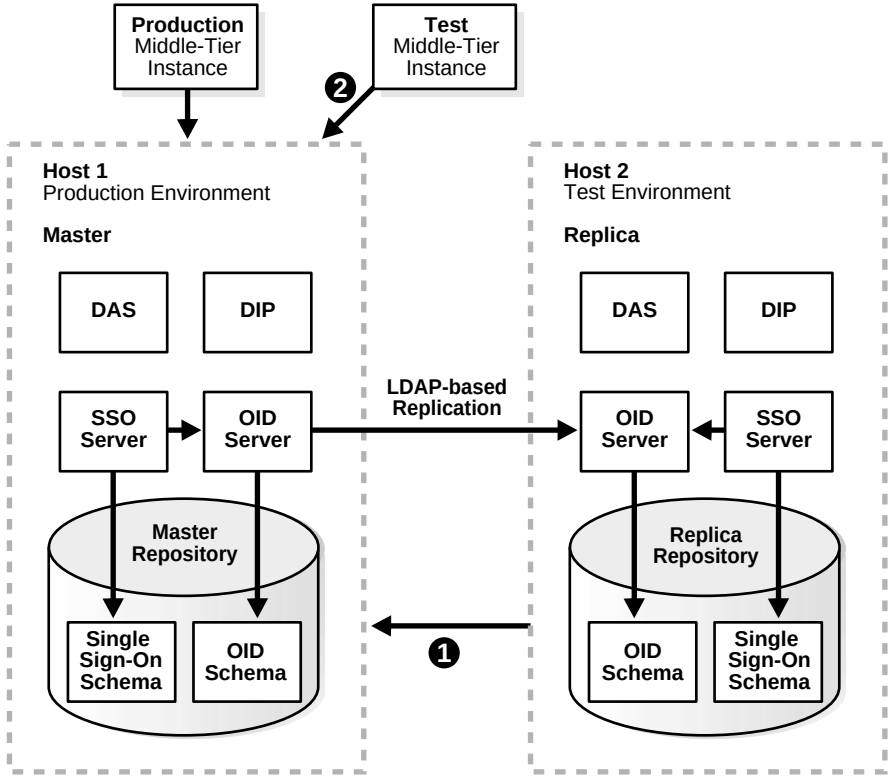
Figure 8–4 Production and Test Environment



2. When you are ready to roll out your test applications to your production environment, you perform the following steps. The steps are shown in Figure 8–5.

   - Step 1: Migrate data from the test environment to the production environment
   - Step 2: Change the test middle-tier instances to use the production environment.

Figure 8–5 Moving from Test to Production



3. You have several options for the test Metadata Repository used for product metadata:

- You can continue to use the test Metadata Repository in your production environment, thereby deeming it to be a production Metadata Repository.
- You can copy the Metadata Repository to a production host and change your middle-tier instances to use it.
- If you do not want to retain the test data in the Metadata Repository, you can install a new Metadata Repository in the production environment, and change the middle-tier instances to use that.
- You may have used a production Metadata Repository to begin with, in which case you can just continue to use that.

Note: You cannot copy parts of a product Metadata Repository to another Metadata Repository; you must copy the entire database. Therefore, it is not possible to migrate only some of your test product metadata to the production environment. You must copy the entire Metadata Repository. Refer to Section 8.6, "Changing the Metadata Repository Used by a Middle-Tier Instance".

8.5.3 Procedure

This procedure contains the following tasks:

- Task 1: Install and Set Up the Test Identity Management and Metadata Repository
- Task 2: Identify the Replica as a Pilot Replica
- Task 3: Start the Test Oracle Internet Directory in Pilot Mode
- Task 4: Install Test Middle-Tier Instances
- Task 5: Develop and Test Your Applications
- Task 6: Migrate Data from the Test to Production Environment
- Task 7: Change Middle-Tier Instances to the Production Identity Management
- Task 8: Move the Test Product Metadata Repository to Production
- Task 9: (Optional) Continue to Use Your Test Environment

Task 1: Install and Set Up the Test Identity Management and Metadata Repository

In this task, you install and set up the test Identity Management and its associated Metadata Repository. The test Identity Management is an LDAP-based replica of the original Identity Management.

1. Read Section F.1, "About LDAP-based Replicas" to learn about LDAP-based Replicas and how they are used for this procedure.
2. Follow the procedure in Section F.2, "Installing and Setting Up an LDAP-based Replica" to install and set up the test Identity Management and Metadata Repository.

Task 2: Identify the Replica as a Pilot Replica

Perform this task in the Oracle home of the test (replica) Oracle Internet Directory:

1. Create a file called `mod.ldif` that contains the following lines:

```
dn:orclreplicaid=replica_replicaid,cn=replication configuration
changetype:modify
replace:orclreplicatype
orclreplicatype:2
```

   Where ***replica_replicaid*** is the test (replica) replica ID you obtained in Section F.2, "Installing and Setting Up an LDAP-based Replica".

2. Run the following command:

```
ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w replica_orcladmin_passwd -p
replica_oid_port -v -f mod.ldif
```

   Where ***replica_orcladmin_passwd*** is the test (replica) `orcladmin` password and ***replica_oid_port*** is the test (replica) non-SSL OID port you obtained in Section F.2, "Installing and Setting Up an LDAP-based Replica".

Task 3: Start the Test Oracle Internet Directory in Pilot Mode

Perform this task in the Oracle home of the test (replica) Oracle Internet Directory:

1. Create a file called `mod.ldif` that contains the following lines:

```
dn:orclreplicaid=replica_replicaid,cn=replication configuration
changetype:modify
replace:orclpilotmode
orclpilotmode:1
```

   Where ***replica_replicaid*** is the test (replica) replica ID you obtained in Section F.2, "Installing and Setting Up an LDAP-based Replica".

2. Run the following command:

```
ORACLE_HOME/bin/ldapmodify -D cn=orcladmin -w replica_orcladmin_passwd -p
replica_oid_port -v -f mod.ldif
```

   Where ***replica_orcladmin_passwd*** is the test (replica) `orcladmin` password and ***replica_oid_port*** is the test (replica) non-SSL OID port you obtained in Section F.2, "Installing and Setting Up an LDAP-based Replica".

3. Restart OID on the test (replica) node:

```
ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OID
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OID
```

Task 4: Install Test Middle-Tier Instances

Install your test middle-tier instances and configure them to use the test Identity Management. You should use a separate Metadata Repository for the product metadata.

Task 5: Develop and Test Your Applications

Develop and test application in your test environment.

Task 6: Migrate Data from the Test to Production Environment

When you are ready to move your applications from your test to production environment, you must migrate data.

Follow the procedure in Section F.4, "Migrating Oracle Internet Directory Data".

Task 7: Change Middle-Tier Instances to the Production Identity Management

In each middle-tier instance, run the Change Identity Management wizard and restart the instance:

1. On Application Server Control, navigate to the Instance Home Page for the middle-tier instance.
2. Click **Infrastructure**.
3. On the Infrastructure Page, in the Identity Management section, click **Change**.
4. Follow the steps in the wizard for supplying the production Identity Management information.
5. When the wizard is finished, navigate to the Instance Home Page and start your instance by clicking **Start All**.

Task 8: Move the Test Product Metadata Repository to Production

You have several options for moving your test product Metadata Repository to your production environment:

- You can continue to use the test Metadata Repository in your production environment, thereby deeming it to be a production Metadata Repository.

  In this case, no further action is required.

- You can copy the Metadata Repository to a production host and change your middle-tier instances to use it.

  Follow the procedure in Section 8.6, "Changing the Metadata Repository Used by a Middle-Tier Instance".

- If you do not want to retain the test data in the Metadata Repository, you can install a new Metadata Repository in the production environment, and change the middle-tier instances to use that.

  Install an Infrastructure using Oracle Universal Installer. Select the Metadata Repository only option. Register the Metadata Repository with the production Identity Management.

  Change each of the former test middle-tier instances to use the new Metadata Repository. On each middle-tier instance:

  1. On Application Server Control, navigate to the Instance Home Page for the middle-tier instance.
  2. Click **Infrastructure**.
  3. On the Infrastructure Page, in the Metadata Repository section, click **Change**.
  4. Follow the steps in the wizard for supplying the new Metadata Repository information.
  5. When the wizard is finished, navigate to the Instance Home Page and start your instance by clicking **Start All**.

Task 9: (Optional) Continue to Use Your Test Environment

You can continue to use your test environment by installing new middle-tier instances against the test Identity Management.

8.6 Changing the Metadata Repository Used by a Middle-Tier Instance

This section provides a procedure for changing the Metadata Repository used by a middle-tier instance. This procedure involves making a copy of the original Metadata Repository on a different host, and then changing the middle-tier instance to use the new Metadata Repository.

Note: You cannot simply change a middle-tier instance from one Metadata Repository to another. The new Metadata Repository must be a copy of the original, created using the instructions in this procedure.

8.6.1 Sample Uses for this Procedure

The following are sample uses for this procedure:

- You have an existing Metadata Repository that is used by one or more middle-tier instances. Your organization intends to replace the current Metadata Repository host with a new system. You can use this procedure to copy the Metadata Repository to the new host and change your middle-tier instances to use the new Metadata Repository. You can then retire the original host.
- You would like to move a Metadata Repository from a host in your test environment, to a host in your Production Environment. You can use this procedure to copy the Metadata Repository from the test to production host, and change your test middle-tier instances to use the new Metadata Repository.

8.6.2 Assumptions and Restrictions

- The middle-tier instances must use Identity Management
- That Identity Management must not use the original Metadata Repository for its Identity Management schemas; it must use a separate Metadata Repository
- The original Metadata Repository:
  - Must be used for product metadata and DCM management only (it cannot be used by Identity Management)
  - Must be registered with Oracle Internet Directory
- The new Metadata Repository:
  - Must not be registered with OID initially. During the procedure, you will register it with the same OID as the original Metadata Repository.

  - Must be created with the same Oracle home, datafile location, SID, and global database name as the original Metadata Repository. You will eventually change the global database name to a unique name.

- This procedure does not take OracleAS Certificate Authority into consideration.

  See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for information on updating OracleAS Certificate Authority when changing Metadata Repository services

- If the Metadata Repository is used for OracleAS Clusters, the cluster members will not be accessible until all members of the cluster have been changed over to the new Metadata Repository.

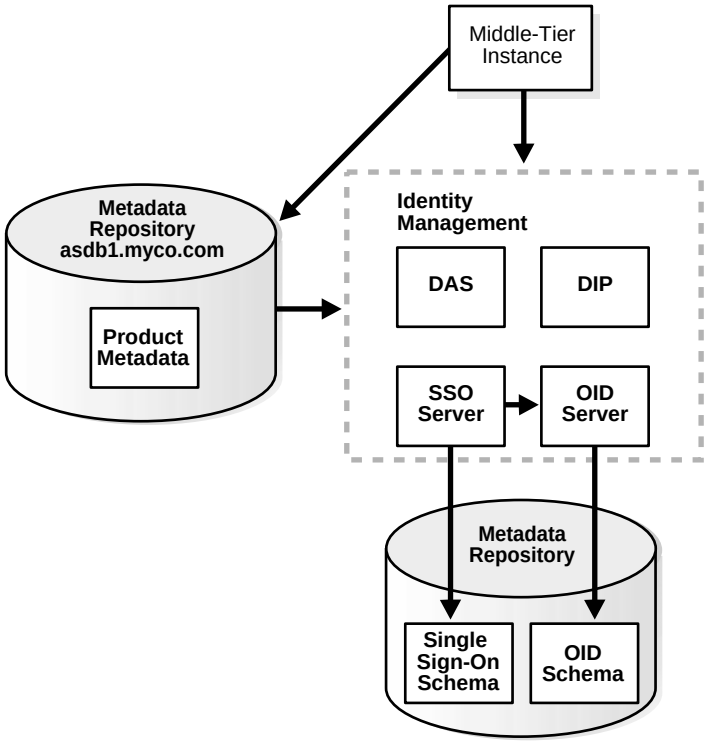
8.6.3 Overview

An overview of the procedure is as follows:

1. You have an original Metadata Repository. It is used by one or more middle-tier instances for product metadata. The middle-tier instances use Identity Management, and the Metadata Repository is registered with Oracle Internet Directory in that Identity Management.

   Figure 8–6 shows a sample original Metadata Repository (`asdb1.myco.com`).

Figure 8–6 Original Metadata Repository



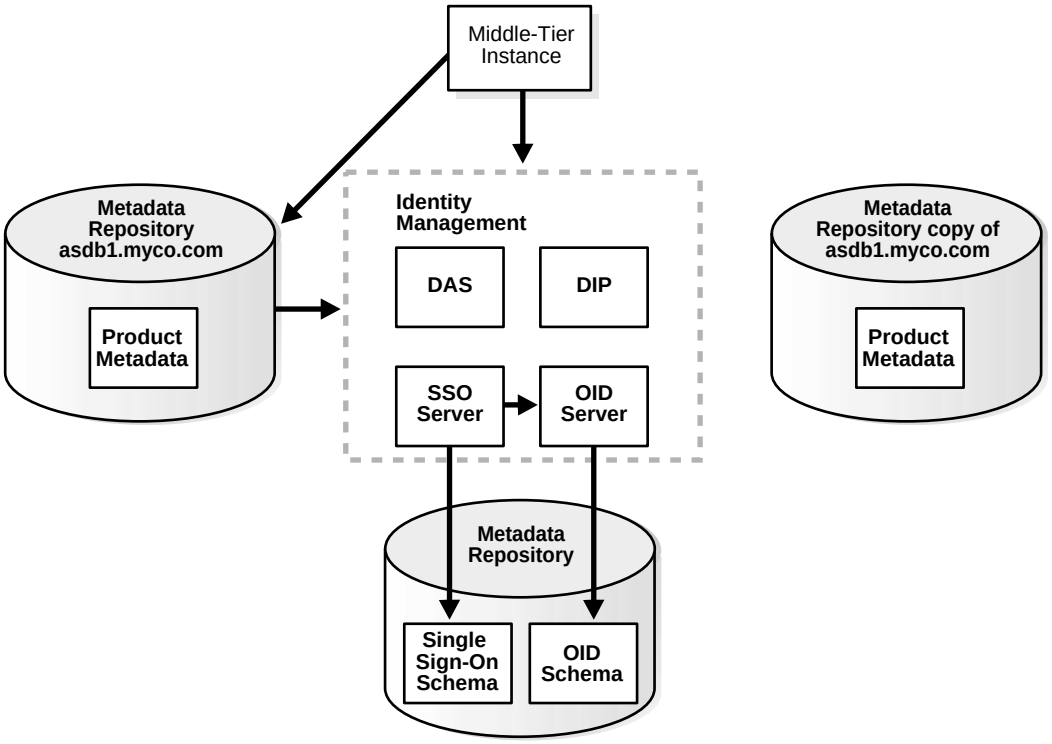
The following table shows sample attributes for the original Metadata Repository:

Attribute	Original Metadata Repository	New Metadata Repository
Oracle home	`/private/oraHome`	N/A
Datafile location	`/private/oraHome/oradata`	N/A
SID	`asdb1`	N/A
Global db name	`asdb1.myco.com`	N/A
Registered with OID?	Yes	N/A

2. You create a copy of the original Metadata Repository by installing a new Metadata Repository, backing up the original Metadata Repository, and restoring to the new Metadata Repository.

Figure 8–7 shows sample original and new Metadata Repositories.

Figure 8–7 Original Metadata Repository and New Metadata Repository

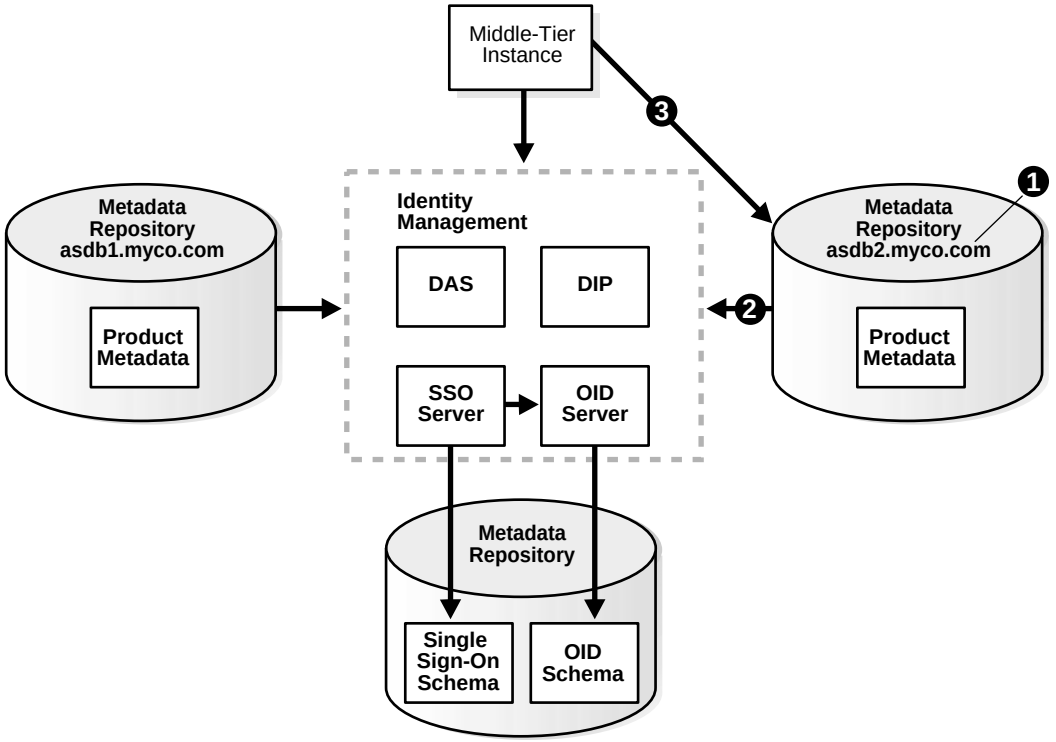


The following table shows sample attributes for the original and new Metadata Repositories:

Attribute	Original Metadata Repository	New Metadata Repository
Oracle home	`/private/oraHome`	`/private/oraHome`
Datafile location	`/private/oraHome/oradata`	`/private/oraHome/oradata`
SID	`asdb1`	`asdb1`
Global db name	`asdb1.myco.com`	`asdb1.myco.com`
Registered with OID?	Yes	**No**

3. You perform the following steps to change to the new Metadata Repository. The steps are shown in Figure 8–8.
   - Step 1: Change the global db name of the new Metadata Repository to a unique name (in this sample, `asdb2.myco.com`).
   - Step 2: Register the new Metadata Repository with the same Oracle Internet Directory as the old Metadata Repository.
   - Step 3: Change the middle-tier instances to use the new Metadata Repository.

Figure 8–8 Changing from the Original to the New Metadata Repository



The following table shows sample attributes for the original and new Metadata Repositories after performing the change:

Attribute	Original Metadata Repository	New Metadata Repository
Oracle home	`/private/oraHome`	`/private/oraHome`
Datafile location	`/private/oraHome/oradata`	`/private/oraHome/oradata`
SID	`asdb1`	`asdb1`
Global db name	`asdb1.myco.com`	**`asdb2.myco.com`**
Registered with OID?	Yes	**Yes**

4. If you are using the scenario where you no longer require the original Metadata Repository, you can discard the original Metadata Repository.

8.6.4 Procedure

This procedure contains the following tasks:

- Task 1: Install the New Metadata Repository
- Task 2: Back Up the Original Metadata Repository
- Task 3: Restore the Backup to the New Metadata Repository
- Task 4: Configure Ultra Search Metadata in the New Metadata Repository
- Task 5: Change the Global DB Name for the New Metadata Repository
- Task 6: Register the New Metadata Repository with OID
- Task 7: Change Middle-Tier Instances to the New Metadata Repository

Before You Begin

If your middle-tier instances use OracleAS Portal and Oracle Ultra Search, you will need to supply the `WKSYS` schema password later in this procedure in Task 4: Configure Ultra Search Metadata in the New Metadata Repository. You should obtain this password now from the old Metadata Repository.

Task 1: Install the New Metadata Repository

Install the new Metadata Repository as follows:

1. Make sure to install the Metadata Repository into an Oracle home that has the same path as the old Metadata Repository Oracle home
2. Use Oracle Universal Installer to install the Metadata Repository

3. Choose to install an Infrastructure
4. Choose to install a Metadata Repository only
5. Do not register the Metadata Repository with OID
6. Specify the same SID and global db name as the old Metadata Repository
7. Specify the same datafile location as the old Metadata Repository

Task 2: Back Up the Original Metadata Repository

In this task, you create a backup of the original Metadata Repository. This task provides the steps for doing this using RMAN, however, if you are an experience DBA, you can back up the Metadata Repository according to your standard practices.

Perform all of the steps in this task on the original Metadata Repository host.

1. Create directories to store backup files and log files. For example:

```
mkdir -p BACKUP_DIR/log_files
mkdir -p BACKUP_DIR/db_files
```

2. Make sure the original Metadata Repository is up and running.
3. Make sure you have set the `ORACLE_HOME` and `ORACLE_SID` environment variables you run the SQL*Plus command.
4. Obtain the DBID of the original Metadata Repository using SQL*Plus:

```
SQL> SELECT DBID FROM v$database;
```

   Make note of this value; you will use it later in the procedure.

5. Create a file named *`BACKUP_DIR`*`/cold_backup.rcv` that contains the following lines. In the file, substitute the full path for *`BACKUP_DIR`*.

```
shutdown immediate;
startup mount;
configure controlfile autobackup on;
configure controlfile autobackup format for device type disk to
'BACKUP_DIR/db_files/%F';

run {
allocate channel dev1 device type disk format
'BACKUP_DIR/db_files/%U';
backup database plus archivelog;
release channel dev1;
```

```
}
```

6. Run RMAN to back up the Metadata Repository (the following is a single command; type it all on one line):

```
ORACLE_HOME/bin/rman target /
cmdfile=BACKUP_DIR/cold_backup.rcv > BACKUP_DIR/log_files/backup.log
```

7. Copy the backup directories to the new host. You do not need to use the same path for *BACKUP_DIR* on the new host.

```
BACKUP_DIR/log_files
BACKUP_DIR/db_files
```

Task 3: Restore the Backup to the New Metadata Repository

In this task you restore the backup to the new Metadata Repository.

Perform all of the steps in this task on the new Metadata Repository host.

1. Make sure the new Metadata Repository is down:

```
sqlplus "sys/SYS_PASSWORD as sysdba"
SQL> shutdown immediate;
```

2. Regenerate the password file:

```
prompt> mv ORACLE_HOME/dbs/orapwORACLE_SID
ORACLE_HOME/dbs/orapwORACLE_SID.old
prompt> ORACLE_HOME/bin/orapwd file=ORACLE_HOME/dbs/orapwORACLE_SID
password=new_password
```

   new_password is the new SYS password. You can use the old SYS password, or set it to a new password.

3. Start the new Metadata Repository but do not mount it:

```
SQL> startup nomount;
```

4. Create a file named *BACKUP_DIR*/restore.rcv that contains the following lines. In the file, substitute the full path for *BACKUP_DIR* and the *DBID* obtained in the previous task.

```
set dbid=DBID;
connect target /;
set controlfile autobackup format for device type disk to
'BACKUP_DIR/db_files/%F';
restore controlfile from autobackup;
```

```
startup mount force;

run {
allocate channel dev1 device type disk format
'BACKUP_DIR/db_files/%U';
restore database;
release channel dev1;
alter database open resetlogs;
}
```

5. Run RMAN to restore the Metadata Repository:

   ```
   prompt> ORACLE_HOME/bin/rman cmdfile=BACKUP_DIR/restore.rcv >
   BACKUP_DIR/log_files/restore.log
   ```

6. After you restore using RMAN, determine if the TEMP tablespace has a datafile by running the following command in SQL*Plus:

   ```
   SQL> select file_name from dba_temp_files where tablespace_name like 'TEMP';
   ```

   If the preceding command does not return any files, add a datafile:

   ```
   SQL> alter tablespace "TEMP" add tempfile
   'ORACLE_HOME/oradata/GDB/temp01.dbf' size 5120K autoextend on next 8k
   maxsize unlimited;
   ```

   GDB is the first part of the global database name.

   Note that the above command creates a file called `temp01.dbf` and adds it to the TEMP tablespace. If the `temp01.dbf` file already exists in the directory, add a "reuse" clause to the command:

   ```
   SQL> alter tablespace "TEMP" add tempfile
   'ORACLE_HOME/oradata/GDB/temp01.dbf' size 5120K reuse autoextend on next 8k
   maxsize unlimited;
   ```

   GDB is the first part of the global database name.

Task 4: Configure Ultra Search Metadata in the New Metadata Repository

Perform this task on the new Metadata Repository.

1. Make sure the ORACLE_HOME and ORACLE_SID environment variables are set.
2. Run the following commands:

   ```
   cd ORACLE_HOME/ultrasearch/admin
   sqlplus "sys/SYS_PASSWORD as sysdba"
   ```

```
SQL> @wk0config.sql WKSYSPW JDBC_CONNSTR LAUNCH_ANYWHERE ""
```

Where:

WKSYSPW is the password of the WKSYS schema that you obtained at the beginning of this procedure.

JDBC_CONNSTR is the JDBC connection string *host*:*port*:*SID*, for example: myhost:1521:testdb.

LAUNCH_ANYWHERE is TRUE if the Metadata Repository is in Real Application Cluster mode, otherwise FALSE. For this procedure, you should set it to FALSE.

Task 5: Change the Global DB Name for the New Metadata Repository

In this task, you change the global db name of the new Metadata Repository to a new, unique name so you can register it with OID.

> **See Also:** You can find more information on changing the global db name in article 137483.1 at http://metalink.oracle.com

Perform all of the steps in this task on the new Metadata Repository host.

1. Run the following commands to set up the database:

```
sqlplus "sys/SYS_PASSWORD as sysdba"
SQL> alter system switch logfile;
SQL> alter database backup controlfile to trace resetlogs;
```

2. Check the spfile using SQL*Plus:

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

3. If the previous command returns no rows, you can skip this step.

   If the previous command returns output like the following:

```
VALUE
---------------------------------
?/dbs/spfile@.ora
```

   run the following command to create a pfile from the spfile:

```
SQL> create pfile='initORACLE_SID.ora' from spfile;
```

   Where *ORACLE_SID* is the SID of the original and new Metadata Repository.

4. Shut down the new Metadata Repository:

```
SQL> shutdown immediate;
```

The database must be shut down with SHUTDOWN NORMAL or SHUTDOWN IMMEDIATE. You should not use SHUTDOWN ABORT.

5. Rename the spfile so the pfile will be used when the database instance is restarted:

```
cd ORACLE_HOME/dbs
mv spfileORACLE_SID.ora spfileORACLE_SID.ora.save
```

6. Edit the following file:

```
ORACLE_HOME/dbs/initORACLE_SID.ora
```

Update the db_name to the new db name (the first portion of the new global db name). For example, if the new global db name is asdb1.myco.com, the value of db_name should be asdb1. Note that this is not necessarily (nor likely) the same value as the SID on the new Metadata Repository.

7. Rename the controls files so they do not exist later when the new ones are created:

```
cd ORACLE_HOME/oradata/GDB
```

Where *GDB* is the first part of the global database name.

```
mv control01.ctl control01.ctl.old
mv control02.ctl control02.ctl.old
mv control03.ctl control03.ctl.old
```

8. Change to the trace file directory:

```
cd ORACLE_HOME/admin/GDB/udump
```

Note that the above is the default location for the trace file directory. This location can be overridden by the user_dump_dest parameter in initORACLE_SID.ora or spfileORACLE_SID.ora.

9. Locate the trace file; it has a name of the form ora_NNNN.trc, where *NNNN* is a number. Choose the trace file with the most recent modification date.

10. Copy the contents of the trace file, starting from the line with "STARTUP NOMOUNT" down to the end of the file, into a new file named *BACKUP_DIR*/ccf.sql.

11. Edit *BACKUP_DIR*/`ccf.sql` as follows (an example of `ccf.sql` after performing the edits in this step is shown in Example 8–1.)

a. Update the following line with the new global db name and change "REUSE" to "SET":

Before modification:

```
CREATE CONTROLFILE REUSE DATABASE "OLD_GLOBAL_DB_NAME" RESETLOGS ...
```

After modification:

```
CREATE CONTROLFILE SET DATABASE "NEW_GLOBAL_DB_NAME" RESETLOGS ...
```

b. Remove the following line:

```
# STANDBY LOGFILE
```

c. Comment out the following lines with "REM", as shown:

```
REM RECOVER DATABASE USING BACKUP CONTROLFILE
REM VARIABLE RECNO NUMBER;
REM EXECUTE :RECNO := SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILE
AUTOBACKUP','ON');
REM VARIABLE RECNO NUMBER;
REM EXECUTE :RECNO :=
SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILEAUTOBACKUP FORMAT FOR
DEVICE TYPE','DISK TO BACKUP_DIR/db_files/%F');
```

d. Change all comment symbols (#) to "REM".

e. Make sure the last uncommented command in the file is:

```
ALTER DATABASE OPEN RESETLOGS
```

Example 8–1 Example ccf.sql File after Edits

```
STARTUP NOMOUNT
CREATE CONTROLFILE set DATABASE "<NEW DATABASE>" RESETLOGS ARCHIVELOG
   MAXLOGFILES 50
   MAXLOGMEMBERS 5
   MAXDATAFILES 100
   MAXINSTANCES 1
   MAXLOGHISTORY 226
LOGFILE
 GROUP 1 '/private1/inst/oradata/asdb/redo01.log'  SIZE 50M,
 GROUP 2 '/private1/inst/oradata/asdb/redo02.log'  SIZE 50M,
 GROUP 3 '/private1/inst/oradata/asdb/redo03.log'  SIZE 50M
```

```
DATAFILE
 '/private1/inst/oradata/asdb/system01.dbf',
 '/private1/inst/oradata/asdb/undotbs01.dbf',
 '/private1/inst/oradata/asdb/drsys01.dbf',
 '/private1/inst/oradata/asdb/dcm.dbf',
 '/private1/inst/oradata/asdb/portal.dbf',
 '/private1/inst/oradata/asdb/ptldoc.dbf',
 '/private1/inst/oradata/asdb/ptlidx.dbf',
 '/private1/inst/oradata/asdb/ptllog.dbf',
 '/private1/inst/oradata/asdb/oca.dbf',
 '/private1/inst/oradata/asdb/discopltc1.dbf',
 '/private1/inst/oradata/asdb/discopltm1.dbf',
 '/private1/inst/oradata/asdb/oss_sys01.dbf',
 '/private1/inst/oradata/asdb/wcrsys01.dbf',
 '/private1/inst/oradata/asdb/uddisys01.dbf',
 '/private1/inst/oradata/asdb/ip_dt.dbf',
 '/private1/inst/oradata/asdb/ip_rt.dbf',
 '/private1/inst/oradata/asdb/ip_idx.dbf',
 '/private1/inst/oradata/asdb/ip_lob.dbf',
 '/private1/inst/oradata/asdb/attrs1_oid.dbf',
 '/private1/inst/oradata/asdb/battrs1_oid.dbf',
 '/private1/inst/oradata/asdb/gcats1_oid.dbf',
 '/private1/inst/oradata/asdb/gdefault1_oid.dbf',
 '/private1/inst/oradata/asdb/svrmg1_oid.dbf',
 '/private1/inst/oradata/asdb/ias_meta01.dbf'
CHARACTER SET WE8MSWIN1252
;
REM Configure RMAN configuration record 1
REM VARIABLE RECNO NUMBER;
REM EXECUTE :RECNO := SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILE
AUTOBACKUP','ON');
REM Configure RMAN configuration record 2
REM VARIABLE RECNO NUMBER;
REM EXECUTE :RECNO := SYS.DBMS_BACKUP_RESTORE.SETCONFIG('CONTROLFILE AUTOBACKUP
FORMAT FOR DEVICE TYPE','DISK TO /private1/inst/backup_dir/db_files/%F');
REM Recovery is required if any of the datafiles are restored backups,
REM or if the last shutdown was not normal or immediate.
REM RECOVER DATABASE USING BACKUP CONTROLFILE
REM Database can now be opened zeroing the online logs.
ALTER DATABASE OPEN RESETLOGS;
REM No tempfile entries found to add.
```

12. Run the `ccf.sql` script:

```
SQL> @BACKUP_DIR/ccf.sql
```

13. Change the global db name in the database:

    ```
    SQL> alter database rename global_name to NEW_GLOBAL_DB_NAME;
    ```

14. Update the service name and the global db name to the new global db name in the following files:

    ```
    ORACLE_HOME/network/admin/tnsnames.ora
    ORACLE_HOME/network/admin/listener.ora
    ```

    Note that you should not change the SID.

Task 6: Register the New Metadata Repository with OID

In this task, you register the new Metadata Repository with the same OID used by the original Metadata Repository. To do this, you run Oracle Application Server Repository Creation Assistant (OracleAS RepCA), a wizard that guides you through the registration.

> **Note:** OracleAS RepCA is available on the "OracleAS RepCA and Utilities" CD-ROM.

To register the new Metadata Repository with Oracle Internet Directory, start up OracleAS RepCA on the host where the new Metadata Repository is installed:

```
runRepca -OH ORACLE_HOME -REGISTER
```

Where *ORACLE_HOME* is the new Metadata Repository Oracle home.

The wizard will guide you through the process.

> **See Also:** *Oracle Application Server 10g Installation Guide* for more information on registering the OracleAS Metadata Repository with Oracle Internet Directory

Task 7: Change Middle-Tier Instances to the New Metadata Repository

On each middle-tier instance you want to change to the new Metadata Repository, run the Change Metadata Repository wizard and restart the instance:

1. On Application Server Control, navigate to the Instance Home Page for the middle-tier instance.

2. Make sure all components except Management are down. If not, click the **Stop All** button to stop them. Note that this will not stop Management.
3. Click **Infrastructure**.
4. On the Infrastructure Page, in the Metadata Repository section, click **Change**.
5. Follow the steps in the wizard for supplying the new Metadata Repository information.
6. When the wizard is finished, navigate to the Instance Home Page and start your instance by clicking **Start All**.

9

Changing Network Configurations

This chapter provides procedures for changing the network configuration of an Oracle Application Server host.

It contains the following topics:

9.1 Which Networking Features are Supported on Your Platform?

Oracle Application Server supports a variety of options for configuring and changing networking features. Depending on your operating system platform, you can install Oracle Application Server on:

- A host with a static IP address and hostname (all platforms support this option)
- A host that uses DHCP
- A host that is off the network

> **See Also:** *Oracle Application Server 10g Installation Guide* for your platform for more information

After installation, you may want to change the networking configuration. This chapter provides procedures for changing the networking configuration of an Oracle Application Server host.

> **See Also:** *Oracle Application Server 10g Release Notes* to determine which networking features are supported for your operating system platform

9.2 Overview of Procedures for Changing Network Configurations

- Changing the Hostname and IP Address (Middle Tier)

  Follow this procedure if your host uses a static IP address and hostname, and you would like to change to a different static IP address, hostname, or both. This procedure is for hosts that contain one or more middle-tier instances.

  Some examples of when to use this procedure are:

  – Your organization moved to a new geographic location and you must move to a new subnet

  – You must change the hostname on your system

- Changing the IP Address (Infrastructure)

  Follow this procedure if your host uses a static IP address and hostname, an you would like to change to a different static IP address. The hostname must remain the same. This procedure is for hosts that contain an Infrastructure. You can use this procedure if your host moves to a new subnet.

- Moving Between Off-network and On-network

This section provides procedures for moving an Oracle Application Server host on and off the network. You may use DHCP or a static IP address when on the network. You can use these procedures, for example, if you installed Oracle Application Server on your laptop and would like to plug in to different networks to use it.

- Changing Between a Static IP Address and DHCP

  This section provides procedures for changing from a static IP address to DHCP, and from DHCP to a static IP address. You might use these if you install on a static IP address but then decide you would like to use DHCP so you can be more mobile, or if you are using DHCP and must plug in to a network using a static IP address.

9.3 Changing the Hostname and IP Address (Middle Tier)

This section describes how to change the hostname and IP address of a host that contains one or more Oracle Application Server middle-tier installations. You can use this procedure to change:

- The hostname only
- The IP address only
- Both the hostname and IP address

You can use this procedure on J2EE and Web Cache, Portal and Wireless, and Business Intelligence and Forms installations. This procedure is not supported for OracleAS Developer Kits 10*g* installations.

> **Note:** If any installations contain Oracle Content Management SDK, you must perform additional steps. Refer to *Oracle Content Management SDK Administrator's Guide* before starting this procedure.

The procedure includes:

- Changing the hostname and IP address on your operating system

  The details on how to do this are not provided, since this varies according to your operating system type and configuration. Consult your operating system documentation to determine how to do this before beginning the procedure.

- Updating Oracle Application Server for the new hostname and IP address

The details on how to do this are provided in the procedure. For tips on recovering from errors, see Section 9.7, "Recovering from Errors when Using chgiphost.sh".

Step 1: Prepare Your Host

In this step, you prepare your host for the change by removing instances from clusters and stopping all processes.

1. If the host contains a middle-tier instance that is part of an OracleAS Cluster, remove the instance from the cluster. You can add the instance back into the cluster at the end of the procedure.

   See Also: *Oracle Application Server 10g High Availability Guide* for instructions on removing instances from a cluster

2. If the host contains a middle-tier instance that is part of an OracleAS Web Cache cluster, remove the instance from the cache cluster. You can add the instance back into the cluster at the end of the procedure.

   See Also: *Oracle Application Server Web Cache Administrator's Guide* for instructions on removing caches from a cluster

3. Shut down each middle-tier instance on the host by running the following commands in each Oracle home:

   ```
   ORACLE_HOME/bin/emctl stop iasconsole
   ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

4. Verify that all Oracle Application Server processes have stopped.
5. Make sure Oracle Application Server processes will not start automatically after a reboot by disabling any automated startup scripts you may have set up, such as `/etc/init.d` scripts.
6. Make sure the Oracle Internet Directory that the middle-tier is using is running.

Step 2: Change the Hostname and IP Address on Your Operating System

In this step, you update your operating system with the new hostname, IP address, or both, reboot, and verify that the host is functioning properly on your network. Consult your operating system documentation, system administrator, and network administrator for more information on how to do this.

1. Make the updates to your operating system to properly change the hostname, IP address, or both.
2. Reboot the host.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new hostname to make sure everything is resolving properly.

Step 3: Update the Middle-Tier Instances on Your Host

In this step, you update the Oracle Application Server middle-tier instances on your host with the new hostname and IP address. Follow these steps for each middle-tier instance on your host. Be sure to complete the steps entirely for one middle-tier instance before you move on to the next.

1. Log in to the host as the user that installed the middle-tier instance.
2. Make sure your `ORACLE_HOME` environment variable is set to the middle-tier Oracle home.
3. Run the following commands in the middle-tier Oracle home:

```
cd ORACLE_HOME/chgip/scripts
./chgiphost.sh -mid
```

The `chgiphost.sh` command prompts for information, as shown in Table 9–1. You may not receive all of the prompts, depending on your middle-tier installation type.

Note that the prompts may provide values in parenthesis. These are not default values—they are just reminders. You must enter a value for each prompt.

Table 9–1 Prompts and Actions for chgiphost.sh

Prompt	Action
`Enter the fully qualified host name (hostname.domainname) of the new system`	If you are changing the hostname of the system, enter the new fully-qualified hostname Otherwise, enter the current fully-qualified hostname
`Enter the IP Address of the new system`	If you are changing the IP address of the system, enter the new IP address Otherwise, enter the current IP address
`Enter the fully qualified host name (hostname.domainname) of the old system`	If you are changing the hostname of the system, enter the old fully-qualified hostname Otherwise, enter the current fully-qualified hostname

Table 9–1 (Cont.) Prompts and Actions for chgiphost.sh

Prompt	Action
`Enter the IP Address of the old system`	If you are changing the IP address of the system, enter the old IP address Otherwise, enter the current IP address
`Enter the password for the Mid Tier IAS instance (ias_admin)`	Enter the `ias_admin` password for the middle-tier instance
`Confirm the password for the Mid Tier IAS instance (ias_admin)`	Enter the `ias_admin` password again
Note: Depending on your configuration, you may not receive the rest of the prompts in this table.	
`Enter the password for the OID Administrator`	Enter the `cn=orcladmin` password for the Oracle Internet Directory in which this instance is registered
`Confirm the password for the OID Administrator`	Enter the `cn=orcladmin` password again
`Enter the password for the SYS user, of the infra database`	Enter the SYS schema password for the Metadata Repository used by this middle-tier instance. Note: You can determine which Metadata Repository is used by an instance by looking in the following file: *ORACLE_HOME*`/config/ias.properties` The Metadata Repository is the value of the `InfrastructureDBCommonName` parameter.
`Confirm the password for the SYS user, of the infra database`	Enter the SYS schema password that you entered in the previous step again.
`Enter the password for the dsGateway user, of the infra database`	If you are using OracleAS Syndication Services, enter the DSGATEWAY schema password for the Metadata Repository used by this middle-tier instance. Refer to Section 9.3.1, "Obtaining the DSGATEWAY Schema Password" for instructions on obtaining this password. If you are not using OracleAS Syndication Services, you can enter any dummy password such as "welcome".
`Confirm the password for the dsGateway user, of the infra database`	Enter the DSGATEWAY schema password that you entered in the previous step again.

4. Verify that the tool ran successfully by checking for errors in the files in the following directory:

   ORACLE_HOME/chgip/log

Step 4: Restart Oracle Application Server

In this step, you restart the middle-tier instances and restore your configuration back to the way it was before you started the procedure.

1. Start each middle-tier instance on your host by running the following commands in each Oracle home:

   ```
   ORACLE_HOME/opmn/bin/opmnctl startall
   ORACLE_HOME/bin/emctl start iasconsole
   ```

2. If you removed any instances from an OracleAS Cluster at the beginning of this procedure, add them back to the cluster.

   See Also: *Oracle Application Server 10g High Availability Guide* for instructions on adding instances to a cluster

3. If you removed any instances from an OracleAS Web Cache cluster at the beginning of this procedure, add them back to the cache cluster.

   See Also: *Oracle Application Server Web Cache Administrator's Guide* for instructions on adding caches to a cluster

4. If you disabled any processes for automatically starting Oracle Application Server at the beginning of this procedure, enable them.

Step 5: Update OracleAS Portal and OracleAS Wireless

This is a special step required for updating OracleAS Portal and OracleAS Wireless when you change the hostname.

- Update the OracleAS Portal Web provider URLs with the new hostname.

  Refer to *Oracle Application Server Portal Configuration Guide* for instructions.

- When you change the hostname, the OracleAS Wireless server URL changes to use the new hostname. You must update OracleAS Portal with the new OracleAS Wireless service URL.

  Refer to the section on "Updating the OracleAS Wireless Portal Service URL Reference" in *Oracle Application Server Portal Configuration Guide* for instructions.

Step 6: Manually Update the Hostname in Files

If you edited a file and entered the hostname as part of a user-defined parameter such as the Oracle Home path, the hostname is not automatically updated by running the `chgiphost.sh` script. To update the hostname in such cases, you need to edit the files manually. For example, the plsql.conf file may contain an NFS path including the hostname, such as: `/net/dsun1/private/...`.

The `chgiphost.sh` script also does not edit the hostname references in the documentation files. You will need to manually edit these files to update the hostname. Examples of such files are the following files in the *ORACLE_HOME*`/Apache/Apache/htdocs` directory.

- `index.html.de`
- `index.html.es_ES`
- `index.html.fr`
- `index.html.it`
- `index.html.ja`
- `index.html.ko`
- `index.html.pt_BR`
- `index.html.zh_CN`
- `index.html.zh_TW`

9.3.1 Obtaining the DSGATEWAY Schema Password

The password for the DSGATEWAY schema in the Metadata Repository is stored in Oracle Internet Directory. It is usually a randomly-generated password. If you do not know the DSGATEWAY password, you can obtain it using the `ldapsearch` command.

> **Note:** You only need to know the DSGATEWAY schema password if you are using OracleAS Syndication Services. If you are not using OracleAS Syndication Services, you can enter any dummy password, such as "welcome", when `chgiphost.sh` prompts for the DSGATEWAY password

Run the following command in the middle-tier Oracle home:

ORACLE_HOME`/bin/ldapsearch -h` ***oid_host*** `-p` ***oid_port*** `-D cn=orcladmin -w` ***orcladmin_password*** `-b "orclresourcename=dsgateway,`

```
orclreferencename=metadata_repository, cn=ias infrastructure databases, cn=ias,
cn=products, cn=oraclecontext" -s base "objectclass=*" orclpasswordattribute
```

Where:

- *oid_host* is the Oracle Internet Directory host name

  If you are not sure of this value, it is listed as `OIDhost` in the following file in the middle-tier Oracle home:

  ORACLE_HOME`/config/ias.properties`

- *oid_port* is the Oracle Internet Directory non-SSL port number

  If you are not sure of this value, it is listed as `OIDport` in the following file in the middle-tier Oracle home:

  ORACLE_HOME`/config/ias.properties`

- *orcladmin_password* is the `cn=orcladmin` user password in Oracle Internet Directory
- *metadata_repository* is the name of the Metadata Repository

  If you are not sure of this value, it is listed as `InfrastructureDBCommonName` in the following file in the middle-tier Oracle home:

  ORACLE_HOME`/config/ias.properties`

For example:

```
ORACLE_HOME/bin/ldapsearch -h myhost -p 3060 -D cn=orcladmin -w welcome1 -b
"orclresourcename=dsgateway, orclreferencename=asdb.myhost.mydomain.com cn=ias
infrastructure databases, cn=ias, cn=products, cn=oraclecontext" -s base
"objectclass=*" orclpasswordattribute
```

The `ldapsearch` command prints several lines of output. The `DSGATEWAY` password is listed as the `orclpasswordattribute`, for example:

```
orclpasswordattribute=B7149q3s
```

9.4 Changing the IP Address (Infrastructure)

This section describes how to change the IP address of a host that contains an Oracle Application Server Infrastructure.

The procedure includes:

- Changing the IP address on your operating system

  The details on how to do this are not provided since this varies according to your operating system type and configuration. Consult your operating system documentation to determine how to do this before beginning the procedure.

- Updating Oracle Application Server for the new IP address

  The details on how to do this are provided in the procedure. For tips on recovering from errors, see Section 9.7, "Recovering from Errors when Using chgiphost.sh".

Step 1: Prepare Your Host

In this step, you prepare your host for the change by stopping all processes.

1. Shut down all middle-tier instances that use the Infrastructure, even if they are on other hosts.
2. Set the `ORACLE_HOME` and `ORACLE_SID` environment variables.
3. Shut down the Infrastructure:

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/bin/lsnrctl stop

ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
SQL> quit
```

4. Verify that all Oracle Application Server processes have stopped.
5. Make sure Oracle Application Server processes will not start automatically after a reboot by disabling any automated startup scripts you may have set up, such as `/etc/init.d` scripts.

Step 2: Change the IP Address on Your Operating System

In this step, you update your operating system with the new IP address, reboot, and verify that the host is functioning properly on your network. Consult your operating system documentation, system administrator, and network administrator for more information on how to do this.

1. Make the updates to your operating system to properly change the IP address.

2. Reboot the host.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new IP address to make sure everything is resolving properly.

Step 3: Update the Infrastructure

In this step, you update the Infrastructure on your host with the new IP address.

1. Log in to the host as the user that installed the Infrastructure.
2. Set the ORACLE_HOME and ORACLE_SID environment variables.
3. Start the database:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect / as SYSDBA
SQL> startup
SQL> quit
```

4. Start OPMN:

```
ORACLE_HOME/opmn/bin/opmnctl start
```

5. Start Oracle Internet Directory:

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OID process-type=OID
```

6. Run the following commands in the Infrastructure Oracle home:

```
cd ORACLE_HOME/chgip/scripts
./chgiphost.sh -infra
```

   The chgiphost.sh command prompts for the old and new IP address.

7. Verify that the tool ran successfully by checking for errors in the files in the following directory:

```
ORACLE_HOME/bin/chgip/log
```

Step 4: Restart the Infrastructure

In this step, you restart the Infrastructure and any middle-tier instances that use it.

1. Set the ORACLE_HOME and ORACLE_SID environment variables.
2. Start the Infrastructure:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
```

```
SQL> startup
SQL> quit

ORACLE_HOME/lsnrctl start
ORACLE_HOME/opmn/bin/opmnctl startall
ORACLE_HOME/bin/emctl start iasconsole
```

3. If a middle-tier instance is on the same host as the infrastructure, then you need to run the `chgiphost.sh` script on the middle-tier instance before restarting the middle-tier processes.
4. If you disabled any processes for automatically starting Oracle Application Server at the beginning of this procedure, enable them.

9.5 Moving Between Off-network and On-network

This section describes how to move an Oracle Application Server host on and off the network. The following assumptions and restrictions apply:

- The host must contain an Infrastructure and middle-tier instance, or a J2EE and Web Cache instance that does not use an Infrastructure, that is, the entire Oracle Application Server environment must be on the host.
- DHCP must be used in loopback mode. Refer to *Oracle Application Server 10g Installation Guide* for more information.
- Only IP address change is supported; the hostname must remain unchanged.
- Hosts in DHCP mode should not use the default hostname (`localhost.localdomain`). The hosts should be configured to use a standard hostname and the loopback IP should resolve to that hostname.

9.5.1 Moving from Off-network to On-network (Static IP Address)

This procedure assumes you have installed Oracle Application Server on a host that is off the network, using a standard hostname (not `localhost`), and would like to move on the network and use a static IP address. The IP address may be the default loopback IP, or any standard IP address.

To move onto the network, you can simply plug the host into the network. If you would like to change the static IP address at that time, follow the appropriate procedure:

- Section 9.3, "Changing the Hostname and IP Address (Middle Tier)"

- Section 9.4, "Changing the IP Address (Infrastructure)"

9.5.2 Moving from Off-network to On-network (DHCP)

This procedure assumes you have installed on a host that is off the network, using a standard hostname (not `localhost`), and would like to move on the network and use DHCP. The IP address of the host can be any static IP address or loopback IP address, and should be configured to the hostname.

1. Connect the host to the network using DHCP and configure the hostname to the loopback IP address only.
2. If the original installation was performed using a static IP address and the new IP address is the DHCP loopback IP address, follow the appropriate procedure to change to the loopback IP address:
   - Section 9.3, "Changing the Hostname and IP Address (Middle Tier)"
   - Section 9.4, "Changing the IP Address (Infrastructure)"

   If the original installation was performed using the loopback IP, you do not need to change the IP address.

9.5.3 Moving from On-network to Off-network (Static IP Address)

Follow this procedure if your host is on the network, using a static IP address, and you would like to move it off the network.

1. Configure the `/etc/hosts` file so the IP address and hostname can be resolved locally.
2. Take the host off the network.
3. There is no need to perform any steps to change the hostname or IP address.

9.5.4 Moving from On-network to Off-network (DHCP)

Follow this procedure if your host is on the network, using DHCP in loopback mode, and you would like to move it off the network.

1. Configure the /etc/hosts file so the IP address and hostname can be resolved locally.
2. Take the host off the network.
3. There is no need to perform any steps to change the hostname or IP address.

9.6 Changing Between a Static IP Address and DHCP

This section describes how to change between a static IP address and DHCP. The following assumptions and restrictions apply:

- The host must contain an Infrastructure and middle-tier instance, or a J2EE and Web Cache instance that does not use an Infrastructure, that is, the entire Oracle Application Server environment must be on the host.
- DHCP must be used in loopback mode. Refer to *Oracle Application Server 10g Installation Guide* for more information.
- Only IP address change is supported; the hostname must remain unchanged.
- Hosts in DHCP mode should not use the default hostname (`localhost.localdomain`). The hosts should be configured to use a standard hostname and the loopback IP should resolve to that hostname.

9.6.1 Changing from a Static IP Address to DHCP

To change a host from a static IP address to DHCP:

1. Configure the host to have a hostname associated with the loopback IP address before you convert the host to DHCP.
2. Convert the host to DHCP and follow the appropriate procedure to change to the loopback IP address:
   - Section 9.3, "Changing the Hostname and IP Address (Middle Tier)"
   - Section 9.4, "Changing the IP Address (Infrastructure)"

9.6.2 Changing from DHCP to a Static IP Address

To change a host from DHCP to a static IP address:

1. Configure the host to use a static IP address.
2. Follow the appropriate procedure to change to the new static IP address:
   - Section 9.3, "Changing the Hostname and IP Address (Middle Tier)"
   - Section 9.4, "Changing the IP Address (Infrastructure)"

9.7 Recovering from Errors when Using chgiphost.sh

This section describes how to recover from typical errors you might encounter when using the `chgiphost.sh` script. It contains the following scenarios:

- Scenario 1: You Specified the Wrong Destination Name
- Scenario 2: You Encountered an Error when Running chgiphost.sh

Scenario 1: You Specified the Wrong Destination Name

Suppose you ran the `chgiphost.sh` script but specified the wrong destination name. In this case, you can remedy the error by running `chgiphost.sh` again. Here are the details.

Suppose the current source hostname is loire985, the incorrect destination hostname you specified is mqa985, and the correct destination hostname is sqb985. Initially, you ran `chgiphost.sh` with source = loire985 and destination = mqa985.

To recover from this error:

1. Run `chgiphost.sh` with source = mqa985 and destination = sqb985.
2. Run `chgiphost.sh` again with source = loire985 and destination = sqb985.

Scenario 2: You Encountered an Error when Running chgiphost.sh

If you encounter an error when running `chgiphost.sh`, you should fix the error and run `chgiphost.sh` again.

For example, you will get an error message if you enter the wrong password for Oracle Internet Directory or OracleAS Syndication Services. In this case, you should run `chgiphost.sh` again, with the same source and destination hostnames as before, and make sure to supply the correct password when prompted.

10

Management Considerations for Recommended Topologies

This chapter provides key considerations for managing the Oracle Application Server recommended topologies.

It contains the following topics:

10.1 About the Recommended Topologies

Oracle Application Server is a flexible product that offers a variety of topology options. To assist users in designing a topology, Oracle developed a set of **recommended topologies** that support common development and deployment requirements. These recommended topologies are documented throughout the Oracle Application Server 10*g* documentation library as described in Table 10–1.

Table 10–1 Oracle Application Server 10g Documentation Guide to Recommended Topologies

Topic	Description	See Also
Overview	High-level overview of each topology, including key considerations in the areas of installation, application deployment and performance, security, management, high availability deployment, and third party products	*Oracle Application Server 10g Concepts*
Installation Steps	System requirements and step-by-step instructions for installing and configuring each topology	*Oracle Application Server 10g Installation Guide* For Enterprise Topologies, see *Oracle Application Server 10g Advanced Topologies for Enterprise Deployments*
Management Considerations	Tips on managing each topology, including recommended tools and management tasks	*Oracle Application Server 10g Administrator's Guide*
Security Considerations	Tips on providing secure Internet access for each topology	*Oracle Application Server 10g Security Guide*
Performance Considerations	Performance goals, component distribution across hardware, application development strategies, and parameter tuning for each topology	*Oracle Application Server 10g Performance Guide*
High Availability Considerations	High Availability tips for the Enterprise Data Center and Departmental topologies	*Oracle Application Server 10g High Availability Guide*

This chapter provides key considerations for managing the following topologies:

- General Development Topologies—these topologies are based on development usage; they are:
  - Java Developer Topology
  - Portal and Wireless Topology
  - Forms, Reports, and Discoverer Developer Topology

  - Integration Architects and Process Modelers Topology
- General Deployment Topologies—these topologies are based on deployment usage; they are:
  - Enterprise Data Center Topologies
  - Departmental Topology
  - Development Life Cycle Support Topology

10.2 General Development Topologies

This section provides management considerations for the following recommended general development topologies:

- Java Developer Topology
- Portal and Wireless Topology
- Forms, Reports, and Discoverer Developer Topology
- Integration Architects and Process Modelers Topology

10.2.1 Java Developer Topology

This topology provides ease of development and deployment for Java developers. It is intended to run on low-end machines with Java IDE tools.

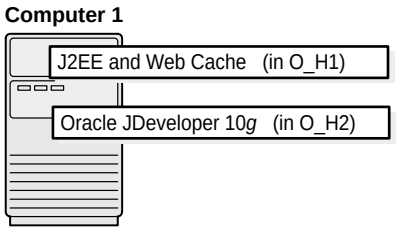
Key management considerations for the Java Developer Topology are:

- Use Application Server Control for:
  - Starting and stopping components as needed
  - Enabling / Disabling unused components so they do not consume system resources
  - Setting or changing configuration parameters for OC4J, Oracle HTTP Server, and OracleAS Web Cache
  - Deploying and configuring applications
  - Managing J2EE application security
  - Monitoring application and component performance and resource consumption in real-time
  - Viewing and setting port numbers

  - Viewing and searching log files
  - Managing OracleAS Clusters
- Use Application Server Control or JDeveloper to deploy applications
- Command-line utilities are available for scripting and automation, or if you use standalone components
- Use Oracle-recommended backup and recovery strategies

Figure 10–1 illustrates the Java Developer Topology. Note that "O_H*x*" in the figure denotes an Oracle home directory.

Figure 10–1 Java Developer Topology



10.2.2 Portal and Wireless Topology

This topology provides an environment for OracleAS Portal and OracleAS Wireless developers. It includes an Infrastructure, which is required to deploy and test their applications. It is intended to run on medium-sized machines.

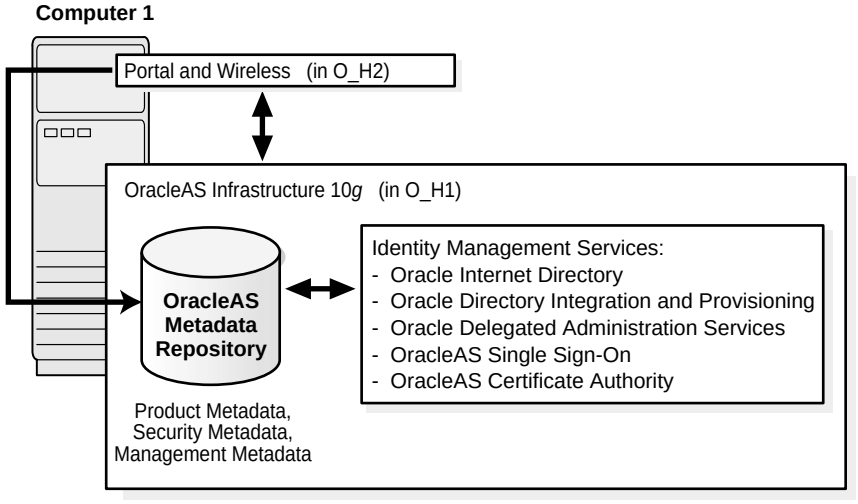
Key management considerations for the Portal and Wireless Developer Topology are:

- Use Application Server Control for:
  - Starting and stopping components as needed
  - Enabling / Disabling unused components so they do not consume system resources
  - Setting or changing configuration parameters for OC4J, Oracle HTTP Server, and OracleAS Web Cache
  - Deploying and configuring applications
  - Managing application security

  - Monitoring application and component performance and resource consumption in real-time
  - Viewing and setting port numbers
  - Viewing and searching log files
  - Managing Infrastructure schemas
- Use Oracle DBA Studio for managing the Metadata Repository
- Command-line utilities are available for scripting and automation
- Use Oracle-recommended backup and recovery strategies

Figure 10–2 illustrates the Portal and Wireless Developer Topology. Note that "O_H*x*" in the figure denotes an Oracle home directory.

Figure 10–2 Portal and Wireless Developer Topology



10.2.3 Forms, Reports, and Discoverer Developer Topology

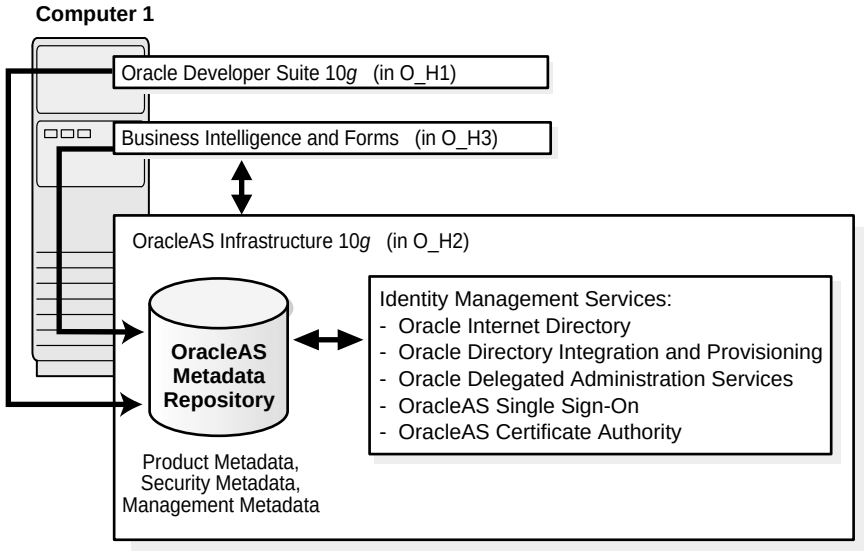
OracleAS Forms Services, OracleAS Reports Services, and OracleAS Discoverer developers have similar application deployment requirements. They need an Infrastructure and Oracle Developer Suite to deploy and test their applications. This topology is intended to run on medium-sized machines

Key management considerations for the Forms, Reports, and Discoverer Developer Topology are:

- Use Application Server Control for:
  - Starting and stopping components as needed
  - Enabling / Disabling unused components so they do not consume system resources
  - Setting or changing configuration parameters for OC4J, Oracle HTTP Server, and OracleAS Web Cache
  - Deploying and configuring applications
  - Managing application security
  - Monitoring application and component performance and resource consumption in real-time
  - Viewing and setting port numbers
  - Viewing and searching log files
  - Managing Infrastructure schemas
- Use Oracle DBA Studio for managing the Metadata Repository
- Command-line utilities are available for scripting and automation
- Use Oracle-recommended backup and recovery strategies

Figure 10–3 illustrates the Forms, Reports, and Discoverer Developer Topology. Note that "O_H*x*" in the figure denotes an Oracle home directory.

Figure 10–3 Forms, Reports, and Discoverer Topology



10.2.4 Integration Architects and Process Modelers Topology

Integration architects and process modelers require the OracleAS ProcessConnect middle-tier installation. They need appropriate adapters and an Infrastructure to deploy and test their integration applications. This topology is intended to run on medium-sized machines.

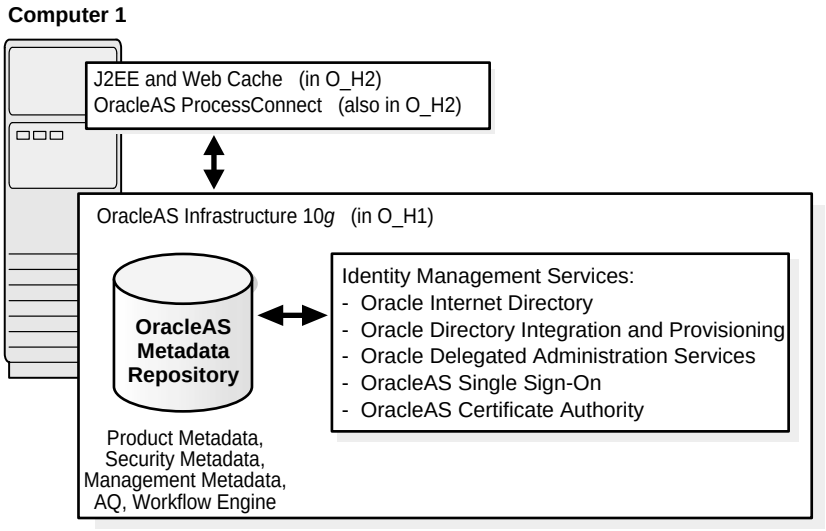
Key management considerations for Integration Architects and Process Modelers Topology are:

- Use Application Server Control for:
  - Starting and stopping components as needed
  - Enabling / Disabling unused components so they do not consume system resources
  - Setting or changing configuration parameters for OC4J, Oracle HTTP Server, and OracleAS Web Cache
  - Deploying and configuring applications
  - Managing application security

  - Monitoring application and component performance and resource consumption in real-time
  - Viewing and setting port numbers
  - Viewing and searching log files
  - Managing Infrastructure schemas
- Use Oracle DBA Studio for managing the Metadata Repository
- Command-line utilities are available for scripting and automation
- Use Oracle-recommended backup and recovery strategies

Figure 10–4 illustrates the Integration Architect and Process Modeler Topology. Note that "O_H*x*" in the figure denotes an Oracle home directory.

Figure 10–4 Integration Architect and Process Modeler Topology



10.3 General Deployment Topologies

This section provides management considerations for the following recommended general deployment topologies:

- Enterprise Data Center Topologies
- Departmental Topology
- Development Life Cycle Support Topology

10.3.1 Enterprise Data Center Topologies

Enterprise Data Center topologies can be used by multiple departments sharing the same data center. There are two Enterprise Data Center topologies:

- Enterprise Data Center Topology for Java Applications
- Enterprise Data Center Topology for Portal, Wireless, Business Intelligence, and Forms Applications

Key management considerations for Enterprise Data Center topologies are:

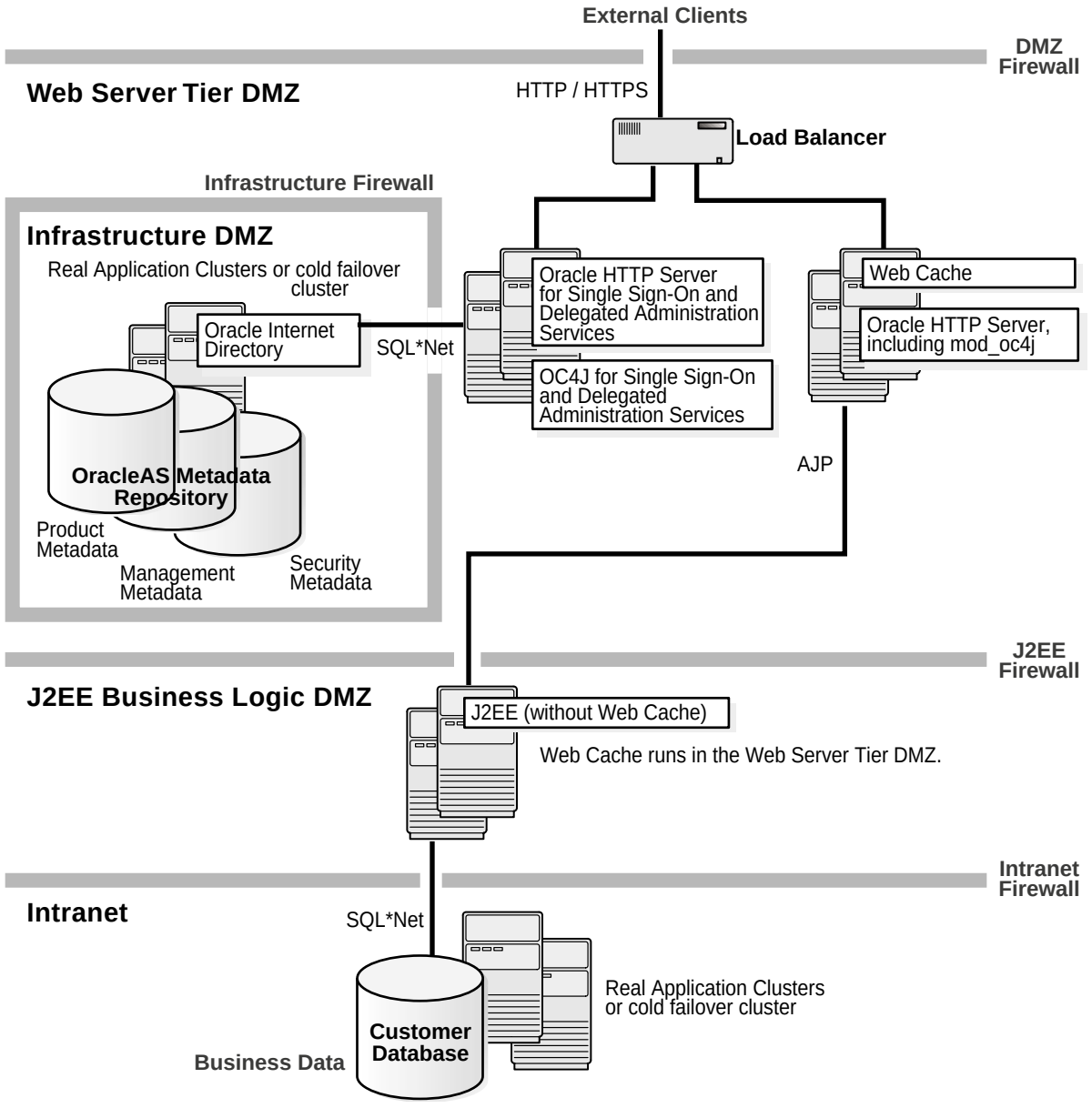
- Use Application Server Control for:
  - Starting and stopping components as needed
  - Enabling / Disabling unused components so they do not consume system resources
  - Setting or changing configuration parameters for OC4J, Oracle HTTP Server, and OracleAS Web Cache
  - Deploying and configuring applications
  - Managing application security
  - Monitoring application and component performance and resource consumption in real-time
  - Viewing and setting port numbers
  - Viewing and searching log files
  - Managing Infrastructure schemas
- Use Oracle DBA Studio for managing the Metadata Repository
- Command-line utilities are available for scripting and automation
- Use Oracle-recommended backup and recovery strategies

Enterprise Data Center Topology for Java Applications

This topology assumes that you want to create new databases for Product, Management, and Security services. If you choose to use an existing database, the product metadata will inherit the high availability solution already deployed for that database.

Figure 10–5 illustrates the Enterprise Data Center Topology for Java Applications.

Figure 10–5 Enterprise Data Center Topology for Java Applications

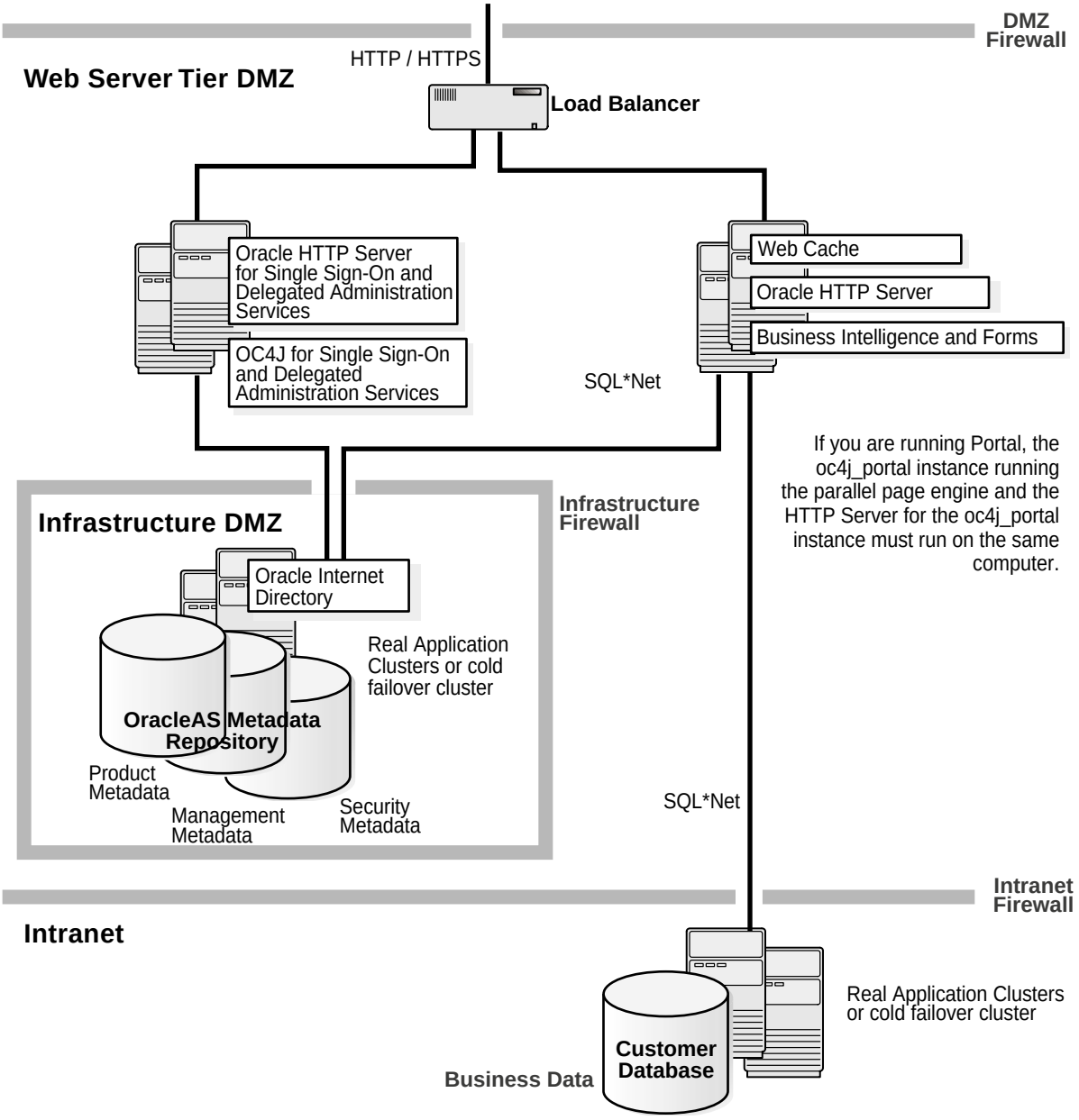


Enterprise Data Center Topology for Portal, Wireless, Business Intelligence, and Forms Applications

This topology assumes that you want to create new databases for Product, Management, and Security services. If you choose to use an existing database, the product metadata will inherit the high availability solution already deployed for that database.

Figure 10–6 illustrates the Enterprise Data Center Topology for Portal, Wireless, Business Intelligence, and Forms Applications.

Figure 10–6 Enterprise Data Center Topology for Portal, Wireless, Business Intelligence, and Forms



10.3.2 Departmental Topology

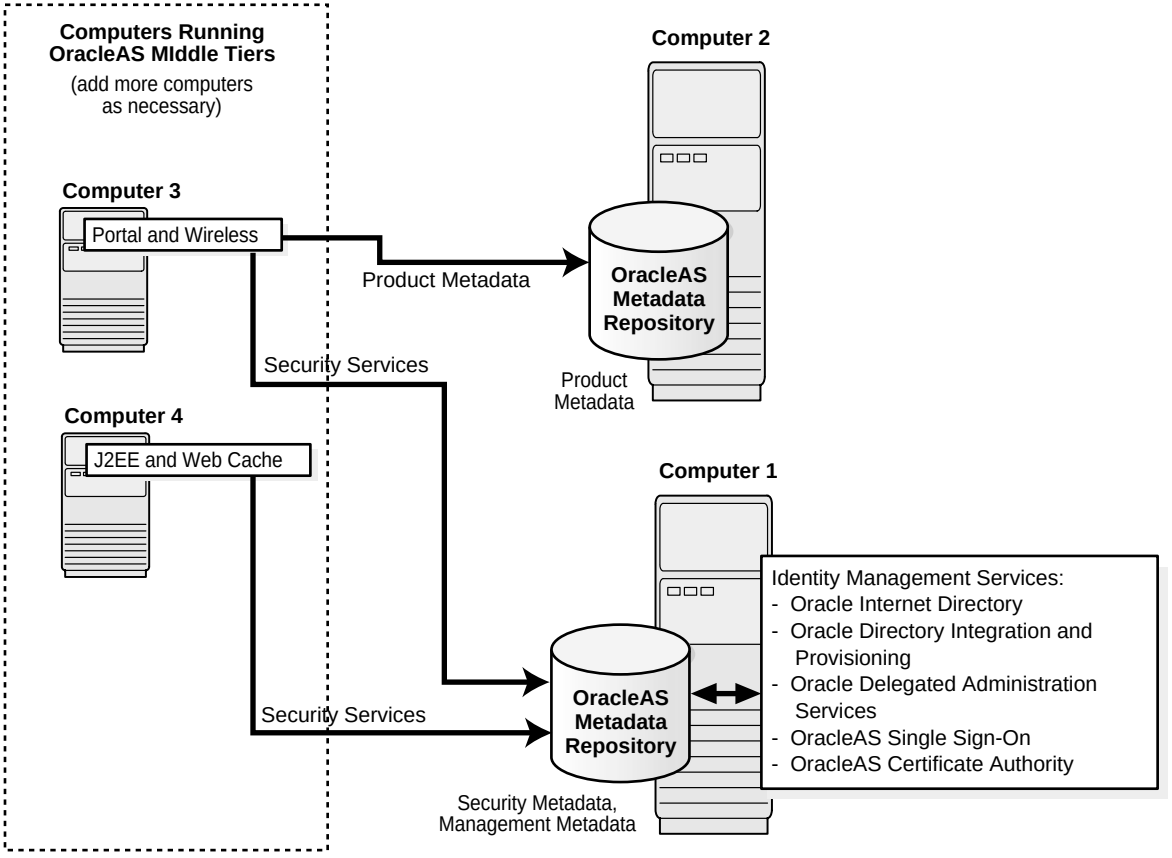
The Departmental Topology can be used by departments hosting their applications. This topology consists of a subset of considerations and requirements from the Enterprise Data Center topologies.

Key management considerations for using the Departmental Topology are:

- Use Application Server Control for:
  - Starting and stopping components as needed
  - Enabling / Disabling unused components so they do not consume system resources
  - Setting or changing configuration parameters for OC4J, Oracle HTTP Server, and OracleAS Web Cache
  - Deploying and configuring applications
  - Managing application security
  - Monitoring application and component performance and resource consumption in real-time
  - Viewing and setting port numbers
  - Viewing and searching log files
  - Managing Infrastructure schemas
- Use Oracle DBA Studio for managing the Metadata Repository
- Command-line utilities are available for scripting and automation
- Use Oracle-recommended backup and recovery strategies

Figure 10–7 illustrates the Departmental Topology.

Figure 10–7 Departmental Topology



10.3.3 Development Life Cycle Support Topology

The Development Life Cycle Support Topology provides a seamless environment for moving applications from the test environment to the staging environment, and from there to the production environment.

The Development Life Cycle Support Topology is a combination of other topologies which support moving applications from test to stage to production environments.

- Test environment: Application developers test their applications in their own environments. Examples of testing environments:
  - Java Developer Topology

    - Portal and Wireless Topology
    - Forms, Reports, and Discoverer Developer Topology
- Stage environment: QA personnel test all applications before deploying them to the production environment. In this environment, you can use the Departmental Topology. This topology in a stage environment runs applications from all departments, not just from a single department.
- Production environment: Applications are ready for use by both internal and external users. See Enterprise Data Center Topologies.

Key management considerations for the Development Life Cycle Support Topology are:

- Use Application Server Control for:
    - Starting and stopping components as needed
    - Enabling / Disabling unused components so they do not consume system resources
    - Setting or changing configuration parameters for OC4J, Oracle HTTP Server, and OracleAS Web Cache
    - Deploying and configuring applications
    - Managing application security
    - Monitoring application and component performance and resource consumption in real-time
    - Viewing and setting port numbers
    - Viewing and searching log files
    - Managing Infrastructure schemas
- Use Oracle DBA Studio for managing the Metadata Repository
- Command-line utilities are available for scripting and automation
- Use Oracle-recommended backup and recovery strategies
- Use the Oracle-recommended procedures for changing Infrastructure services from test to production.

    See Also: Chapter 8, "Changing Infrastructure Services"

Part IV

Backup and Recovery

Backup and recovery refers to the various strategies and procedures involved in guarding against hardware failures and data loss, and reconstructing data should loss occur. This part describes how to back up and recover Oracle Application Server.

This part contains the following chapters:

- Introduction to Backup and Recovery
- Oracle Application Server Backup and Recovery Tool
- Backup Strategy and Procedures
- Recovery Strategies and Procedures

11

Introduction to Backup and Recovery

This chapter provides information on getting started with Oracle Application Server backup and recovery.

It contains the following topics:

11.1 Philosophy of Oracle Application Server Backup and Recovery

This section introduces the philosophy for backing up and recovering your Oracle Application Server environment.

A typical Oracle Application Server environment contains:

- An **Infrastructure installation** that contains Identity Management and a Metadata Repository
- One or more **middle-tier installations** (J2EE and Web Cache, Portal and Wireless, or Business Intelligence and Forms) that may use the Infrastructure

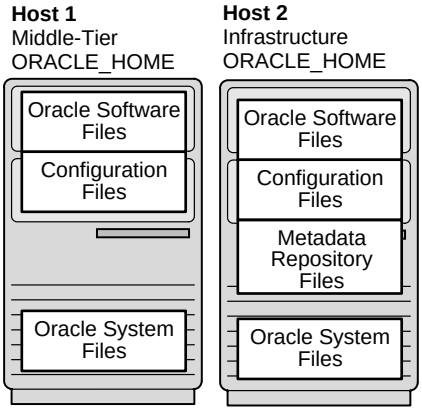
The installations in an Oracle Application Server environment are interdependent in that they contain configuration information, applications, and data that are kept in sync. For example, when you perform a configuration change, you might update configuration files in the middle-tier installation and Infrastructure; when you deploy an application, you might deploy it to all middle-tier installations; and when you perform an administrative change on a middle-tier installation, you might update data in the Metadata Repository.

It is, therefore, important to consider your entire Oracle Application Server environment when performing backup and recovery. For example, you should not back up your middle-tier installation on Monday and your Infrastructure on Tuesday. If you lose files in your middle-tier installation, you could restore it to Monday's state. However, your Infrastructure would be in its current state—out of sync with the middle tier. And, because you backed up the Infrastructure on Tuesday, you would have no means of restoring it to a state in sync with Monday's middle-tier installation. You would not be able to restore your environment to a consistent state.

Instead, you should back up your entire Oracle Application Server environment at once. Then, if a loss occurs, you can restore your entire environment to a consistent state.

For the purposes of backup and recovery, you can divide your Oracle Application Server into different types of files, as shown in Figure 11–1.

Figure 11–1 Types of Files for Oracle Application Server Backup and Recovery



The types of files for backup and recovery are:

- **Oracle software files**

  These are static files such as binaries and libraries. They reside in the middle-tier and Infrastructure Oracle homes. They are created at installation time.

- **Configuration files**

  These files contain configuration information and deployed applications. They reside in the middle-tier and Infrastructure Oracle homes. They are created at installation time and are updated during the normal operation of your application server.

- **Metadata Repository files**

  These are the datafiles and control files that make up your Metadata Repository. They reside in the Infrastructure Oracle home. They are created at installation time and are updated during the normal operation of your application server.

- **Oracle system files**

  These files may be in the `/var/opt/oracle` or `/etc` directory, and the `oraInventory` directory. They exist on each host in your Oracle Application Server environment. They usually reside outside of your Oracle Application

Server installations, although the `oraInventory` directory may be in an Oracle home. They are created and updated by Oracle Universal Installer at installation time and contain information about your installations.

The strategies and procedures in this book involve backing up and recovering these different types of files in a manner that maintains your Oracle Application Server environment in a consistent state.

Note: Your Oracle Application Server environment contains additional files to those mentioned in this section, such as log files; database configuration files, including `tnsnames.ora`, `listener.ora`, `sqlnet.ora`, `orapwd`, and `spfile/pfile`; and additional files you may deploy in the Oracle home, such as static HTML files and CGI scripts.

The tools and procedures in this book do not cover these files. Oracle recommends you protect yourself from loss of these files using your routine filesystem backup procedures.

11.2 Overview of the Backup Strategy

This section describes the backup strategy used in this book. It contains the following topics:

- Types of Backups
- Recommended Backup Strategy

11.2.1 Types of Backups

The Oracle Application Server backup strategy involves two types of backups:

- Complete Oracle Application Server Environment Backup
- Online Backup

Complete Oracle Application Server Environment Backup

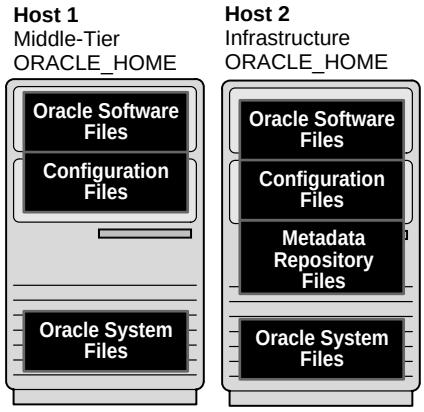
A complete Oracle Application Server environment backup includes:

- A full backup of all files in the middle-tier Oracle homes (this includes Oracle software files and configuration files)
- A full backup of all files in the Infrastructure Oracle home (this includes Oracle software files and configuration files)

- A complete cold backup of the Metadata Repository
- A full backup of the Oracle system files on each host in your environment

In Figure 11–2, the files that are backed up during a complete Oracle Application Server environment backup are shaded. The complete Oracle Application Server environment backup includes everything necessary to restore the initial installation of your Oracle Application Server environment. You must shut down your Oracle Application Server environment before performing this backup.

Figure 11–2 Files Backed Up in a Complete Oracle Application Server Environment Backup



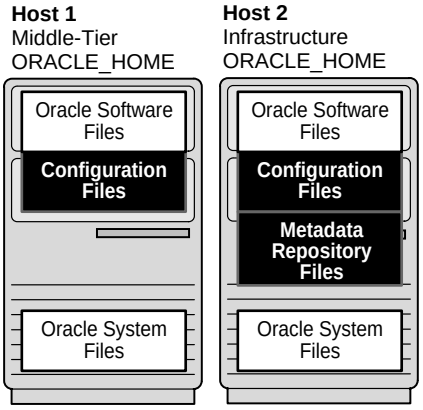
Online Backup

An online backup includes:

- An incremental backup of the configuration files in the middle-tier Oracle homes.
- An incremental backup of the configuration files in the Infrastructure Oracle home
- An online backup of the Metadata Repository

In Figure 11–3, the files that are backed up during an online backup are shaded. The online backup involves saving the configuration information, applications, and data across your entire Oracle Application Server environment at the same point in time. You can leave your Oracle Application Server up while performing an online backup.

Figure 11–3 Files Backed Up in an Online Backup



11.2.2 Recommended Backup Strategy

This section outlines the recommended strategy for performing backups. Using this strategy ensures that you will be able to perform the recovery procedures in this book.

1. **Perform a complete Oracle Application Server environment backup.**

   Immediately after you install Oracle Application Server, you should perform a complete Oracle Application Server environment backup. This backup contains everything you need in order to restore your environment to its initial state. It servers as a baseline for all subsequent online backups.

2. **Perform online backups on a regular basis.**

   After every administrative change, or, if this is not possible, on a regular basis, perform an online backup of your Oracle Application Server environment. This will enable you to restore your environment to a consistent state as of the time of your most recent online backup.

   > **See Also:** Appendix G, "Examples of Administrative Changes" to learn more about administrative changes

3. **After a major change, perform a new complete Oracle Application Server environment backup.**

If you make a major change to your Oracle Application Server environment, perform a new complete Oracle Application Server environment backup. This backup will serve as the basis for subsequent online backups.

Perform a new complete Oracle Application Server environment backup after:

- An operating system software upgrade
- An Oracle Application Server software upgrade or patch application

4. **Perform online backups on a regular basis.**

   After you establish a new complete Oracle Application Server environment backup, return to Step 2 and continue to perform online backups on a regular basis.

11.3 Overview of Recovery Strategies

There are two types of Oracle Application Server recovery strategies used in this book:

- Recovery Strategies for Data Loss, Host Failure, or Media Failure (Critical)
- Recovery Strategies for Process Crashes or System Outages (Non-Critical)

Recovery Strategies for Data Loss, Host Failure, or Media Failure (Critical)

These strategies enable you to recover from critical failures that involve actual data loss. Depending on the type of loss, they can involve recovering any combination of the following types of files:

- Oracle software files
- Configuration files
- Metadata Repository files
- Oracle system files

In all cases, these strategies involve making sure your state is consistent across all installations.

Recovery Strategies for Process Crashes or System Outages (Non-Critical)

These strategies involve restarting processes that have stopped or failed. They do not involve restoring data. They are included in this book for completeness.

11.4 What is the Oracle Application Server Backup and Recovery Tool?

The Oracle Application Server Backup and Recovery Tool (OracleAS Backup and Recovery Tool) is a Perl script and associated configuration files. You can use the tool to backup and recover the following types of files:

- Configuration files in the middle-tier and Infrastructure Oracle home
- Metadata Repository files

The OracleAS Backup and Recovery Tool is available on the "OracleAS RepCA and Utilities" CD-ROM. Instructions for installing and configuring the tool are in Chapter 12, "Oracle Application Server Backup and Recovery Tool".

11.5 Assumptions and Restrictions

The following assumptions and restrictions apply to the backup and recovery procedures in this book:

- The following installation types are supported:
  - J2EE and Web Cache
  - Portal and Wireless
  - Business Intelligence and Forms
  - Infrastructure (Identity Management and Metadata Repository)
  - Infrastructure (Identity Management only)
  - Infrastructure (Metadata Repository only)
  - OracleAS TopLink (Standalone or installed into a middle-tier Oracle home)
  - OracleAS ProcessConnect
  - Oracle Content Management Software Development Kit
- **Warning:** You ***cannot*** use the OracleAS Backup and Recovery Tool on a Metadata Repository that was created by running Oracle Application Server Repository Creation Assistant (OracleAS RepCA) on an existing database. You must backup and recover that type of Metadata Repository using standard database backup and recovery.
- The procedures in this book assume the Metadata Repository is a single instance database. If you are using OracleAS Cold Failover Cluster, OracleAS Active Failover Cluster, or Disaster Recovery, refer to Section 11.7, "Backup and

Recovery Considerations for High Availability Environments" for special considerations.

- If you would like to use the OracleAS Backup and Recovery Tool in a standalone OracleAS TopLink installation, you must manually edit `config.inp` and set `config_files_list` as follows:

  ```
  config_files_list=config_toplink_files.inp,config_misc_files.inp
  ```

  Refer to Section 12.4, "How to Configure the OracleAS Backup and Recovery Tool".

11.6 Backup and Recovery Considerations for DCM

Distributed Configuration Management (DCM) is a framework for managing configuration information for application server instances, OracleAS Clusters, and the following components: Oracle HTTP Server, OC4J, OPMN, and JAZN.

This section discusses features of DCM that require consideration when performing backup and recovery. It contains the following topics:

- Considerations for DCM File-based Repositories
- Considerations for DCM Archives

11.6.1 Considerations for DCM File-based Repositories

All middle-tier instances that are part of a farm use a DCM repository. The DCM repository contains configuration information and deployed J2EE applications.

There are two types of DCM repositories:

- Database repository—this is stored in the DCM schema in a Metadata Repository.
- File-based repository—this is stored on the filesystem in the Oracle home of one middle-tier instance in the farm, known as the *repository host instance*.

If your environment contains a database repository, you do not need to perform any special steps because the repository will be backed up and recovered during normal Metadata Repository backup and recovery.

If your environment contains a file-based repository, there are some special considerations for backup and recovery.

- **Backup Considerations for DCM File-based Repositories**

When you back up the middle-tier instance that contains the file-based repository (the repository host instance), you should perform an additional step to create a backup of the file-based repository. Then, in case you lose the instance, you can recover the repository. The steps for creating the repository backup are included in the backup procedures in this book.

You can identify the repository host instance using the following command:

```
ORACLE_HOME/dcm/bin/dcmctl whichFarm
```

This command returns a Repository Type of "Distributed File Based (host)" when run in the Oracle home of the repository host instance.

- **Recovery Considerations for DCM File-based Repositories**

  If you lose the repository host instance, you must restore the file-based repository as part of restoring the instance. If you restore the instance to a new host, you must perform an additional step to notify the other members of the farm that the repository is on a new host. These steps are included in the recovery procedures in this book.

  See Also: *Oracle Application Server 10g High Availability Guide* for more information on DCM file-based repositories

11.6.2 Considerations for DCM Archives

A DCM archive is a snapshot of the configuration of an Oracle Application Server instance or cluster at a particular point in time. You can apply archived configurations to the same instance or cluster, or to a different instance or cluster.

DCM archives are stored in the DCM repository (file-based or database). For standalone J2EE and Web Cache instances, archives are stored on the local filesystem.

You can use DCM archiving separately from OracleAS Backup and Recovery. It is an easy way to save configurations before making changes to your system, or to save and restore a particular configuration for specific purposes, such as operating one configuration during the day and another at night.

In addition, you can incorporate DCM archiving into your OracleAS Backup and Recovery strategies as follows:

- **Backup Considerations for DCM Archives**

  Oracle recommends that you create a DCM archive of each middle-tier instance every time you perform a backup, and export the archives to a backup location.

This provides an additional measure of safety. The steps for creating and exporting a DCM archive are included in the backup procedures in this book.

- **Recovery Considerations for DCM Archives**

  Typically, you will not require a DCM archive for restoring your environment. However, there may be situations when you cannot restore middle-tier configuration files or the repository successfully. You can then use the DCM archive to restore your DCM configurations.

  > **See Also:** *Distributed Configuration Management Reference Guide* for more information on DCM archiving, and Oracle Technology Network (`http://otn.oracle.com`) for the latest information on DCM

11.7 Backup and Recovery Considerations for High Availability Environments

This section provides considerations for performing backup and recovery in Oracle Application Server environments that use high availability solutions. It contains the following topics:

- Considerations for OracleAS Cold Failover Cluster
- Considerations for OracleAS Active Failover Cluster
- Considerations for OracleAS Disaster Recovery

11.7.1 Considerations for OracleAS Cold Failover Cluster

If you use OracleAS Cold Failover Cluster, you can use the procedures in this book to backup and recover your environment, with the following additional considerations:

- **Backup Considerations for OracleAS Cold Failover Cluster**
  - Oracle recommends that you locate archive logs for the Metadata Repository on the shared disk. This ensures that, when failing over from one cluster node to another in the case of media recovery, the archive logs are also failed over and available.
  - You can generate archive logs to a local filesystem, however, the same path must be available during runtime on whichever node is hosting the Infrastructure instance.

  - Proper capacity planning is required in order to ensure adequate space is available to store the desired number of archive logs.

- **Recovery Considerations for OracleAS Cold Failover Cluster**

  There are no special considerations for recovering OracleAS Cold Failover Cluster. As mentioned in the previous backup section, if archive logs are stored on a local filesystem, in the case of media recovery, all archive logs must be made available to the application server instance performing the recovery. Recovery can be performed on either node of the cluster.

  See Also: *Oracle Application Server 10g High Availability Guide* for more information on OracleAS Cold Failover Cluster

11.7.2 Considerations for OracleAS Active Failover Cluster

If you use OracleAS Active Failover Cluster (AFC), you can use the procedures in this book to backup and recover your environment, with the following additional considerations:

Note: In the initial release of Oracle Application Server 10*g* (9.0.4), Active Failover Cluster is a Limited Release feature. Please check Metalink (`http://metalink.oracle.com`) for the current certification status of this feature, or consult your Sales Representative, before deploying this feature in a production environment.

- **Backup Considerations for OracleAS Active Failover Cluster**
  - In the case of AFC where the Metadata Repository is a RAC database:
    - When you enable automatic archiving, you must perform the step on every RAC instance.
    - Enabling `ARCHIVELOG` mode is done at the database level. Make sure to shut down all RAC instances (the entire database), mount one instance, and then enable `ARCHIVELOG` mode one that instance with the `ALTER SYSTEM` command.
  - Ensure archive destinations are the same on all nodes.
  - Keep backups consistent across all AFC nodes. Perform configuration file backups and Metadata Repository backups using the OracleAS Backup and

Recovery Tool on one node. Then perform backups of only the configuration files on the additional AFC nodes.

Once the configuration files and Metadata Repository have been backed up on the first AFC node, ensure no administrative changes take place until the configuration files on the additional AFC nodes have been backed up. If any administrative changes occur before you have a chance to backup the additional AFC nodes, a new backup of all AFC nodes is required.

See Also: Appendix G, "Examples of Administrative Changes" to learn more about administrative changes

- **Recovery Considerations for OracleAS Active Failover Cluster**
  - In case of media recovery, ensure the archive logs from all AFC nodes are available in the archive log destination on the node where recovery is taking place.
  - Complete the recovery of configuration files and the Metadata Repository on one node first. Recover only the configuration files (not the Metadata Repository) on the additional AFC nodes. In an AFC Infrastructure configuration, the Metadata Repository is shared between all nodes. Once you have recovered the Metadata Repository on one node, there is no need to recover the Metadata Repository on the additional nodes.

    See Also: *Oracle Application Server 10g High Availability Guide* for more information on OracleAS Active Failover Cluster

11.7.3 Considerations for OracleAS Disaster Recovery

If you are using OracleAS Disaster Recovery, refer to the OracleAS Disaster Recovery documentation for considerations on using backup and recovery in an OracleAS Disaster Recovery environment.

See Also: *Oracle Application Server 10g High Availability Guide*

11.8 Roadmap for Getting Started with Backup and Recovery

This section provides a roadmap for getting started with Oracle Application Server backup and recovery.

1. **Learn About Database Backup and Recovery.**

The Oracle Application Server environment includes the Metadata Repository—an Oracle9*i* database. Performing backup and recovery on Oracle Application Server includes performing backup and recovery of a database. It is, therefore, important for application server administrators to understand database backup and recovery.

If you are not experienced with database backup and recovery, Oracle recommends you read *Oracle9i Backup and Recovery Concepts Release 1 (9.0.1)*, which is available in the Oracle9*i* document library.

In particular, the following topics apply to Oracle Application Server backup and recovery:

- Using `ARCHIVELOG` mode
- Performing cold database backups
- Performing online database backups
- Using the RMAN backup and recovery utility

2. **Install and Configure the OracleAS Backup and Recovery Tool.**

   Oracle recommends you install and configure the tool and familiarize yourself with its features. Even if you do not use the tool in the long run, it will help you get started with backup and recovery.

   You must install the tool into each of your Infrastructure and middle-tier installations. This is because you will customize the tool for each installation. Chapter 12, "Oracle Application Server Backup and Recovery Tool" provides instructions.

3. **Implement the Backup Strategy.**

   Chapter 13, "Backup Strategy and Procedures" outlines the Oracle-recommended backup strategy and backup procedures. Following this backup strategy ensures that you will be able to perform the recovery procedures in this book.

4. **Recover as Necessary.**

   In the event of system failure or data loss, refer to Chapter 14, "Recovery Strategies and Procedures". It outlines different types of failures and describes the procedures you can follow to recover.

12

Oracle Application Server Backup and Recovery Tool

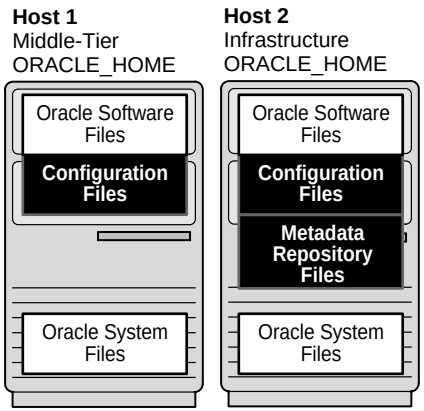
This chapter describes how to install, configure, and use the Oracle Application Server Backup and Recovery Tool (OracleAS Backup and Recovery Tool).

It contains the following topics:

12.1 What is the Oracle Application Server Backup and Recovery Tool?

The Oracle Application Server Backup and Recovery Tool (OracleAS Backup and Recovery Tool) is a Perl script and associated configuration files you can use to backup and recover configuration files and the Metadata Repository in your Oracle Application Server environment. The types of files you can back up and recover using the tool are shaded in Figure 12–1.

Figure 12–1 Files You Can Backup and Recover Using OracleAS Backup and Recovery Tool



The tool can be used in different ways, depending on your level of experience and requirements:

- At a minimum, all users can refer to the tool for the list of Oracle Application Server configuration files that must be backed up
- If you are new to backup and recovery, you can use the tool to perform configuration file and Metadata Repository backup and recovery
- If you are experienced with backup and recovery, you can refer to the tool for guidance when setting up your own configuration file and Metadata Repository backup and recovery scripts

12.2 How to Obtain the OracleAS Backup and Recovery Tool

You can obtain the Oracle Application Server Backup and Recovery Tool from the "OracleAS RepCA and Utilities" CD-ROM. The tool is located on the CD-ROM in the `utilities/backup` directory.

> **See Also:** *Oracle Application Server 10g Installation Guide* for information about the "OracleAS RepCA and Utilities" CD-ROM

12.3 How to Install the OracleAS Backup and Recovery Tool

Before you install the OracleAS Backup and Recovery Tool, review the following notes:

- You should install the tool multiple times—once for each Infrastructure and middle-tier installation in your environment. This is because you will customize the tool for each installation.

  > **Note:** You cannot use the tool on a Metadata Repository installation that was created by running OracleAS RepCA in an existing database. Refer to Section 11.5, "Assumptions and Restrictions".

- You must install the tool on the same host as its corresponding installation. You can install the tool in the Oracle home of its corresponding installation, or you can install it into a directory outside of the Oracle home.

To install the OracleAS Backup and Recovery Tool:

1. Log in as the user who installed Oracle Application Server.
2. Extract the contents of the `backup_restore.tar` file from the "OracleAS RepCA and Utilities" CD-ROM to your disk. You can install in the Oracle home, or in another directory outside of the Oracle home. For example, to install it in the Oracle home:

   ```
   cd ORACLE_HOME
   tar xvf CD_ROM/utilities/backup/backup_restore.tar
   ```

3. Make sure the `bkp_restore.pl` file has execute permission, for example:

   ```
   chmod 755 ORACLE_HOME/backup_restore/bkp_restore.pl
   ```

4. Familiarize yourself with the OracleAS Backup and Recovery Tool files, which are described in the Table 12–1. Instructions for editing the configuration files are in subsequent steps.

Table 12–1 OracleAS Backup and Recovery Tool Files

File[1]	Description
`bkp_restore.pl`	The Perl script that you execute to perform backup and recovery operations
`config/config.inp`	The main configuration file that contains parameters for customizing the tool for your environment
`config/config_<component>_files.inp`	Component configuration files—each contains a list of configuration files for a particular component. These specify which files to back up when performing a configuration file backup.
`*.tmpl`	Templates for scripts for performing database backup and recovery operations using RMAN. When you initially configure the tool, a customized `.dat` file will be created from each `.tmpl` file.
`query_dbid.sql`	A SQL script called by the tool to initialize your configuration

[1] Paths are relative to the root of the OracleAS Backup and Recovery Tool directory.

12.4 How to Configure the OracleAS Backup and Recovery Tool

This section describes how to configure the OracleAS Backup and Recovery Tool. You must follow these steps for each installation in your environment.

1. The tool writes out log files and backup files, and you must create the following directories to hold these.

   a. **Log file directory**: (Middle tier and Infrastructure) This directory holds log files created by the tool. This directory should have several megabytes of space.

   b. **Configuration file backup directory**: (Middle tier and Infrastructure) This directory hold configuration file backups. This directory should have several hundred megabytes of space.

c. **Database backup directory**: (Infrastructure only) This directory holds datafile and control files backups of the Metadata Repository, as well as archived redo logs. This directory should have several gigabytes of space.

Recommendations for creating these directories are as follows:

- Create your backup directories on a filesystem on a separate disk and, if possible, a separate disk controller, than your Oracle Application Server Oracle home. This will give you the best chance of recovering data in the event of a hardware failure.
- Make sure your backup directories are writable by the user that installed Oracle Application Server.

  For example, to create a log file directory, configuration file backup directory, and database backup directory on `/disk1`:

```
mkdir -p /disk1/backups/log_files
mkdir -p /disk1/backups/config_files
mkdir -p /disk1/backups/db_files
cd /disk1/backups
chmod 755 log_files config_files db_files
chown OracleAS_user log_files config_files db_files
```

2. Edit `config.inp` and modify the parameters as described in Table 12–2. Notice that some of the instructions are different depending on whether this is a middle-tier or Infrastructure installation.

Table 12–2 Parameters in config.inp

Parameter	Value
`oracle_home`	Specify the full path of the Oracle home.
`log_path`	Specify the full path of the log file directory.
`config_files_list`	Do not insert a value for this; leave it as `config_files_list=DO_NOT_SET`. This parameter will be updated with the appropriate list of configuration files for your installation when you run `bkp_restore.pl -m configure`.
`config_backup_path`	Specify the full path of the configuration file backup directory.

Table 12–2 (Cont.) Parameters in config.inp

Parameter	Value
install_type	Do not insert a value for this; leave is as install_type=DO_NOT_SET. This parameter will be updated with the appropriate value for your installation when you run bkp_restore.pl -m configure.
dbid	Do not insert a value for this; leave it as dbid=DO_NOT_SET. For Infrastructure installations, this value will be updated when you run bkp_restore.pl -m configure. By default, the tool obtains the dbid from the Metadata Repository. Or, you can supply a dbid in special cases involving migrating a Metadata Repository from one host to another, such as for Disaster Recovery. For middle-tier installations, this value will stay untouched.
oracle_home	**Middle-tier Installation:** Leave this line commented out. **Infrastructure:** If desired, specify an alternate pfile to use when starting up the database. Otherwise, leave the line commented out and the default pfile will be used: ■ *ORACLE_HOME*/dbs/initasdb.ora Be sure to leave the pfile entry commented out if you want to use the default because blank values are not allowed in this file.
log_path	**Middle-tier Installation:** Do not insert a value for this; leave it as database_backup_path=VALUE_NOT_SET. **Infrastructure:** Specify the full path of the database backup directory.

3. Set the ORACLE_HOME environment variable to the Oracle Application Server Oracle home.
4. If this is an Infrastructure installation:
   a. Set the ORACLE_SID environment variable to the Metadata Repository SID. The default is asdb.
   b. Make sure the Metadata Repository is started.

5. Configure the tool by running it with the `-m configure` option, for example:

```
cd BACKUP_TOOL_DIR
./bkp_restore.pl -m configure
```

This updates parameters in `config.inp` and, in the case of an Infrastructure, creates customized `.dat` files, which are used to backup, restore, and recover the Metadata Repository.

You are now ready to use the OracleAS Backup and Recovery Tool.

12.5 Customizing the Tool for Your Configuration Files

As shipped, the OracleAS Backup and Recovery Tool backs up all of the Oracle Application Server configuration files that are necessary to reconstruct an Oracle Application Server installation.You can customize the tool to include any additional files that you would like to back up regularly, or to exclude any configuration files you do not want to back up.

12.5.1 How the Tool Works When Backing Up Configuration Files

Before you customize the tool, you should understand how it works. When you use the tool to back up your configuration files, it:

1. Opens `config.inp` (unless another environment file was specified with the `-e` option) and retrieves `config_files_list`.
2. Attempts to open each file in `config_files_list` and exits with an error if it cannot open all of the files.
3. Examines the contents of `config_exclude_files.inp`. The tool will not attempt to back up the files listed in this file.
4. Walks through each file in `config_files_list` and examines the first entry in each file. This entry is the *key file*. The key file is used to determine if the component exists in this installation.
   - If the tool finds the key file, it knows the component is installed, and attempts to back up all of the entries in the file. It logs an error whenever it cannot find a file.
   - If the key file does not exist, the tool does not attempt to back up any entries in the configuration file. It logs an error to the log file and skips to the next configuration file.

12.5.2 How to Customize the Tool

Since the tool knows how to determine which configuration files exist in your installation, it is not necessary to customize the tool. However, you may want to customize the tool by:

- Adding Files to a Backup

  You may want to add your own local configuration files or any other files you would like to back up regularly, such as log files

- Excluding Files from a Backup

  You may want to exclude files from being backed up

Adding Files to a Backup

To add a files to a backup, add entries to the `config_misc_files.inp` file as follows:

- To specify a particular file:

  `${OH}/directorypath/file`

- To specify an entire directory:

  `${OH}/directorypath/`

- To use wildcards:

  `${OH}/directorypath/*.html`

You can add as many entries as you like. The `config_misc_files.inp` file is always included in the `config_files_list` in parameter in `config.inp`, so there is no need to edit `config.inp`.

Note that you do not need to specify a key file in `config_misc_files.inp`.

Excluding Files from a Backup

You can exclude files from a backup in either of the following ways:

- You can simply remove the file entry from its `config_component.inp` file.
- If you have a situation where a `config_component.inp` file specifies an entire directory to back up, and you would like to exclude a specific file from that directory, you can add an entry for that file to `config_exclude_files.inp`. The tool will back up the entire directory

except for the file you specify. You cannot specify directories or use wildcards in `config_exclude_files.inp`—only single file entries are allowed.

Note that you do not need to specify a key file in `config_exclude_files.inp`.

12.6 OracleAS Backup and Recovery Tool Usage Summary

This section summarizes usage for the OracleAS Backup and Recovery Tool.

It contains the following topics:

- Prerequisites for Running the Tool
- Syntax
- Usage Examples

12.6.1 Prerequisites for Running the Tool

Before running the OracleAS Backup and Recovery Tool:

- Log in as the user that installed Oracle Application Server.
- Make sure the `ORACLE_HOME` environment variable is set.
- If you are performing a database backup, make sure the `ORACLE_SID` environment variable is set. The default is `asdb`.
- Change (`cd`) to the directory in which the tool resides.

12.6.2 Syntax

The syntax for the OracleAS Backup and Recovery Tool is:

```
bkp_restore.pl [-defsv] -m mode [args]
```

It accepts the following options:

`-d` Print a trace without executing.
`-e` Specify an environment file (default is `config.inp`).
`-f` Force log file, database backup, and configuration file directories to be created if they are required by the current command and do not exist.
`-s` Run in silent mode.
`-v` Run in verbose mode.

Use the -m option to specify which mode to run. Some modes take arguments. Table 12–3 describes the OracleAS Backup and Recovery Tool modes and their arguments. All modes and arguments are case-sensitive.

Table 12–3 Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
`backup_cold`	Performs a complete cold backup of the Metadata Repository. ■ Opens `config.inp` (or the alternate file specified with the `-e` option) and retrieves `log_path`. ■ Shuts down the database, starts it in mounted mode, but does not open it. ■ Performs a backup of the datafiles and control files using RMAN. The commands are in `backup_cold.dat`. ■ Stores the backup in the directory specified in `backup_cold.dat`. (This is usually set to the `database_backup_path` in `config.inp`.) ■ Stores a log file in `log_path`. ■ Opens the database.
`backup_cold_incr` `-l` *`incr_backup_level`*	Performs an incremental backup of the Metadata Repository. Works the same as `backup_cold`, except: ■ The `-l` option specifies the increment level (`0 - 4`). ■ Uses the `backup_cold_incr`*`level`*`.dat file` There are two types of incremental backups, cumulative and differential. The tool uses the default type, which is differential. For more information, refer to *Oracle9i Recovery Manager User's Guide* in the Oracle9*i* Documentation Library.

Table 12–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
`backup_config`	Performs a full configuration file backup. ■ Opens `config.inp` (or the alternate file specified with the `-e` option) and retrieves `config_files_list`, `config_backup_path`, and `log_path`. ■ Attempts to open each file in `config_files_list`. Exits with an error if it cannot open all of the files. ■ For each file in `config_files_list`, checks if the first entry (the key file) exists. If it does not exist, assumes this component does not exist and moves on to the next file. Otherwise, backs up all files in the list. If any files do not exist, logs an error and continues. ■ Excludes files listed in `config_exclude_files.inp`. ■ When finished, stores the backup in *`config_backup_path`*`/config_bkp_`*`timestamp`*. ■ If any errors are encountered, creates a log file in *`log_path`*`/config_bkp_`*`timestamp`*.
`backup_config_incr`	Performs an incremental configuration file backup. Works the same as `backup_config`, except: ■ Backs up all configuration files that have changed since the last full or incremental configuration file backup.
`backup_online`	Performs an online backup of the Metadata Repository. ■ Opens `config.inp` (or the alternate file specified with the `-e` option) and retrieves `log_path`. ■ Assumes the database is open. ■ Performs a backup of the datafiles and control files using RMAN. The commands are in `backup_online.dat`. ■ Stores the backup in the directory specified in `backup_online.dat`. (This is usually set to the `database_backup_path` in `config.inp`.) ■ Stores a log file in `log_path`. ■ Leaves the database open.

Table 12–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
`backup_online_incr` `-l` *`incr_backup_level`*	Performs an incremental online backup of the Metadata Repository. Works the same as `backup_online`, except: ■ The `-l` option specifies the increment level (`0 - 4`). ■ Uses the `backup_online_incr`*`level`*`.dat file` There are two types of incremental backups, cumulative and differential. The tool uses the default type, which is differential. For more information, refer to *Oracle9i Recovery Manager User's Guide* in the Oracle9*i* Documentation Library.
`configure` `[-i` *`dbid`*`]`	Configures the tool. When using this on an Infrastructure, make sure the Metadata Repository is up before you run this command. ■ Updates `config_files_list` and `install_type` in `config.inp` with the appropriate information for your installation. ■ If using this on an Infrastructure, updates the configuration file with the database id (`dbid`) and creates customized `*.dat` files from the database backup `*.tmpl` files. By default, it queries the Metadata Repository for the `dbid`. If you use the `-i` option, you can supply the `dbid` (this is used for migrating the Metadata Repository from one node to another, such as for Disaster Recovery).
`configure_nodb`	Same as "`configure`" but does not perform the Infrastructure configuration. Note: You should use "`configure`" for all middle-tier and Infrastructure installations; "`configure_nodb`" applies to disaster recovery strategies described in *Oracle Application Server 10g High Availability Guide*.
`help`	Prints a usage message.
`list_changed_config`	Lists any configuration files that have changed since the last full or incremental backup. This command checks the modification date of each file; it doesn't check the actual contents of the file. It writes the list of files to a log file and prints the name of the log file.

Table 12–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description

`restore_config`
`[-t config_bkp_`*`timestamp`*`]`
`[-n]`
	Restores configuration files.
	■ Opens `config.inp` (or the alternate file specified with the `-e` option) and retrieves `config_backup_path` and `log_path`.
	■ If the `-t` option is supplied and it is the timestamp from a full backup, it restores that full backup.
	■ If the `-t` option is supplied and it is the timestamp from an incremental backup, it restores the full backup and all incremental backups up to and including the specified incremental backup.
	■ If the `-t` option is not supplied, displays a list of configuration file backups in `config_backup_path` and exits. You can then rerun the command and supply one of these files with the `-t` option.
	■ Restores all files from the configuration file backup to the Oracle home, preserving owner, group, permissions, and timestamp.
	■ If any errors are encountered, creates a log file in *`log_path`*/config_rst_*`timestamp`*.
	The `-n` option suppresses prompts so you can use the tool in batch mode.

`restore_db` `[-u `*`timestamp`*`][-c][-n]`	Restores and recovers the Metadata Repository from the available cold and online backups. ■ Opens `config.inp` (or the alternate file specified with the `-e` option) and retrieves `log_path`. ■ Restores the control files and datafiles, and performs recovery using RMAN. The commands are in `restore_db.dat`. ■ Stores a log file in `log_path`. ■ Leaves the database open. By default, this command restores and recovers the database to its most recent state. You can use the `-u` option to restore and recover the database to its state at a particular point in time. For example: `bkp_restore.pl -m restore_db -u 7/26/2003_13:45:06` By default, this command does not restore the control file. You can use the `-c` option to restore the control file. If you use the `-u` or `-c` option, be sure to do a full backup right away because all past backups are invalidated. The `-n` option suppresses prompts so you can use the tool in batch mode. Refer to Section 12.7, "Best Practices for Restoring and Recovering the Metadata Repository" for more information.

12.6.3 Usage Examples

This section contains usage examples for the OracleAS Backup and Recovery Tool.

- Configure the tool using the default `config.inp` file:

  ```
  bkp_restore.pl -m configure
  ```

- Configure the tool using a configuration file called `myconfig.inp`:

  ```
  bkp_restore.pl -m configure -e myconfig.inp
  ```

- Perform a full configuration file backup:

  ```
  bkp_restore.pl -v -m backup_config
  ```

- Perform a full configuration file backup using an environment file called `myconfig.inp`:

  ```
  bkp_restore.pl -v -m backup_config -e myconfig.inp
  ```

- Perform an incremental configuration file backup:

  ```
  bkp_restore.pl -v -m backup_config_incr
  ```

- Restore configuration files.

  ```
  bkp_restore.pl -m restore_config -t config_bkp_2003-02-27_13-45
  ```

- Perform a full cold backup of the Metadata Repository:

  ```
  bkp_restore.pl -m backup_cold
  ```

- Perform a level 2 incremental cold backup of the Metadata Repository:

  ```
  bkp_restore.pl -m backup_cold_incr -l 2
  ```

- Perform an full online backup of the Metadata Repository:

  ```
  bkp_restore.pl -m backup_online
  ```

- Perform a level 0 incremental online backup of the Metadata Repository:

  ```
  bkp_restore.pl -m backup_online_incr -l 0
  ```

- Restore the Metadata Repository to its most recent state:

  ```
  bkp_restore.pl -m restore_db
  ```

- Restore the Metadata Repository to its state at a particular time:

```
bkp_restore.pl -m restore_db -u 7/26/2003_13:45:06
```

12.7 Best Practices for Restoring and Recovering the Metadata Repository

This section describes best practice tips for using the OracleAS Backup and Recovery Tool to restore and recover the Metadata Repository. It contains the following sections:

- Restoring and Recovering the Metadata Repository to the Same Host
- Restoring and Recovering the Metadata Repository to a New Host

> **Note:** This best practices in this section use the OracleAS Backup and Recovery Tool. There are many other options available for restoring and recovering a database when you use the RMAN command directly. For more information, refer to *Oracle9i Recovery Manager User's Guide* in the Oracle9*i* documentation library.

12.7.1 Restoring and Recovering the Metadata Repository to the Same Host

This section covers several circumstances under which you may need to restore and recover the Metadata Repository to the same host:

- Corrupted or Lost Datafile
- Corrupted or Lost Control File
- Point-in-time Recovery

Corrupted or Lost Datafile

If a datafile is corrupted or lost, you can use the following command to restore from the latest backup and perform a full recovery:

```
bkp_restore.pl -m restore_db
```

Corrupted or Lost Control File

If a control file is corrupted or lost, you can use the following command to restore a control file backup, restore the datafiles, and perform a full recovery:

```
bkp_restore.pl -m restore_db -c
```

When you use the `-c` option, it restores the control file. This causes entries for tempfiles in locally-managed temporary tablespaces to be removed. You must add a new tempfile to the TEMP tablespace, or Oracle will display error ORA-25153: Temporary Tablespace is Empty.

To add a tempfile to the TEMP tablespace:

```
SQL> alter tablespace "TEMP" add tempfile 'ORACLE_HOME/oradata/GDB/temp01.dbf'
size 5120K autoextend on next 8k maxsize unlimited;
```

GDB is the first part of the global database name.

Note that when you restore a control file, the tool performs an "alter database open resetlogs." This invalidates all backups and archivelogs. You should immediately perform a complete cold backup of the Metadata Repository, which will serve as the new baseline for your subsequent partial online backups.

Point-in-time Recovery

If you lost configuration files in your middle-tier or Infrastructure installation and restored those, you may want to restore the database to the same point-in-time as the configuration file backup. You can do this using the following command:

```
bkp_restore.pl -m restore_db -u timestamp
```

You can specify any time between the time of your first backup and the current time, as long as none of the online redo logs were compromised. If any online redo logs are missing or corrupted, the latest time that can be specified is the time at which the last backup was made.

Note that when you do point-in-time recovery, the tool performs an "alter database open resetlogs." This invalidates all backups and archivelogs. You should immediately perform a complete cold backup of the Metadata Repository, which will serve as the new baseline for your subsequent partial online backups.

12.7.2 Restoring and Recovering the Metadata Repository to a New Host

When you restore the Metadata Repository to a new host (with the same hostname and IP address), the new host will not have the online redo logs that existed on the original host. Therefore, you cannot perform a full recovery—RMAN would give an error stating that it cannot find a certain log file (the online redo log file). Instead, you should do a point-in-time recovery using a time sometime between the first and most recent backup. You can do this using the following command:

```
bkp_restore.pl -m restore_db -c -u timestamp
```

If this command returns an error and the log shows that the datafiles were restored and recovered, then issue an "alter database open resetlogs" and the database will be opened in a consistent state. If no datafiles were restored and recovered, it is most likely an early timestamp was specified and you should retry the command with a later timestamp.

When you use the `-c` option, it restores the control file. This causes entries for tempfiles in locally-managed temporary tablespaces to be removed. You must add a new tempfile to the TEMP tablespace, or Oracle will display error ORA-25153: Temporary Tablespace is Empty.

To add a tempfile to the TEMP tablespace:

```
SQL> alter tablespace "TEMP" add tempfile 'ORACLE_HOME/oradata/GDB/temp01.dbf'
size 5120K autoextend on next 8k maxsize unlimited;
```

GDB is the first part of the global database name.

Note that whenever you restore the Metadata Repository to a new host, the control file will be restored from backup. This means that an "alter database open resetlogs" is always done, which invalidates all backups and archivelogs. You should immediately perform a complete cold backup of the Metadata Repository, which will serve as the new baseline for your subsequent partial online backups.

12.8 Error Messages You Can Ignore

This section lists OracleAS Backup and Recovery Tool error messages you can ignore for certain configurations.

- When performing a configuration file backup in a Metadata Repository-only installation, you can ignore the following error message:

  ```
  Could not copy ORACLE_HOME/Apache/Apache/conf/osso/osso.conf to
  BACKUP_DIR/Apache/Apache/conf/osso/osso.conf: No such file or directory
  ```

- When performing a configuration file backup in a J2EE and Web Cache installation that does not use Identity Management, you can ignore the following error message:

  ```
  Could not copy ORACLE_HOME/Apache/Apache/conf/osso/osso.conf to
  BACKUP_DIR/Apache/Apache/conf/osso/osso.conf: No such file or directory
  ```

- When performing a configuration file backup in an OracleAS TopLink installation in which you have not yet opened the Mapping Workbench and created a project, you can ignore the following error message:

  ```
  Could not copy ORACLE_HOME/toplink/config/workbench.xml to
  BACKUP_DIR/toplink/config/workbench.xml: No such file or directory
  ```

13

Backup Strategy and Procedures

This chapter describes the Oracle Application Server backup strategy and procedures.

It contains the following topics:

13.1 Backup Strategy

This section describes the backup strategy for Oracle Application Server. Using this strategy ensures that you can perform the recovery procedures described in this book.

The backup strategy is as follows:

- Step 1: Perform a Complete Oracle Application Server Environment Backup
- Step 2: Perform Online Backups on a Regular Basis
- Step 3: Perform a New Complete Oracle Application Server Environment Backup After a Major Change
- Step 4: Perform Online Backups on a Regular Basis (Return to Step 2)

Step 1: Perform a Complete Oracle Application Server Environment Backup

The first backup you perform should be a complete Oracle Application Server environment backup, which includes all of the files in your environment. Before you perform your first backup, make sure `ARCHIVELOG` mode is enabled in the Metadata Repository. You should also create a record of your environment.

1. Enable `ARCHIVELOG` mode in the Metadata Repository.

   By default, the Metadata Repository does not have `ARCHIVELOG` mode enabled. You should enable it immediately so your online redo logs are archived. You should enable `ARCHIVELOG` mode before you perform your first complete cold backup. Otherwise, your backup control files will contain the `NOARCHIVELOG` mode setting.

   Refer to Section 13.2.1, "Enabling ARCHIVELOG Mode".

2. Perform a complete Oracle Application Server environment backup.

   This will serve as the baseline for all subsequent online backups.

   Refer to Section 13.2.3, "Performing a Complete Oracle Application Server Environment Backup".

3. Create a record of your Oracle Application Server environment.

   In the event you need to reconstruct your environment, you can refer this record.

   Refer to Section 13.2.2, "Creating a Record of Your Oracle Application Server Configuration".

Step 2: Perform Online Backups on a Regular Basis

After every administrative change, or, if this is not possible, on a regular basis, perform an online backup of your Oracle Application Server environment.

> **See Also:** Appendix G, "Examples of Administrative Changes" to learn more about administrative changes

Refer to Section 13.2.4, "Performing an Online Backup".

Step 3: Perform a New Complete Oracle Application Server Environment Backup After a Major Change

If you make a major change to your Oracle Application Server environment, you must perform a new complete Oracle Application Server environment backup. This backup will serve as the basis for subsequent online backups. You should also update the record of your environment with the new configuration information.

Perform a new complete Oracle Application Server environment backup after:

- An operating system software upgrade
- An Oracle Application Server software upgrade or patch application

To do so:

1. Update the record of your Oracle Application Server environment.

   Refer to Section 13.2.2, "Creating a Record of Your Oracle Application Server Configuration".

2. Perform a complete Oracle Application Server environment backup.

   Refer to Section 13.2.3, "Performing a Complete Oracle Application Server Environment Backup".

Step 4: Perform Online Backups on a Regular Basis (Return to Step 2)

After you establish a new complete Oracle Application Server environment backup, return to Step 2 and continue to perform online backups on a regular basis.

Additional Tips:

- Create a backup of the JRE/JDK on your system. This isn't an Oracle product, but it is utilized by Oracle Application Server and, if accidentally lost or corrupted, would need to be restored in order for Oracle Application Server to function. This issue only applies to HP-UX, HP Tru64, and IBM AIX systems.

- Make sure your backups are valid by routinely verifying that they can be restored.

13.2 Backup Procedures

This section describes the backup procedures in detail.

It contains the following topics:

13.2.1 Enabling ARCHIVELOG Mode

By default, the Metadata Repository does not have ARCHIVELOG mode enabled. You must enable ARCHIVELOG mode, which enables the archiving of online redo logs. This will allow you to perform the recovery strategies in this book.

See Also: You can find more detailed information on the parameters in this section, and setting up archive logging in general, in *Oracle9i Database Administrator's Guide Release 1 (9.0.1)*.

To enable ARCHIVELOG mode:

1. Enable automatic archiving by editing the following initialization file:

   INFRA_ORACLE_HOME/dbs/init<SID>.ora

   a. (Mandatory) Enable automatic archiving each time an instance is started by including the initialization parameter LOG_ARCHIVE_START in the initialization file and set it to TRUE:

      ```
      LOG_ARCHIVE_START = TRUE
      ```

   b. (Mandatory) Specify the destination directory for your archives by including the initialization parameter LOG_ARCHIVE_DEST in the initialization file, for example:

      ```
      LOG_ARCHIVE_DEST = 'LOCATION = /disk1/oraHome/archive'
      ```

c. (Optional) The default filename format for archive logs is:

```
%t_%s.dbf
```

If you would like to use a different format, include the initialization parameter LOG_ARCHIVE_FORMAT in the initialization file, for example:

```
LOG_ARCHIVE_FORMAT = arch%s.dbf
```

2. Make sure the ORACLE_HOME and ORACLE_SID (the default is asdb) environment variables are properly set.
3. Make sure nobody is using the database.
4. Perform a clean, normal shutdown of the database instance.

```
INFRA_ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> shutdown
```

5. Start up the instance and mount, but do not open, the database.

```
SQL> startup mount;
```

6. Enable database ARCHIVELOG mode.

```
SQL> alter database archivelog;
```

7. Shut down and restart the database instance.

```
SQL> shutdown
SQL> startup
```

8. Verify the database is now in ARCHIVELOG mode.

Execute the following command and verify that Database log mode is Archive Mode and Automatic archival is Enabled.

```
SQL> archive log list;
Database log mode           Archive Mode
Automatic archival          Enabled
Archive destination         /disk1/oraHome/archive
Oldest on-line log sequence 19
Next log sequence to archive 21
Current log sequence        21
```

13.2.2 Creating a Record of Your Oracle Application Server Configuration

In the event you need to restore and recover your Oracle Application Server environment, it is important to have all the necessary information at your disposal. This is especially true in the event of a hardware loss that requires you to reconstruct all or part of your Oracle Application Server environment on a new disk or host.

You should maintain an up-to-date record of your Oracle Application Server environment that includes the information listed in this section. You should keep this information both in hardcopy and electronic form. The electronic form should be stored on a host or email system that is completely separate from your Oracle Application Server environment.

Your Oracle Application Server hardware and software configuration record should include:

- The following information for each host in your environment:
  - Hostname
  - Virtual hostname (if any)
  - Domain name
  - IP address
  - Hardware platform
  - Operating system release level and patch information
- The following information for each Oracle Application Server installation in your environment:
  - Installation type (For example: Infrastructure or J2EE and Web Cache)
  - Host on which the installation resides
  - User name, userid number, group name, groupid number, environment profile, and type of shell for the operating system user that owns the Oracle home (`/etc/passwd` and `/etc/group` entries)
  - Directory structure, mount points, and full path for `ORACLE_HOME`
  - Amount of disk space used by the installation
  - Port numbers used by the installation

> **Note:** *ORACLE_HOME*`/install/portlist.ini` contains the port numbers assigned during installation. However, this file is not updated if you change port numbers after installation, so you need to keep track of those changes manually.

- The following information for the Metadata Repository:
  - Database version and patch level
  - Base language
  - Character set
  - Global database name
  - SID

13.2.3 Performing a Complete Oracle Application Server Environment Backup

This section describes how to perform a complete Oracle Application Server environment backup. It contains the following steps:

- Step 1: Shut Down Your Oracle Application Server Environment
- Step 2: Back Up the Infrastructure
- Step 3: Back Up the Middle-tier Installations
- Step 4: Back Up the DCM File-based Repository (If Required)
- Step 5: Back Up the Oracle System Files
- Step 6: Start Your Oracle Application Server Environment

Step 1: Shut Down Your Oracle Application Server Environment

1. Stop the middle-tier instances.

   Refer to Section 3.2.4, "Stopping a Middle-Tier Instance" for instructions.

2. Stop the Infrastructure.

   Refer to Section 3.2.2, "Stopping an Infrastructure" for instructions.

Step 2: Back Up the Infrastructure

1. Perform a cold database backup of the Metadata Repository.

You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd INFRA_BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m backup_cold
```

Note that the tool leaves the database running when finished. Shut down the database before continuing with the rest of these steps.

> **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information

2. Back up the Infrastructure Oracle home.

> **Note:** If your Infrastructure is split and has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes.

Perform a complete backup of all files in the Infrastructure Oracle home using your preferred operating system command, such as `tar` or `cpio`.

Be sure to perform this backup as root because some of the files in the Oracle home are owned by root. It is important to perform the backup so that file owners, groups, permissions, and timestamps are preserved.

For example:

```
cd INFRA_ORACLE_HOME
tar cvf full_path_of_backup_file .
```

3. Back up the Infrastructure configuration files.

> **Note:** If your Infrastructure is split and has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes.

Perform a backup of all configuration files in the Infrastructure Oracle home. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd INFRA_BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m backup_config
```

> **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information.

> **Note:** The tool may report harmless error messages in some configurations. Refer to Section 12.8, "Error Messages You Can Ignore".

The reason for doing a configuration file backup immediately after backing up the entire Oracle home is that it provides a snapshot of your initial configuration files. You can use this if you start to reconfigure your system and then would like to restore the configuration files to their original state.

Step 3: Back Up the Middle-tier Installations

For each middle-tier installation in your environment:

1. Back up the middle-tier Oracle home.

   Perform a complete backup of all files in the middle-tier Oracle home using your preferred operating system command, such as `tar` or `cpio`.

   Be sure to perform this backup as root because some of the files in the Oracle home are owned by root. It is important to perform the backup so that file owners, groups, permissions, and timestamps are preserved.

   For example:

   ```
   cd MID_TIER_ORACLE_HOME
   tar cvf full_path_of_backup_file .
   ```

2. Back up the middle-tier configuration files.

   Perform a backup of all configuration files in the middle-tier Oracle home. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

   ```
   cd MID_TIER_BACKUP_TOOL_DIRECTORY
   ./bkp_restore.pl -m backup_config
   ```

   > **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information.

> **Note:** The tool may report harmless error message in some configurations. Refer to Section 12.8, "Error Messages You Can Ignore".

The reason for doing a configuration file backup immediately after backing up the entire Oracle home is that it provides a snapshot of your initial configuration files, in case you start to reconfigure your system and then would like to restore the configuration files to their original state.

3. Create a DCM archive.

   Create a DCM archive of the middle-tier instance:

   ```
   ORACLE_HOME/dcm/bin/dcmctl createArchive -archive archive_name
   ```

   Export the archive from the DCM repository to a backup location:

   ```
   ORACLE_HOME/dcm/bin/dcmctl exportArchive -archive archive_name -f
   file_name.jar
   ```

   Make sure no configuration changes take place between the configuration file backup in step 2 and DCM archive in this step.

   See Also: Section 11.6.2, "Considerations for DCM Archives"

Step 4: Back Up the DCM File-based Repository (If Required)

Perform this step only if you are using a DCM file-based repository.

If you have a DCM file-based repository, it exists in one of your middle-tier installations, known as the *repository host instance*. You should back up (export) the DCM file-based repository by running this command in the Oracle home of the repository host instance:

```
ORACLE_HOME/dcm/bin/dcmctl exportRepository -file file_name
```

Oracle recommends you copy the repository backup file to a different host, or some other backup media. You will need this file to recover in the event of a lost host.

See Also: Section 11.6.1, "Considerations for DCM File-based Repositories"

Step 5: Back Up the Oracle System Files

On each host in your Oracle Application Server environment:

1. Make a backup of your Oracle system files using your preferred operating system command, such as `tar` or `cpio`.

   Consult your operating system-specific documentation to determine which directory contains your Oracle system files. For example, on UNIX systems, they may be in the `/var/opt/oracle` or `/etc` directory.

2. If the `oraInventory` directory resides outside of your Oracle Application Server Oracle home, make a backup of it using your preferred operating system command, such as `tar` or `cpio`.

   If you are not sure of the location of your `oraInventory` directory, you can find it in the `oraInst.loc` file. For example, on UNIX systems, look in `/var/opt/oracle/oraInst.loc` or `/etc/oraInst.loc`.

Step 6: Start Your Oracle Application Server Environment

1. Start the Infrastructure.

   Refer to Section 3.2.1, "Starting an Infrastructure" for instructions.

2. Start the middle-tier instances.

   Refer to Section 3.2.3, "Starting a Middle-Tier Instance" for instructions.

13.2.4 Performing an Online Backup

Once you have performed a complete Oracle Application Server environment backup, you should perform subsequent online backups after every administrative change, or, if this is not possible, on a regular basis.

> **See Also:** Appendix G, "Examples of Administrative Changes" to learn more about administrative changes

These backups can be performed online (while Oracle Application Server is up and running), and only contain configuration files and the Metadata Repository.

This section describes how to perform an online backup of your Oracle Application Server environment. It contains the following steps:

- Step 1: Back Up the Infrastructure
- Step 2: Back Up the Middle-tier Installations
- Step 3: Back Up the DCM File-based Repository (If Required)

Step 1: Back Up the Infrastructure

1. Perform an incremental backup of the configuration files.

   You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

   ```
   cd INFRA_BACKUP_TOOL_DIRECTORY
   ./bkp_restore.pl -m backup_config_incr
   ```

   See Also: Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information

   Note: The tool may report harmless error message in some configurations. Refer to Section 12.8, "Error Messages You Can Ignore".

2. Perform an online database backup of the Metadata Repository.

   You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

   ```
   cd INFRA_BACKUP_TOOL_DIRECTORY
   ./bkp_restore.pl -m backup_online
   ```

   See Also: Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information

Step 2: Back Up the Middle-tier Installations

For each middle-tier installation in your environment:

1. Perform an incremental backup of configuration files.

   You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

   ```
   cd MID_TIER_BACKUP_TOOL_DIRECTORY
   ./bkp_restore.pl -m backup_config_incr
   ```

   See Also: Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information

> **Note:** The tool may report harmless error message in some configurations. Refer to Section 12.8, "Error Messages You Can Ignore".

2. Create a DCM archive.

   Create a DCM archive of the middle-tier instance:

   ```
   ORACLE_HOME/dcm/bin/dcmctl createArchive -archive archive_name
   ```

   Export the archive from the DCM repository to a backup location:

   ```
   ORACLE_HOME/dcm/bin/dcmctl exportArchive -archive archive_name -f
   file_name.jar
   ```

   Make sure no configuration changes take place between the configuration file backup in the previous step and DCM archive in this step.

   > **See Also:** Section 11.6.2, "Considerations for DCM Archives"

Step 3: Back Up the DCM File-based Repository (If Required)

Perform this step only if you are using a DCM file-based repository.

If you have a DCM file-based repository, it exists in one of your middle-tier installations, known as the *repository host instance*. You should back up (export) the DCM file-based repository by running this command in the Oracle home of the repository host instance:

```
ORACLE_HOME/dcm/bin/dcmctl exportRepository -file file_name
```

Oracle recommends you copy the repository backup file to a different host, or some other backup media. You will need this file to recover in the event of a lost host.

> **See Also:** Section 11.6.1, "Considerations for DCM File-based Repositories"

14

Recovery Strategies and Procedures

This chapter describes Oracle Application Server recovery strategies and procedures for different types of failures and outages.

It contains the following topics:

14.1 Recovery Strategies

This section describes Oracle Application Server recovery strategies for different types of failures and outages. It contains the following topics:

- Recovery Strategies for Data Loss, Host Failure, or Media Failure (Critical)
- Recovery Strategies for Process Crashes and System Outages (Non-Critical)

14.1.1 Recovery Strategies for Data Loss, Host Failure, or Media Failure (Critical)

This section describes recovery strategies for outages that involve actual data loss or corruption, host failure, or media failure where the host or disk cannot be restarted and are permanently lost. This type of failure requires some type of data restoration before the Oracle Application Server environment (middle tier, Infrastructure, or both) can be restarted and continue with normal processing.

The strategies in this section use point-in-time recovery of the middle tier and Infrastructure. This means that, no matter where the loss occurred, the middle tier and Infrastructure are always restored together so they are in sync as they were at the time of the last backup.

Assumptions

The following assumptions apply to the recovery strategies in this section:

- `ARCHIVELOG` mode was enabled for all Metadata Repository backups.
- Complete recovery of the database can be performed, that is, no redo log files have been lost.
- No administrative changes were made since the last backup. If administrative changes were made since the last backup, they will need to be reapplied after recovery is complete.

  See Also: Appendix G, "Examples of Administrative Changes" to learn more about administrative changes

Determining Which Strategy To Use

Recovery strategies are listed in the following tables:

- Table 14–1, " Recovery Strategies for Data Loss, Host Failure, and Media Failure in Infrastructures"

  Use this table if you experience data loss, host failure, or media failure in an Infrastructure installation. Find the type of loss and follow the recommended

procedure. The procedures apply to Infrastructure that are installed into a single Oracle home, as well as Infrastructures with Identity Management in one Oracle home and a Metadata Repository in another Oracle home or host.

- Table 14–2, " Recovery Strategies for Data Loss, Host Failure, and Media Failure in Middle-tier Instances"

  Use this table if you experience data loss, host failure, or media failure in a middle-tier installation. Find the type of loss and follow the recommended procedure.

If the loss occurred in both the Infrastructure and middle tier, follow the Infrastructure recovery strategy first, then the middle tier.

Table 14–1 Recovery Strategies for Data Loss, Host Failure, and Media Failure in Infrastructures

Type of Loss	Recovery Strategies
Loss of host	You can restore to a new host that has the same hostname and IP address. Follow the procedure in Section 14.2.2, "Restoring an Infrastructure to a New Host".
Oracle software / binary loss or corruption	If any Oracle binaries have been lost or corrupted, you must recover the entire Infrastructure. Follow the procedure in Section 14.2.1, "Restoring an Infrastructure to the Same Host".
Database or data failure of the Metadata Repository (datafile loss, control file loss, media failure, disk corruption)	If the Metadata Repository is corrupted due to data loss or media failure, you can restore and recover it. Follow the procedure in Section 14.2.3, "Restoring and Recovering the Metadata Repository".
Deletion or corruption of configuration files	If you lose any configuration files in the Infrastructure Oracle home, you can restore them. Follow the procedure in Section 14.2.4, "Restoring Infrastructure Configuration Files".
Deletion or corruption of configuration files and data failure of the Metadata Repository	If you lose configuration files and the Metadata Repository is corrupted, you can restore and recover both. Follow these procedures: 1. Section 14.2.4, "Restoring Infrastructure Configuration Files" 2. Section 14.2.3, "Restoring and Recovering the Metadata Repository"

Table 14–2 Recovery Strategies for Data Loss, Host Failure, and Media Failure in Middle-tier Instances

Type of Loss	Recovery Strategies
Loss of host	If the host has been lost, you have two options: ■ You can restore to a new host that has the same hostname and IP address. ■ You can restore to a new host that has a different hostname and IP address. In either case, follow the procedure in Section 14.2.6, "Restoring a Middle-tier Installation to a New Host". Note that if the original host had a middle-tier installation and an Infrastructure, you cannot restore the middle-tier to a host with a different hostname or IP address.
Oracle software/binary deletion or corruption	If any Oracle binaries have been lost or corrupted, you must restore the entire middle tier to the same host. Follow the procedure in Section 14.2.5, "Restoring a Middle-tier Installation to the Same Host".
Deletion or corruption of configuration files	If you lose any configuration files in the middle tier Oracle home, you can restore them. Follow the procedure in Section 14.2.7, "Restoring Middle-tier Configuration Files".

14.1.2 Recovery Strategies for Process Crashes and System Outages (Non-Critical)

This section describes recovery strategies for process crashes and system outages. These types of outages do not involve any data loss, and therefore do not require any files to be recovered. In some cases, failure may be transparent and no manual intervention is required to recover the failed component. However, in some cases, manual intervention is required to restart a process or component. While these strategies do not strictly fit into the category of backup and recovery, they are included in this book for completeness.

Determining Which Strategy to Use

Recovery strategies for process crashes and system outages are listed in the following tables:

- Table 14–3, " Recovery Strategies for Process Crashes and System Outages in Infrastructures"

  Use this table if you experience crash or outage in an Infrastructure. Find the type of outage and follow the recommended procedure. The procedures apply to Infrastructures that are installed into a single Oracle home, as well as Infrastructures with Identity Management in one Oracle home and a Metadata Repository in another Oracle home or host.

- Table 14–4, " Recovery Strategies for Process Crashes and System Outages in Middle-tier Instances"

  Use this table if you experience a crash or outage on a middle-tier installation. Find the type of outage and follow the recommended procedure.

Table 14–3 Recovery Strategies for Process Crashes and System Outages in Infrastructures

Type of Outage	How to Check Status and Restart
Host crash - no data loss	**To restart:** **1.** Reboot the host **2.** Start the Infrastructure. Refer to Section 3.2.1, "Starting an Infrastructure".

Metadata Repository instance failure (loss of the contents of a buffer cache or data residing in memory)	**To check status:**
	1. Try connecting to the database using SQL*Plus.
	2. Check the state as follows:
	`SQL> select status from v$instance;`
	To restart:
	ORACLE_HOME`/bin/sqlplus /nolog`
	`SQL> connect sys/`*password*` as sysdba`
	`SQL> startup`
	`SQL> quit`

Metadata Repository listener failure	**To check status:** *ORACLE_HOME*`/bin/lsnrctl status` **To restart:** *ORACLE_HOME*`/bin/lsnrctl start`
Oracle Internet Directory server process (`oidldapd`) failure	**To check status:** *ORACLE_HOME*`/ldap/bin/ldapcheck` **To restart:** *ORACLE_HOME*`/opmn/bin/opmnctl startproc ias-component=OID`
Oracle Internet Directory monitor process (`oidmon`) failure	**To check status:** *ORACLE_HOME*`/ldap/bin/ldapcheck` **To restart:** *ORACLE_HOME*`/opmn/bin/opmnctl startproc ias-component=OID`
Application Server Control failure	**To check status:** *ORACLE_HOME*`/bin/emctl status iasconsole` **To restart:** *ORACLE_HOME*`/bin/emctl start iasconsole`

Table 14–3 (Cont.) Recovery Strategies for Process Crashes and System Outages in Infrastructures

Type of Outage	How to Check Status and Restart
Oracle HTTP Server process failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl startproc ias-component=HTTP_Server
OC4J instance failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl startproc process-type=*OC4J_instance_name*
DAS instance failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl startproc ias-component=OC4J process-type=OC4J_SECURITY
OPMN daemon failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl start

Table 14–4 Recovery Strategies for Process Crashes and System Outages in Middle-tier Instances

Type of Outage	How to Check Status and Restart
Host crash - no data loss	**To restart:** **1.** Reboot Host **2.** Start the middle tier. Refer to Section 3.2.3, "Starting a Middle-Tier Instance"
Application Server Control failure	**To check status:** *ORACLE_HOME*/bin/emctl status iasconsole **To restart:** *ORACLE_HOME*/bin/emctl start iasconsole
Oracle HTTP Server process failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl startproc ias-component=HTTP_Server
OC4J instance failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl startproc process-type=*OC4J_instance_name*
OPMN daemon failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl start
OracleAS Web Cache failure	**To check status:** *ORACLE_HOME*/opmn/bin/opmnctl status **To restart:** *ORACLE_HOME*/opmn/bin/opmnctl startproc ias-component=WebCache

14.2 Recovery Procedures

This section contains the procedures for performing different types of recovery.

It contains the following topics:

- Restoring an Infrastructure to the Same Host
- Restoring an Infrastructure to a New Host
- Restoring and Recovering the Metadata Repository
- Restoring Infrastructure Configuration Files
- Restoring a Middle-tier Installation to the Same Host
- Restoring a Middle-tier Installation to a New Host
- Restoring Middle-tier Configuration Files

14.2.1 Restoring an Infrastructure to the Same Host

This section describes how to restore an Infrastructure to the same host. You can use this procedure when you have lost some or all of your Oracle binaries.

It contains the following steps:

- Step 1: Stop the Infrastructure
- Step 2: Restore the Infrastructure Oracle Home
- Step 3: Restore Infrastructure Configuration Files
- Step 4: Restore and Recover the Metadata Repository
- Step 5: Start the Infrastructure

Step 1: Stop the Infrastructure

Refer to Section 3.2.2, "Stopping an Infrastructure" for instructions.

Step 2: Restore the Infrastructure Oracle Home

Note: If your Infrastructure is split and has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes.

Restore the backup (`tar`, `cpio`) of the Infrastructure Oracle home from your complete Oracle Application Server environment backup. Be sure your method of restoring the files preserves the original owner, group, permissions, and timestamps.

Step 3: Restore Infrastructure Configuration Files

> **Note:** If your Infrastructure is split and has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes.

Restore all configuration files from your most recent backup. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

> **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information.

Step 4: Restore and Recover the Metadata Repository

Restore and recover the Metadata Repository from your latest backup. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool.

> **See Also:** Section 12.7, "Best Practices for Restoring and Recovering the Metadata Repository" to determine the best method for restoring and recovering the Metadata Repository

Step 5: Start the Infrastructure

Refer to Section 3.2.1, "Starting an Infrastructure" for instructions.

14.2.2 Restoring an Infrastructure to a New Host

This section describes how to restore an Infrastructure to a host with the same hostname and IP address as the original host. You can use this procedure to:

- Restore an Infrastructure to the same host after the operating system has been reinstalled. The hostname and IP address must remain the same on the host.

- Restore an Infrastructure to a new host that has the same hostname and IP address as the original host.

It contains the following steps:

- Step 1: Prepare the New Host
- Step 2: Restore Oracle System Files
- Step 3: Restore the Infrastructure Oracle Home
- Step 4: Restore Infrastructure Configuration Files
- Step 5: Restore and Recover the Metadata Repository
- Step 6: Start the Infrastructure

Step 1: Prepare the New Host

If you are restoring to a new host, make sure it has an identical system configuration to the original host. Refer to the record you created in Section 13.2.2, "Creating a Record of Your Oracle Application Server Configuration".

1. On the new host, make sure the following is identical to the original host:
   - Hostname
   - Virtual hostname
   - Domain name
   - IP address
   - Hardware platform
   - Operating system release and patch levels
2. Make sure the entry for the new host in `/etc/hosts` is identical to the original `/etc/hosts` file. Make sure the values for IP address, hostname, and aliases are identical and in the same order.
3. Check port usage on the new host. Make sure there aren't any processes using the same ports as the Oracle Application Server installations you are about to restore. If there are, you must reconfigure these processes to use different ports before you begin restoring your Oracle Application Server installations.
4. On the new host, create an operating system user that is identical to the user who installed Oracle Application Server on the original host. The following attributes should be the same:
   - User name

- Numerical userid
- Group name
- Numerical groupid
- Environment profile
- Shell

The user may have the same password or a different password than the original user.

5. Create the Infrastructure Oracle home:
   a. Create an empty Oracle home directory using the same mount point and full path as the original Infrastructure Oracle home. Do not use symbolic links anywhere in the path.
   b. Make sure the directory is on a filesystem with enough space to hold the Infrastructure.
   c. Make sure the directory is owned by the same user and group as on the original host.

Step 2: Restore Oracle System Files

1. Restore the Oracle system files from your complete Oracle Application Server environment backup. For example, on UNIX, these files may be in `/var/opt/oracle` or `/etc`.
2. If the `oraInventory` directory resided in a directory that was separate from the Infrastructure Oracle home, restore it.

Step 3: Restore the Infrastructure Oracle Home

Note: If your Infrastructure is split and has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes.

Restore the backup (`tar`, `cpio`) of the Infrastructure Oracle home from your complete Oracle Application Server environment backup. Be sure your method of restoring the files preserves the original owner, group, permissions, and timestamps.

Step 4: Restore Infrastructure Configuration Files

> **Note:** If your Infrastructure is split and has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes.

Restore all configuration files from your most recent backup. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

> **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information.

Step 5: Restore and Recover the Metadata Repository

Restore and recover the Metadata Repository from your latest complete Oracle Application Server environment backup or online backup, whichever was most recent.

You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool.

> **See Also:** Section 12.7, "Best Practices for Restoring and Recovering the Metadata Repository" to determine the best method for restoring and recovering the Metadata Repository

Step 6: Start the Infrastructure

1. Set file permissions by running the following command as root:

   ```
   ORACLE_HOME/root.sh
   ```

2. Start the Infrastructure.

   Refer to Section 3.2.1, "Starting an Infrastructure" for instructions.

14.2.3 Restoring and Recovering the Metadata Repository

This section describes how to restore and recover the Metadata Repository. You can use this when there has only been corruption to the Metadata Repository, and not to any other files in the Oracle home.

Restore and recover the Metadata Repository from your latest backup using your own procedure or the OracleAS Backup and Recovery Tool.

> **See Also:** Section 12.7, "Best Practices for Restoring and Recovering the Metadata Repository" to determine the best method for restoring and recovering the Metadata Repository

14.2.4 Restoring Infrastructure Configuration Files

This section describes how to restore the configuration files in an Infrastructure Oracle home. You can use this procedure when configuration files have been lost or corrupted.

It contains the following steps:

- Step 1: Stop the Infrastructure
- Step 2: Restore Infrastructure Configuration Files
- Step 3: Apply Recent Administrative Changes
- Step 4: Start the Infrastructure

Step 1: Stop the Infrastructure

Refer to Section 3.2.2, "Stopping an Infrastructure" for instructions.

Step 2: Restore Infrastructure Configuration Files

> **Note:** If your Infrastructure is split and has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes.

Restore all configuration files from your most recent backup. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

> **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information.

Step 3: Apply Recent Administrative Changes

If you made any administrative changes since the last time you did an online backup, reapply them now.

> **See Also:** Appendix G, "Examples of Administrative Changes" to learn more about administrative changes

Step 4: Start the Infrastructure

Refer to Section 3.2.1, "Starting an Infrastructure" for instructions.

14.2.5 Restoring a Middle-tier Installation to the Same Host

This section describes how to restore a middle-tier installation to the same host. You can use this procedure when you have lost some or all of your Oracle binaries.

It contains the following steps:

- Step 1: Stop the Middle-tier Instance
- Step 2: Restore the Middle-tier Oracle Home
- Step 3: Restore Middle-tier Configuration Files
- Step 4: Start the Middle-tier Instance

Step 1: Stop the Middle-tier Instance

Refer to Section 3.2.4, "Stopping a Middle-Tier Instance" for instructions.

If the middle-tier instance uses a DCM repository (file-based or database), make sure the DCM repository is up.

Step 2: Restore the Middle-tier Oracle Home

Restore the backup (`tar`, `cpio`) of the middle-tier Oracle home from your complete Oracle Application Server environment backup. Be sure your method of restoring the files preserves the original owner, group, permissions, and timestamps.

Step 3: Restore Middle-tier Configuration Files

Restore all configuration files from your most recent backup. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

See Also: Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information.

Step 4: Start the Middle-tier Instance

Refer to Section 3.2.3, "Starting a Middle-Tier Instance" for instructions.

14.2.6 Restoring a Middle-tier Installation to a New Host

This section describes how to restore and recover a middle-tier installation to a new host. You can use this procedure to

- Restore a middle-tier installation to the same host after the operating system has been reinstalled
- Restore a middle-tier installation to a new host. The new host may have the same hostname and IP address as the original host, or a different hostname, IP address, or both.

It contains the following steps:

- Step 1: Prepare the New Host
- Step 2: Restore Oracle System Files
- Step 3: Restore the Middle-tier Oracle Home
- Step 4: Restore Middle-tier Configuration Files
- Step 5: Restore the DCM File-based Repository (If Required)
- Step 6: Set the New Hostname and IP Address (If Required)
- Step 7: Start the Middle-tier Instance

Step 1: Prepare the New Host

If you are restoring to a new host, make sure it has an identical system configuration to the original host. Refer to the record you created in Section 13.2.2, "Creating a Record of Your Oracle Application Server Configuration".

1. On the new host, make sure the following is identical to the original host:
   - Hardware platform
   - Operating system release and patch levels

   The new host may have the same or different hostname and IP address.

2. Make sure the entry for the new host in `/etc/hosts` lists the IP address, hostname, and aliases in the same order as the original `/etc/hosts` file.
3. Check port usage on the new host. Make sure there aren't any processes using the same ports as the Oracle Application Server installations you are about to restore. If there are, you must reconfigure these processes to use different ports before you begin restoring your Oracle Application Server installations.
4. On the new host, create an operating system user that is identical to the user who installed Oracle Application Server on the original host. The following attributes should be the same:
   - User name
   - Numerical userid
   - Group name
   - Numerical groupid
   - Environment profile
   - Shell

   The user may have the same password or a different password than the original user.
5. Create the middle-tier Oracle home:
   a. Create an empty Oracle home directory using the same mount point and full path as the original middle-tier Oracle home. Do not use symbolic links anywhere in the path.
   b. Make sure the directory is on a filesystem with enough space to hold the middle-tier installation.
   c. Make sure the directory is owned by the same user and group as on the original host.

Step 2: Restore Oracle System Files

1. Restore the Oracle system files from your complete Oracle Application Server environment backup. For example, on UNIX, these files may be in `/var/opt/oracle` or `/etc`.
2. If the `oraInventory` directory resided in a directory that was separate from the middle-tier Oracle home, restore it.

Step 3: Restore the Middle-tier Oracle Home

Restore the backup (`tar`, `cpio`) of the middle-tier Oracle home from your complete Oracle Application Server environment backup. Be sure your method of restoring the files preserves the original owner, group, permissions, and timestamps.

Step 4: Restore Middle-tier Configuration Files

Restore all configuration files from your most recent backup. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

> **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information.

Step 5: Restore the DCM File-based Repository (If Required)

This step is required only if all of the following conditions are true:

- You are using a DCM file-based repository
- You are restoring to a new host
- You are restoring the instance that contains the DCM file-based repository (the repository host instance)

Since the DCM file-based repository on the original host was lost, you must restore (import) the DCM file-based repository to the new host as follows:

1. Stop the DCM daemon on all other instances in the farm by running the following command in the Oracle home of each instance:

   ```
   ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=dcm-daemon
   ```

2. Restore (import) the DCM file-based repository to the new host:

   ```
   ORACLE_HOME/dcm/bin/dcmctl importRepository -file file_name
   ```

   Where *file_name* is the repository backup you made during your most recent backup.

3. Start the DCM daemon on all other instances in the farm by running the following command in the Oracle home of each instance (do not start DCM in the instance you are currently restoring):

   ```
   ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=dcm-daemon
   ```

When you run the `importRepository` command, the middle-tier instance you are currently restoring on the new host becomes the repository host instance. If you intend to continue to use the original host, you must notify the original host that it is no longer the repository host instance. To do this, run the following command in the middle-tier instance on the original host:

```
ORACLE_HOME/dcm/bin/dcmctl repositoryRelocated
```

> **See Also:** *Oracle Application Server 10g High Availability Guide* for instructions on importing a DCM file-based repository

Step 6: Set the New Hostname and IP Address (If Required)

1. Set file permissions by running the following command as root:

   ```
   ORACLE_HOME/root.sh
   ```

2. If the new host has a different hostname or IP address as the original host, follow the procedure in Section 9.3, "Changing the Hostname and IP Address (Middle Tier)" to change the hostname, IP address, or both, as required.

Step 7: Start the Middle-tier Instance

Start OPMN and OPMN-managed processes:

```
ORACLE_HOME/opmn/bin/opmnctl startall
```

Start Application Server Control:

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

14.2.7 Restoring Middle-tier Configuration Files

This section describes how to restore the configuration files in a middle-tier Oracle home. Use this procedure when configuration files have been lost or corrupted.

It contains the following steps:

- Step 1: Stop the Middle-tier Instance
- Step 2: Restore Middle-tier Configuration Files
- Step 3: Apply Recent Administrative Changes
- Step 4: Start the Middle-tier Instance

Step 1: Stop the Middle-tier Instance

Refer to Section 3.2.4, "Stopping a Middle-Tier Instance" for instructions.

If the middle-tier instance uses a DCM repository (file-based or database), make sure the DCM repository is up.

Step 2: Restore Middle-tier Configuration Files

Restore all configuration files from your most recent backup. You can perform this step using your own procedure or the OracleAS Backup and Recovery Tool. For example, to do this using the tool:

```
cd BACKUP_TOOL_DIRECTORY
./bkp_restore.pl -m restore_config -t config_bkp_timestamp
```

> **See Also:** Chapter 12, "Oracle Application Server Backup and Recovery Tool" for more information

Step 3: Apply Recent Administrative Changes

If you made any administrative changes since the last time you did an online backup, reapply them now.

> **See Also:** Appendix G, "Examples of Administrative Changes" to learn more about administrative changes

Step 4: Start the Middle-tier Instance

Refer to Section 3.2.3, "Starting a Middle-Tier Instance" for instructions.

Part V

Appendixes

This part contains the following appendixes:

- Managing and Configuring Application Server Control
- Oracle Application Server Command-Line Tools
- Oracle Application Server Port Numbers
- Metadata Repository Schemas
- printlogs Tool Syntax and Usage
- Auxiliary Procedures for Changing Infrastructure Services
- Examples of Administrative Changes
- Viewing Oracle Application Server Release Numbers

A

Managing and Configuring Application Server Control

When you install Oracle Application Server, the installation procedure automatically starts Application Server Control and its related processes. You can then immediately start using Application Server Control to manage the application server components.

You can also control and configure Application Server Control. For example, you can start and stop Application Server Control, change the Application Server Control password, and configure security for Application Server Control.

This appendix covers how to manage and configure Application Server Control. It contains the following topics:

A.1 Starting and Stopping Application Server Control

To use the Oracle Enterprise Manager home pages, you must start Application Server Control. Application Server Control is automatically started after you install the application server. You must start it manually after each system reboot, or create a script to automatically start it during system boot.

If you need to start or stop Application Server Control on a UNIX system, use the `emctl` command shown in Table A–1.

The `emctl` command is available in the *`ORACLE_HOME`*`/bin` directory after you install Oracle Application Server.

Table A–1 Starting and Stopping Application Server Control

If you want to...	Enter the command...
Start Application Server Control	`emctl start iasconsole`
Stop Application Server Control	`emctl stop iasconsole`
Verify the status of Application Server Control	`emctl status iasconsole`

You can verify Application Server Control is started by pointing your browser to the Application Server Control URL:

`http://`*`hostname.domain`*`:`*`port`*

You can locate the Application Server Control port number in *`ORACLE_HOME`*`/install/portlist.ini`. For example:

`http://`*`hostname.domain`*`:1810`

See Also: Section 2.3.1, "Displaying Oracle Enterprise Manager Application Server Control"

A.2 Understanding Application Server Control Processes

When you start Application Server Control, Enterprise Manager starts up three distinct processes on your UNIX system. To identify these processes, you can do the following:

1. Locate the and view the contents of the following file in the application server home directory:

ORACLE_HOME/bin/emctl.pid

This file contains the process ID for Application Server Control. For example:

```
$PROMPT> cat emctl.pid
5874
```

2. Use the following operating system command to list information about the process, including the parent process ID:

```
$PROMPT> ps -ef | grep process_id_from_the_emctl.pid_file
```

For example:

```
$PROMPT> ps -ef | grep 5874
pjones 5874 7983 0 14:40:44 pts/13 1:08 /disk03/oracle/app1/jdk/bin/java
-Xmx256m -DORACLE_HOME=/disk03/oracle/appserver
```

3. Note the number that appears immediately after the process ID; this is the process ID for the Application Server Control parent process.

4. Use the following operating system command to list all the processes associated with Application Server Control:

```
$PROMPT> ps -ef | grep parent_process_id
```

Sample output from this command is shown in Example A–1. Descriptions of each process shown in the example are provided in Table A–2.

Example A–1 Viewing Application Server Control Processes

```
$PROMPT> ps -ef | grep 7983
pjones  5873  7983 0 14:40:44 pts/10 14:42 /disk03/oracle/app1/bin/emagent
pjones  7983    1  0 14:40:41 pts/10  0:27 /disk03/oracle/app1/perl/bin/perl
pjones  5874  7983 0 14:40:44 pts/10  2:05 /disk03/oracle/app1/jdk/bin/java
-Xmx256m -DORACLE_HOME=/private/90
```

Table A–2 Summary of Application Server Control Processes

Process	Description
emagent	This is the first process shown in Example A–1. This process is for the Oracle Management Agent, which is a local version of the Management Agent designed specifically for monitoring and administerting Oracle Application Server components.

Table A–2 (Cont.) Summary of Application Server Control Processes

Process	Description
perl	This is the second process shown in Example A–1. This process is for the Management Watchdog Process, which monitors the Management Agent and Application Server Control to make sure both processes are running and available at all times.
java	This is the third process shown in Example A–1. This process is for Application Server Control itself

A.3 Changing the ias_admin Password

The `ias_admin` password is required to use Application Server Control. The following sections describe how you can change the `ias_admin` user password:

- Changing the Password Using Application Server Control
- Changing the Password Using the emctl Command-Line Tool

Caution: If you use Infrastructure Services, you must adhere to the Oracle Internet Directory password policy when setting the `ias_admin` password. This is because, even though the `ias_admin` password is not stored in Oracle Internet Directory, it may be used to set component passwords within Oracle Internet Directory. The default password policy is a minimum of five characters, with at least one numeric character.

For more information, see the *Oracle Internet Directory Administrator's Guide*.

A.3.1 Changing the Password Using Application Server Control

To change the `ias_admin` user password using Oracle Enterprise Manager Application Server Control:

1. Navigate to the Application Server home page and select **Preferences** in the top right corner of the page.

   Enterprise Manager displays the Change Password page.

2. Enter the current `ias_admin` password, the new password, the new password again for confirmation.

The new password must be between 5 and 30 characters, it must begin with an alphabetic character, and it must contain at least one number.

3. Click **OK** to reset the `ias_admin` password for the current application server instance.

   The next time you log in, you must use the new password.

A.3.2 Changing the Password Using the emctl Command-Line Tool

To change the `ias_admin` user password using a command-line tool:

1. Enter the following command in the Oracle home of your Oracle Application Server installation:

   ```
   ORACLE_HOME/bin/emctl set password old_password new_password
   ```

   For example:

   ```
   ORACLE_HOME/bin/emctl set password m5b8r5 b8s0d9
   ```

2. Restart Application Server Control.

   See Also: "Starting and Stopping Application Server Control" on page A-2

A.4 Configuring Security for Enterprise Manager Application Server Control

Application Server Control relies on several underlying technologies, including a version of the Management Agent that is designed to provide monitoring data to Application Server Control.

By default, you access Application Server Control through your Web browser using the non-secure, HTTP protocol. In addition, communications between the local Management Agent and Application Server Control are transferred over insecure connections.

To secure the communications between the Management Agent and Application Server Control, and to provide HTTPS browser access to Application Server Control, Enterprise Manager provides the `emctl secure em` command-line utility.

The `emctl secure em` utility enables HTTPS and Public Key Infrastructure (PKI) components, including signed digital certificates, for communications between Application Server Control and the local Management Agent.

See Also: *Oracle Application Server 10g Security Guide*

To configure security for Application Server Control:

1. Stop Application Server Control by entering the following command:

   ORACLE_HOME`/bin/emctl stop iasconsole`

2. Enter the following command:

   ORACLE_HOME`/bin/emctl secure em`

   Enterprise Manager secures Application Server Control. Sample output of the `emctl secure em` command is shown in Example A–2.

3. Start Application Server Control by entering the following command:

   ORACLE_HOME`/bin/emctl start iasconsole`

4. Test the security of Application Server Control by entering the following URL in your Web browser:

   `https://`*hostname.domain*`:`*port*`/`

   For example:

   `https://mgmthost1.myco:1810/`

Example A–2 Sample Output from the emctl secure em Command

```
$PROMPT> ./emctl secure em
Enterprise Manager 9.0.4.0.0
Copyright (c) 2002, 2003 Oracle Corporation.  All rights reserved.
Generating Standalone Console Root Key (this takes a minute)...   Done.
Fetching Standalone Console Root Certificate...   Done.
Generating Standalone Console Agent Key...   Done.
Generating Oracle Wallet for the Standalone Console Agent...   Done.
Configuring Agent for HTTPS...   Done.
EMD_URL set in /dsk02/oracle/appserv1/sysman/config/emd.properties
Generating Standalone Console Java Keystore...   Done.
```

A.5 Enabling ODL for the Application Server Control Log File

By default, the log file generated for Application Server Control is saved in text format. However, you can configure Application Server Control so its log file will be saved using the Oracle Diagnostic Logging (ODL) format.

When you enable ODL for the Application Server Control log files, the logging and diagnostic information is saved in XML format and the contents of the log files are loaded automatically into the Log Repository. You can then use the Log Repository to search for diagnostic information generated by Application Server Control.

See Also: Chapter 4, "Managing Log Files"

By default, Application Server Control logs information and errors to the following log file in the application server home directory:

ORACLE_HOME/sysman/config/log/emias.log

After you perform the following procedure, Application Server Control will instead log information and error messages to the following file, which formats the data according to the ODL standard:

ORACLE_HOME/sysman/config/log/log.xml

As soon as Application Server Control creates the `log.xml` file, the Log Loader begins loading the logging data into the Oracle Application Server Log Repository on the Log Loader's next run.

Refer to the following sections for more information:

- Modifying Application Server Control Logging Properties
- More About Application Server Control Log File Properties

A.5.1 Modifying Application Server Control Logging Properties

To configure Application Server Control to support ODL:

1. Use a text editor to edit the following file in the Oracle Application Server home directory:

   ORACLE_HOME/sysman/config/emiasconsolelogging.properties

2. Follow the instructions in the file to replace the default properties with those that are commented by default.

Example A–3 shows the properties in the `emiasconsolelogging.properties` file that enable ODL for the Application Server Control log file.

Table A–3 describes the logging properties available in the `emiasconsolelogging.properties` file.

3. Save and close the `emiasconsolelogging.properties` file.
4. Restart Application Server Control.

Example A–3 ODL Logging Properties for Application Server Control

```
# To support the ODL log appender, replace the lines above
# with the following and restart EM.  The resulting ODL log files
#  will be read by the Log Loader and written to the Log Repository.
#
# log4j.appender.emiaslogAppender=oracle.core.ojdl.log4j.OracleAppender
# log4j.appender.emiaslogAppender.ComponentId=EM
#
log4j.appender.emiaslogAppender.LogDirectory=/private/904_shiphomes/m21_infra/sy
sman/log
# log4j.appender.emiaslogAppender.MaxSize=20000000
# log4j.appender.emiaslogAppender.MaxSegmentSize=5000000
```

Table A–3 ODL Properties in Application Server Control Logging Properties

Property	Description
`log4j.appender.emiaslogAppender .LogDirectory`	Determines the directory where the log.xml file will be saved.
`log4j.appender.emiaslogAppender .MaxSize`	Determines the maximum amount of disk space to be used by the log.xml file and the logging rollover files. For more information, see "" on page A-8.
`log4j.appender.emiaslogAppender .MaxSegmentSize`	Determines the maximum size of the log.xml file. When the log.xml file reaches this size, a rollover file is created. For more information, see "" on page A-8.

A.5.2 More About Application Server Control Log File Properties

When you enable ODL, the resulting `log.xml` file increases in size over time as information is written to the file. The file is designed to reach a maximum size, determined by the `MaxSegmentSize` property shown in Example A–3. When the file reaches the predefined maximum size, Application Server Control renames (or

rolls) the logging or trace information to a new file name and starts a new log or trace file. This process keeps the log file from growing too large.

To be sure you have access to important log information, Application Server Control will rollover the `log.xml` file until the log file and its rollover files consume a predefined, maximum amount of disk space, determined by the MaxSize property shown in Example A–3. When the log file and its rollover files reach this predefined target, Application Server Control deletes the oldest rollover file.

As a result, you will often see multiple log files in the log directory. The following example shows three Application Server Control rollover files and the current log file in the log directory:

```
log.xml
log1.xml
log2.xml
log3.xml
```

A.6 Enabling Enterprise Manager Accessibility Mode

The following sections provide information on the benefits of running Enterprise Manager in accessibility mode, as well as instructions for enabling accessibility mode:

- Making HTML Pages More Accessible
- Providing Textual Descriptions of Enterprise Manager Charts
- Modifying the uix-config.xml File to Enable Accessibility Mode

A.6.1 Making HTML Pages More Accessible

Enterprise Manager takes advantage of user interface development technologies that improve the responsiveness some user operations. For example, when you navigate to a new record set in a table, Enterprise Manager does not redisplay the entire HTML page.

However, this performance-improving technology is generally not supported by screen readers. When you enable accessibility mode, you disable this feature, and as a result, make the Enterprise Manager HTML pages more accessible for disabled users.

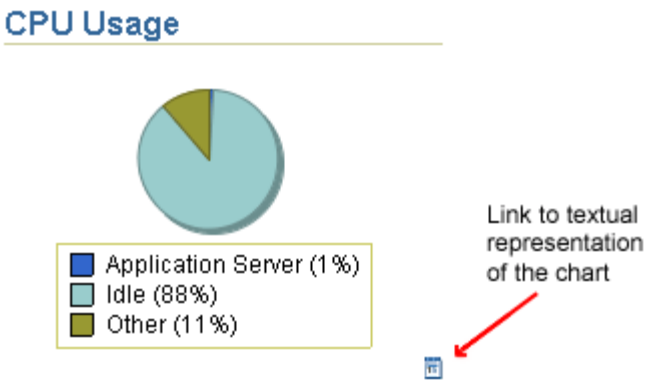
A.6.2 Providing Textual Descriptions of Enterprise Manager Charts

Throughout Enterprise Manager, charts are used to display performance data. For most users, these charts provide a valuable graphical view of the data that can reveal trends and help identify minimum and maximum values for performance metrics.

However, charts do not convey information in a manner that can be read by a screen reader. To remedy this problem, you can configure Enterprise Manager to provide a complete textual representation of each performance chart. When you enable accessibility mode, Enterprise Manager displays a small icon for each chart that can be used as a drill-down link to the textual representation.

Figure A–1 shows an example of the icon that appears below each chart after you enable accessibility mode.

Figure A–1 Icon Representing the Textual Representation of a Chart



A.6.3 Modifying the uix-config.xml File to Enable Accessibility Mode

1. Locate the `uix-config.xml` configuration file in the Oracle Application Server home directory:

   ORACLE_HOME`/sysman/webapps/emd/WEB-INF`

2. Open the `uix-config.xml` file using your favorite text editor and locate the following entry:

   ```
   <!-- An alternate configuration that disables accessibility features  -->
   <default-configuration>
   ```

```
  <accessibility-mode>inaccessible</accessibility-mode>
</default-configuration>
```

3. Change the value of the `accessibility-mode` property from `inaccessible` to `accessible`.
4. Save and close the file.
5. Restart Application Server Control.

B

Oracle Application Server Command-Line Tools

This appendix summarizes the command-line tools available in Oracle Application Server, with descriptions and pointers to more information on each tool.

It contains the following topics:

B.1 Oracle Application Server Command-Line Tools (Sorted by Command)

Table B–1 lists the Oracle Application Server command-line tools, sorted by command. You can find descriptions of each command and pointers to more information in Section B.3, "Oracle Application Server Command-Line Tool Descriptions".

Table B–1 Oracle Application Server Command-Line Tools (Sorted by Command)

Command	Path from Oracle Home	Component
bulkdelete.sh	`ldap/bin/bulkdelete.sh`	Oracle Internet Directory
bulkload.sh	`ldap/bin/bulkload.sh`	Oracle Internet Directory
bulkmodify	`bin/bulkmodify`	Oracle Internet Directory
catalog.sh	`ldap/bin/catalog.sh`	Oracle Internet Directory
dcmctl	`dcm/bin/dcmctl`	Distributed Configuration Management (DCM)
dipassistant	`bin/dipassistant`	Oracle Internet Directory
dmstool	`bin/dmstool`	Dynamic Monitoring Service (DMS)
emctl	`bin/emctl`	Oracle Enterprise Manager
eulbuilder.jar	`bin/eulbuilder.jar`	OracleAS Discoverer
fplsqlconv90	`bin/fplsqlconv90`	OracleAS Forms Services
hiqpurge.sh	`ldap/bin/hiqpurge.sh`	Oracle Internet Directory
hiqretry.sh	`ldap/bin/hiqretry.sh`	Oracle Internet Directory
iasua.sh	`upgrade/iasua.sh`	OracleAS Upgrade Assistant
ifbld90	`bin/ifbld90`	OracleAS Forms Services
ifcmp90	`bin/ifcmp90`	OracleAS Forms Services
iff2xml90	`bin/iff2xml90`	OracleAS Forms Services
ifweb90	`bin/ifweb90`	OracleAS Forms Services
ifxml2f90	`bin/ifxml2f90`	OracleAS Forms Services
ifxmlv90	`bin/ifxmlv90`	OracleAS Forms Services
jazn.jar	`j2ee/home/jazn.jar`	OracleAS JAAS Provider

Table B–1 (Cont.) Oracle Application Server Command-Line Tools (Sorted by Command)

Command	Path from Oracle Home	Component
ldapadd	bin/ldapadd	Oracle Internet Directory
ldapaddmt	bin/ldapaddmt	Oracle Internet Directory
ldapbind	bin/ldapbind	Oracle Internet Directory
ldapcompare	bin/ldapcompare	Oracle Internet Directory
ldapdelete	bin/ldapdelete	Oracle Internet Directory
ldapmoddn	bin/ldapmoddn	Oracle Internet Directory
ldapmodify	bin/ldapmodify	Oracle Internet Directory
ldapmodifymt	bin/ldapmodifymt	Oracle Internet Directory
ldapsearch	bin/ldapsearch	Oracle Internet Directory
ldifmigrator	bin/ldifmigrator	Oracle Internet Directory
ldifwrite	bin/ldifwrite	Oracle Internet Directory
ocactl	oca/bin/ocactl	OracleAS Certificate Authority
oidctl	bin/oidctl	Oracle Internet Directory
oidmon	bin/oidmon	Oracle Internet Directory
oidpasswd	bin/oidpasswd	Oracle Internet Directory
oidprovtool	bin/oidprovtool	Oracle Internet Directory
oidreconcile	bin/oidreconcile	Oracle Internet Directory
oidstats.sh	ldap/bin/oidstats.sh	Oracle Internet Directory
ojspc	bin/ojspc	Oracle Application Server Containers for J2EE (OC4J)
opmnctl	opmn/bin/opmnctl	Oracle Process Manager and Notification Server (OPMN)
ossoca.jar	portal/admin/plsql/sso/ossoca.jar	OracleAS Single Sign-On
ossoreg.jar	sso/lib/ossoreg.jar	OracleAS Single Sign-On
portalRegistrar.sh	wireless/bin/portalRegistrar.sh	OracleAS Portal and OracleAS Wireless
printlogs	diagnostics/bin/printlogs	Oracle Application Server
remtool	ldap/bin/remtool	Oracle Internet Directory

Table B–1 (Cont.) Oracle Application Server Command-Line Tools (Sorted by Command)

Command	Path from Oracle Home	Component
reRegisterSSO.sh	`wireless/bin/reRegisterSSO.sh`	OracleAS Wireless
resetiASpasswd.sh	`bin/resetiASpasswd.sh`	Oracle Internet Directory
rwbuilder	`bin/rwbuilder`	OracleAS Reports Services
rwcgi	`bin/rwcgi`	OracleAS Reports Services
rwclient	`bin/rwclient`	OracleAS Reports Services
rwconverter	`bin/rwconverter`	OracleAS Reports Services
rwrun	`bin/rwrun`	OracleAS Reports Services
rwserver	`bin/rwserver`	OracleAS Reports Services
schemasync	`bin/schemasync`	Oracle Internet Directory
ssocfg.sh	`portal/admin/plsql/sso/ssoocfg.sh`	OracleAS Single Sign-On
ssooconf.sql	`portal/admin/plsql/sso/ssooconf.sql`	OracleAS Single Sign-On
stopodis.sh	`ldap/odi/admin/stopodis.sh`	Oracle Internet Directory
uddiadmin.jar	`uddi/lib/uddiadmin.jar`	OracleAS Web Services
webcachectl	`bin/webcachectl`	OracleAS Web Cache

B.2 Oracle Application Server Command-Line Tools (Sorted by Component)

Table B–2 lists the Oracle Application Server command-line tools, sorted by component. You can find descriptions of each command and pointers to more information in Section B.3, "Oracle Application Server Command-Line Tool Descriptions".

Table B–2 Oracle Application Server Command-Line Tools (Sorted by Component)

Component	Command	Path from Oracle Home
Distributed Configuration Management (DCM)	dcmctl	`dcm/bin/dcmctl`
Dynamic Monitoring Service (DMS)	dmstool	`bin/dmstool`
Oracle Application Server	printlogs	`diagnostics/bin/printlogs`
Oracle Application Server Containers for J2EE (OC4J)	ojspc	`bin/ojspc`
Oracle Enterprise Manager	emctl	`bin/emctl`
Oracle Internet Directory	bulkdelete.sh	`ldap/bin/bulkdelete.sh`
Oracle Internet Directory	bulkload.sh	`ldap/bin/bulkload.sh`
Oracle Internet Directory	bulkmodify	`bin/bulkmodify`
Oracle Internet Directory	catalog.sh	`ldap/bin/catalog.sh`
Oracle Internet Directory	dipassistant	`bin/dipassistant`
Oracle Internet Directory	hiqpurge.sh	`ldap/bin/hiqpurge.sh`
Oracle Internet Directory	hiqretry.sh	`ldap/bin/hiqretry.sh`
Oracle Internet Directory	ldapadd	`bin/ldapadd`
Oracle Internet Directory	ldapaddmt	`bin/ldapaddmt`
Oracle Internet Directory	ldapbind	`bin/ldapbind`
Oracle Internet Directory	ldapcompare	`bin/ldapcompare`
Oracle Internet Directory	ldapdelete	`bin/ldapdelete`
Oracle Internet Directory	ldapmoddn	`bin/ldapmoddn`
Oracle Internet Directory	ldapmodify	`bin/ldapmodify`

Table B–2 (Cont.) Oracle Application Server Command-Line Tools (Sorted by Component)

Component	Command	Path from Oracle Home
Oracle Internet Directory	ldapmodifymt	bin/ldapmodifymt
Oracle Internet Directory	ldapsearch	bin/ldapsearch
Oracle Internet Directory	ldifmigrator	bin/ldifmigrator
Oracle Internet Directory	ldifwrite	bin/ldifwrite
Oracle Internet Directory	oidctl	bin/oidctl
Oracle Internet Directory	oidmon	bin/oidmon
Oracle Internet Directory	oidpasswd	bin/oidpasswd
Oracle Internet Directory	oidprovtool	bin/oidprovtool
Oracle Internet Directory	oidreconcile	bin/oidreconcile
Oracle Internet Directory	oidstats.sh	ldap/bin/oidstats.sh
Oracle Internet Directory	remtool	ldap/bin/remtool
Oracle Internet Directory	resetiASpasswd.sh	bin/resetiASpasswd.sh
Oracle Internet Directory	schemasync	bin/schemasync
Oracle Internet Directory	stopodis.sh	ldap/odi/admin/stopodis.sh
Oracle Process Manager and Notification Server (OPMN)	opmnctl	opmn/bin/opmnctl
OracleAS Certificate Authority	ocactl	oca/bin/ocactl
OracleAS Discoverer	eulbuilder.jar	bin/eulbuilder.jar
OracleAS Forms Services	fplsqlconv90	bin/fplsqlconv90
OracleAS Forms Services	ifbld90	bin/ifbld90
OracleAS Forms Services	ifcmp90	bin/ifcmp90
OracleAS Forms Services	iff2xml90	bin/iff2xml90
OracleAS Forms Services	ifweb90	bin/ifweb90
OracleAS Forms Services	ifxml2f90	bin/ifxml2f90
OracleAS Forms Services	ifxmlv90	bin/ifxmlv90
OracleAS JAAS Provider	jazn.jar	j2ee/home/jazn.jar
OracleAS Portal	portalRegistrar.sh	wireless/bin/portalRegistrar.sh
OracleAS Reports Services	rwbuilder	bin/rwbuilder

Table B–2 (Cont.) Oracle Application Server Command-Line Tools (Sorted by Component)

Component	Command	Path from Oracle Home
OracleAS Reports Services	rwcgi	bin/rwcgi
OracleAS Reports Services	rwclient	bin/rwclient
OracleAS Reports Services	rwconverter	bin/rwconverter
OracleAS Reports Services	rwrun	bin/rwrun
OracleAS Reports Services	rwserver	bin/rwserver
OracleAS Single Sign-On	ossoca.jar	portal/admin/plsql/sso/ossoca.jar
OracleAS Single Sign-On	ossoreg.jar	sso/lib/ossoreg.jar
OracleAS Single Sign-On	ssocfg.sh	portal/admin/plsql/sso/ssoocfg.sh
OracleAS Single Sign-On	ssooconf.sql	portal/admin/plsql/sso/ssooconf.sql
OracleAS Upgrade Assistant	iasua.sh	upgrade/iasua.sh
OracleAS Web Cache	webcachectl	bin/webcachectl
OracleAS Web Services	uddiadmin.jar	uddi/lib/uddiadmin.jar
OracleAS Wireless	portalRegistrar.sh	wireless/bin/portalRegistrar.sh
OracleAS Wireless	reRegisterSSO.sh	wireless/bin/reRegisterSSO.sh

B.3 Oracle Application Server Command-Line Tool Descriptions

This section describes each Oracle Application Server command-line tool and provides pointers to more information.

bulkdelete.sh

Delete a subtree efficiently in Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

bulkload.sh

Create Oracle Internet Directory entries from data residing in or created by other applications.

See Also: *Oracle Internet Directory Administrator's Guide*

bulkmodify

Modify a large number of existing Oracle Internet Directory entries in an efficient way.

See Also: *Oracle Internet Directory Administrator's Guide*

catalog.sh

Add and delete catalog entries in Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

dcmctl

Manage application server instances and clusters, deploy applications, manage the DCM repository.

See Also: *Distributed Configuration Management Reference Guide*

dipassistant

Directory Integration and Provisioning Assistant—assists in performing all operations in the Oracle Directory Integration and Provisioning platform.

See Also: *Oracle Internet Directory Administrator's Guide*

dmstool

View performance metrics and set reporting intervals.

See Also: *Oracle Application Server 10g Performance Guide*

emctl

Start, stop, and manage security for Oracle Enterprise Manager.

See Also: Chapter 2, "Introduction to Administration Tools"

eulbuilder.jar

Discoverer EUL Java command-line interface. A set of text-based commands that enable you to create and manipulate Discoverer EULs without installing Oracle9*i* Discoverer Administrator.

See Also: *Oracle Discoverer EUL Java Command Line User's Guide*

fplsqlconv90

Update obsolete usage in your PL/SQL code in order to migrate your Forms6*i* applications to Oracle Application Server Forms Services.

See Also: Oracle Application Server Forms Services Online Help

hiqpurge.sh

Move the changes from the human intervention queue to the purge queue.

See Also: *Oracle Internet Directory Administrator's Guide*

hiqretry.sh

Move the changes from the human intervention queue to the retry queue.

See Also: *Oracle Internet Directory Administrator's Guide*

iasua.sh

Oracle Application Server Upgrade Assistant.

See Also: *Oracle Application Server 10g Upgrading to 10g (9.0.4)*

ifbld90

Start Forms Developer with specific options for a Forms session.

See Also: Oracle Application Server Forms Services Online Help

ifcmp90

Start Form Compiler to generate a form.

See Also: Oracle Application Server Forms Services Online Help

iff2xml90

Traverse a module object hierarchy and produce an XML representation of it.

See Also: Oracle Application Server Forms Services Online Help

ifweb90

Preview a form in a Web browser.

See Also: Oracle Application Server Forms Services Online Help

ifxml2f90

Take well-defined XML format and convert it back into a module.

See Also: Oracle Application Server Forms Services Online Help

ifxmlv90

XML Validator that can be used on the command line or called from Java to validate .xml files or XMLDocument Java objects respectively against the Forms XML Schema.

See Also: Oracle Application Server Forms Services Online Help

jazn.jar

Manage both XML-based and LDAP-based JAAS data.

See Also: *Oracle Application Server Containers for J2EE Security Guide*

ldapadd

Add entries, their object classes, attributes, and values to Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapaddmt

Add entries, their object classes, attributes, and values to Oracle Internet Directory. Like `ldapadd`, except supports multiple threads for adding entries concurrently.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapbind

Determine if you can authenticate a client to a server.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapcompare

Match attribute values you specify in the command-line with the attribute values in the Oracle Internet Directory entry.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapdelete

Remove entire entries from Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapmoddn

Modify the DN or RDN of an Oracle Internet Directory entry.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapmodify

Perform actions on attributes in Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapmodifymt

Modify several Oracle Internet Directory entries concurrently.

See Also: *Oracle Internet Directory Administrator's Guide*

ldapsearch

Search and retrieve specific entries in Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

ldifmigrator

Migrate data from application-specific repositories into Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

ldifwrite

Convert to LDIF all or part of the information residing in an Oracle Internet Directory. This makes that information available for loading into a new node in a replicated directory or into another node for backup storage.

See Also: *Oracle Internet Directory Administrator's Guide*

ocactl

OracleAS Certificate Authority administration tool.

See Also: *Oracle Application Server Certificate Authority Administrator's Guide*

oidctl

Start and stop Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

oidmon

Initiate, monitor, and terminate Oracle Internet Directory processes.

See Also: *Oracle Internet Directory Administrator's Guide*

oidpasswd

Change the Oracle Internet Directory database password.

See Also: *Oracle Internet Directory Administrator's Guide*

oidprovtool

Administer provisioning profile entries in Oracle Internet Directory.

See Also: *Oracle Internet Directory Administrator's Guide*

oidreconcile

Synchronize Oracle Internet Directory entries.

See Also: *Oracle Internet Directory Administrator's Guide*

oidstats.sh

Analyze the various database ods schema objects to estimate statistics.

See Also: *Oracle Internet Directory Administrator's Guide*

ojspc

JSP back precompiler.

See Also: *Oracle Application Server Containers for J2EE Support for JavaServer Pages Developer's Guide*

opmnctl

Start, stop, and get status on OPMN-managed processes.

See Also: *Oracle Process Manager and Notification Server Administrator's Guide*

ossoca.jar

Configure additional languages for OracleAS Single Sign-On.

See Also: *Oracle Application Server 10g Globalization Guide*

ossoreg.jar

`mod_osso` registration tool.

See Also: *Oracle Application Server Single Sign-On Administrator's Guide*

portalRegistrar.sh

Reregister the mobile gateway parameter with OracleAS Portal. Run this tool if one of the mobile gateway URLs have changed since installation.

See Also: *Oracle Application Server Portal Configuration Guide* and *Oracle Application Server Wireless Administrator's Guide*

printlogs

Print the contents of diagnostic log files to standard output.

See Also: Appendix E, "printlogs Tool Syntax and Usage"

remtool

Search for problems and seek to rectify them in the event of an Oracle Internet Directory replication failure.

See Also: *Oracle Internet Directory Administrator's Guide*

reRegisterSSO.sh

Reregister the Wireless Single Sign-On partner application with the Single Sign-On server. Run this tool if the hostname, port, or protocol has changed.

See Also: *Oracle Application Server Wireless Administrator's Guide*

resetiASpasswd.sh

Reset the internal password that instances use to authenticate themselves with Oracle Internet Directory. Resets it to a randomly generated password.

See Also: *Oracle Application Server 10g Security Guide*

rwbuilder

Invoke the Reports Builder.

See Also: *Oracle Application Server Reports Services Publishing Reports to the Web*

rwcgi

Like `rwservlet`, translate and deliver information between HTTP and the Reports Server. The `rwservlet` command is the recommended choice; `rwcgi` is maintained only for backward compatibility.

See Also: *Oracle Application Server Reports Services Publishing Reports to the Web*

rwclient

Parse and transfer a command line to the specified (or default) Reports Server.

See Also: *Oracle Application Server Reports Services Publishing Reports to the Web*

rwconverter

Convert one or more report definitions or PL/SQL libraries from one storage format to another.

See Also: *Oracle Application Server Reports Services Publishing Reports to the Web*

rwrun

Run a report using the Oracle Application Server Reports Services in-process server.

See Also: *Oracle Application Server Reports Services Publishing Reports to the Web*

rwserver

Invoke the Reports Server.

See Also: *Oracle Application Server Reports Services Publishing Reports to the Web*

schemasync

Synchronize schema elements—namely attributes and object classes—between an Oracle directory server and third-party LDAP directories.

See Also: *Oracle Internet Directory Administrator's Guide*

ssocfg.sh

Update host, port, and protocol of OracleAS Single Sign-On URL.

See Also: *Oracle Application Server Single Sign-On Administrator's Guide*

ssooconf.sql

Script to point OracleAS Single Sign-On server to a different Oracle Internet Directory.

See Also: *Oracle Application Server Single Sign-On Administrator's Guide*

stopodis.sh

In a client-only installation where the Oracle Internet Directory Monitor and Oracle Internet Directory Control Utility are not available, you can start the directory integration and provisioning server without the `oidctl` tool. To stop the server, use the `stopodis.sh` tool.

See Also: *Oracle Internet Directory Administrator's Guide*

uddiadmin.jar

Manage the UDDI registry, which is part of OracleAS Web Services.

See Also: *Oracle Application Server Web Services Developer's Guide*

webcachectl

Administer OracleAS Web Cache processes, including the administration server process, cache server process, and auto-restart process.

See Also: *Oracle Application Server Web Cache Administrator's Guide*

C

Oracle Application Server Port Numbers

This appendix provides information about Oracle Application Server port numbers.

It contains the following topics:

- Port Numbers and How They Are Assigned (Sorted by Installation)

  This section provides the following information for each Oracle Application Server service that uses a port:

  - Allotted Port Range
  - Default Port Number
  - When is the port number assigned?
  - Can you override the port number assignment during installation?
- Port Numbers (Sorted by Port Number)

  This section provides a table that lists all allotted port ranges. It is useful for determining if a particular port number is used by Oracle Application Server.
- Guidelines for Changing Port Numbers (Sorted by Installation Type)

  This section provides the following information for changing port numbers after installation:

  - Can you change the port number?
  - Are you required to update other components to register the change?
  - What is the recommended method for changing the port number?

C.1 Port Numbers and How They Are Assigned (Sorted by Installation)

This section provides the following information for each Oracle Application Server service that uses a port:

- **Allotted Port Range**: The set of port numbers Oracle Application Server attempts to use when assigning a port.
- **Default Port Number**: The first port number Oracle Application Server attempts to assign to a service. It is usually the lowest number in the allotted port range.
- **When Assigned?**:
  - **Installation**: Most port numbers are assigned by Oracle Application Server during installation. Oracle Application Server chooses a free port from the allotted port range.
  - **After Installation**: You can optionally configure some services after installation.
- **Override during installation in staticports.ini?**: Indicates whether you can override the default port assignment during installation by specifying a port number in `staticports.ini`. You create a template called `staticports.ini` with the port numbers you would like to use, and launch Oracle Universal Installer with special options.

  See Also: *Oracle Application Server 10g Installation Guide* for information on how to use `staticports.ini`

The ports are sorted by the following installation types:

- J2EE and Web Cache Ports
- Portal and Wireless Ports
- Business Intelligence and Forms Ports
- Infrastructure Ports
- OracleAS ProcessConnect Ports
- Oracle Content Management Software Development Kit Ports
- OracleAS Developer Kits

C.1.1 J2EE and Web Cache Ports

Table C–1 lists the ports in a J2EE and Web Cache installation.

Table C–1 J2EE and Web Cache Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Oracle HTTP Server				
Listen	7777 - 7877	Without Web Cache: 7777 With Web Cache: 7778	Installation	Yes
Port	7777 - 7877	Without Web Cache: 7777 With Web Cache: 7777	Installation	Yes
Listen (SSL)	4443 - 4543	Without Web Cache: 4443 With Web Cache: 4444	Installation This port is not used unless you enable SSL after installation. Refer to *Oracle HTTP Server Administrator's Guide.*	Yes
Port (SSL)	4443 - 4543	Without Web Cache: 4443 With Web Cache: 4443	Installation This port is not used unless you enable SSL after installation. Refer to *Oracle HTTP Server Administrator's Guide.*	Yes
Diagnostic	7200 - 7299	7200	Installation	Yes
OracleAS Web Cache				
HTTP Listen	7777 - 7877	7777	Installation	Yes
HTTP Listen (SSL)	4443 - 4543	4443	Installation This port is not used unless you enable SSL after installation. Refer to *Oracle Application Server Web Cache Administrator's Guide.*	Yes
Administration	4000 - 4030	4000	Installation	Yes
Invalidation	4001 - 4030	4001	Installation	Yes

Table C–1 (Cont.) J2EE and Web Cache Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Statistics	4002 - 4030	4002	Installation	Yes
OC4J				
AJP	3301 - 3400	3301	Installation	No
JMS	3701 - 3800	3701	Installation	No
RMI	3201 - 3300	3201	Installation	No
IIOP	3401 - 3500	3401	After installation, when you configure IIOP. Refer to *Oracle Application Server Containers for J2EE User's Guide*.	No
IIOPS1 (Server only)	3501 - 3600	3501	After installation, when you configured IIOPS1.	No
IIOPS2 (Server and client)	3601 - 3700	3601	After installation, when you configured IIOPS2.	No
OPMN				
ONS Local	6100 - 6199	6100	Installation	Yes
ONS Remote	6200 - 6299	6200	Installation	Yes
ONS Request	6003 - 6099	6003	Installation	Yes
Oracle Enterprise Manager				
Application Server Control	1810 - 1829	1810	Installation	Yes
Application Server Control (SSL)	1810 - 1829	1810	After installation, when you configure Application Server Control for SSL. Refer to Section A.4, "Configuring Security for Enterprise Manager Application Server Control".	No
Application Server Control RMI	1850 - 1869	1850	Installation	Yes
Oracle Management Agent	1830 - 1849	1830	Installation	Yes
Miscellaneous Services				
DCM Java Object Cache	7100 - 7199	7100	Installation	Yes

Table C–1 (Cont.) J2EE and Web Cache Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Java Object Cache	7000 - 7099	7000	Installation	Yes
JServ Servlet Engine	8007 - 8107	8007	Installation The port is not used unless you configure JServ after installation. Refer to Section 7.2.1, "Configuring JServ After Installation".	Yes
Log Loader	44000 - 44099	44000	Installation	Yes
Port Tunneling	7501 - 7599	7501	After installation, when you configure Port Tunneling.	No

C.1.2 Portal and Wireless Ports

A Portal and Wireless installation uses the ports listed in:

- Table C–1, " J2EE and Web Cache Ports"
- Table C–2, " Portal and Wireless Ports".

Table C–2 Portal and Wireless Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Oracle Ultra Search				
RMI Daemon	1098	1098	Installation	No
RMI Registry	1099	1099	Installation	No
OracleAS Portal				
OracleAS Portal[1]	N / A	N / A	N / A	N / A
OracleAS Wireless				
OracleAS Wireless[1]	N / A	N / A	N / A	N / A
Wireless Notification Dispatcher Calendar	9100 - 9199	9100	Installation	No

[1] This service does not have its own port. You can access it through the HTTP listener port.

C.1.3 Business Intelligence and Forms Ports

A Business Intelligence and Forms installation uses the ports listed in:

- Table C–1, " J2EE and Web Cache Ports"
- Table C–2, " Portal and Wireless Ports"
- Table C–3, " Business Intelligence and Forms Ports"

Table C–3 Business Intelligence and Forms Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
OracleAS Discoverer				
OracleAS Discoverer[1]	N / A	N / A	N / A	N / A
OracleAS Discoverer OSAgent	16001 - 16020	16001	Installation	Yes
OracleAS Forms Services				
OracleAS Forms Services[1]	N / A	N / A	N / A	N / A
OracleAS Reports Services				
SQL*Net *For 6i Backward Compatibility Only*	1950 - 1960	1950	Installation	Yes
Visigenics CORBA - Reports 9*i*	14000 - 14010	14000	Installation	No

[1] This service does not have its own port. You can access it through the HTTP listener port.

C.1.4 Infrastructure Ports

An Infrastructure installation uses the ports listed in:

- Table C–1, " J2EE and Web Cache Ports"
- Table C–4, " Infrastructure Ports"

Table C–4 Infrastructure Ports

Component / Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in statisports.ini?
Oracle Internet Directory				
Oracle Internet Directory	389, 3060 - 3129	389[1]	Installation	Yes
Oracle Internet Directory (SSL)	636, 3130 - 3199	636[2]	Installation	Yes
OracleAS Certificate Authority				
Server Authentication Virtual Host (SSL)	4400 - 4419	4400	Installation	Yes
Mutual Authentication Virtual Host (SSL)	4400 - 4419	4401	Installation	Yes
OracleAS Metadata Repository				
Oracle Net Listener	1521	1521	Installation	No
OracleAS Single Sign-On				
OracleAS Single Sign-On[3]	N/A	N/A	N/A	N/A

[1] Some versions of UNIX use port 389 in /etc/services. On these systems, the default Oracle Internet Directory non-SSL port number is 3060.

[2] Some versions of UNIX use port 636 in /etc/services. On these systems, the default Oracle Internet Directory SSL port number is 3130.

[3] This service does not have its own port. You can access it through the HTTP listener port.

C.1.5 OracleAS ProcessConnect Ports

Table C–5 lists the ports used in an OracleAS ProcessConnect installation.

Table C–5 OracleAS ProcessConnect Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Actional Agent	20300 - 20350	20300	Installation	No[1]
Actional Listener	4550 - 4599	4550	Installation	No[1]
Adapter Framework	8777 - 8900	8778	Installation	No[1]
Attunity Adapters (Legacy Adapters)	2550 - 2577	2552	Installation	No[1]
B2B Adapter RMI	1110 - 1120	1110	Installation	No[1]
Integration Manager	8777 - 8900	8777	Installation	No[1]

[1] The feature of overriding port numbers with staticports.ini during installation is not available with the OracleAS ProcessConnect installation.

C.1.6 OracleAS InterConnect Ports

Table C–6 lists the ports used in an OracleAS InterConnect installation.

Table C–6 OracleAS InterConnect Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
OracleAS InterConnect Adapters	Configurable	Configurable	After Installation Refer to *Oracle Application Server InterConnect User's Guide*	No[1]
OracleAS InterConnect Repository	Configurable	Configurable	After Installation Refer to *Oracle Application Server InterConnect User's Guide*	No[1]
RMI port for HTTP	9901	9901	Installation	No[1]

[1] The feature of overriding port numbers with staticports.ini during installation is not available with the OracleAS InterConnect installation.

C.1.7 Oracle Content Management Software Development Kit Ports

Table C–7 lists the ports used in an Oracle Content Management Software Development Kit installation.

Table C–7 Oracle Content Management Software Development Kit Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
AFP *(myhost.mydomain Node)*	548	548	Installation	No[1]
CUP *(myhost.mydomain Node)*	4180	4180	Installation	No[1]
Domain Controller	53140 - 53999	N / A	Installation	No[1]
FTP *(myhost.mydomain Node)*	21	21	Installation	No[1]
IMAP *(myhost.mydomain Node)*	143	143	Installation	No[1]
IMAP (SSL) *(myhost.mydomain Node)*	993	993	Installation	No[1]
NB UDP *(myhost.mydomain Node)*	137	137	Installation	No[1]
NFS *(myhost.mydomain Node)*	2049	2049	Installation	No[1]
NFS Mount Point *(myhost.mydomain Node)*	N / A	N / A	Installation	No[1]
Node Guardian *(myhost.mydomain Node)*	53140 - 53999	N / A	Installation	No[1]
Node Guardian *(myhost.mydomain HTTP Node)*	53140 - 53999	N / A	Installation	No[1]
Node Manager *(myhost.mydomain Node)*	53140 - 53999	N / A	Installation	No[1]

Table C–7 (Cont.) Oracle Content Management Software Development Kit Ports

Service	Allotted Port Range	Default Port Number	When Assigned?	Override during installation in staticports.ini?
Node Manager *(myhost.mydomain HTTP Node)*	53140 - 53999		Installation	No[1]
SMB *(myhost.mydomain Node)*	139	139	Installation	No[1]
SMTP *(myhost.mydomain Node)*	25	25	Installation	No[1]

[1] The feature of overriding port numbers with staticports.ini during installation is not available for Oracle Content Management Software Development Kit.

C.1.8 OracleAS Developer Kits

OracleAS Developer Kits use the same ports as the J2EE and Web Cache installation type.

See Also: Section C.1.1, "J2EE and Web Cache Ports"

C.2 Port Numbers (Sorted by Port Number)

Table C–8 lists Oracle Application Server ports numbers and services, sorted in ascending order by port number.

Table C–8 Port Numbers (Sorted by Port Number)

Port Number	Service
21	Oracle Content Management Software Development Kit FTP
25	Oracle Content Management Software Development Kit SMTP
137	Oracle Content Management Software Development Kit NB UDP
139	Oracle Content Management Software Development Kit SMB
143	Oracle Content Management Software Development Kit IMAP (non-SSL)
389	Oracle Internet Directory (non-SSL)
548	Oracle Content Management Software Development Kit AFP
636	Oracle Internet Directory Server (SSL)
993	Oracle Content Management Software Development Kit IMAP (SSL)
1098	Oracle Ultra Search RMI Daemon
1099	Oracle Ultra Search RMI Registry
1110 - 1120	OracleAS ProcessConnect B2B Adapter RMI
1521	OracleAS Metadata Repository Oracle Net Listener
1810 - 1829	Oracle Enterprise Manager Application Server Control (non-SSL and SSL)
1830 - 1849	Oracle Management Agent
1850 - 1869	Oracle Enterprise Manager Application Server Control RMI
1950 - 1960	OracleAS Reports Services SQL*Net
2049	Oracle Content Management Software Development Kit NFS
2550 - 2577	OracleAS ProcessConnect Attunity Adapters (Legacy Adapters)
3060 - 3129	Oracle Internet Directory (non-SSL)
3130 - 3199	Oracle Internet Directory (SSL)
3201 - 3300	OC4J RMI
3301 - 3400	OC4J AJP
3401 - 3500	OC4J IIOP

Table C–8 (Cont.) Port Numbers (Sorted by Port Number)

Port Number	Service
3501 - 3600	OC4J IIOPS1 (Server only)
3601 - 3700	OC4J IIOPS2 (Server and client)
3701 - 3800	OC4J JMS
4000 - 4030	OracleAS Web Cache Administration OracleAS Web Cache Invalidation OracleAS Web Cache Statistics
4180	Oracle Content Management Software Development Kit CUP
4400 - 4419	OracleAS Certificate Authority Server Authentication Virtual Host (SSL) OracleAS Certificate Authority Mutual Authentication Virtual Host (SSL)
4443 - 4543	Oracle HTTP Server Listen (SSL) and Oracle HTTP Server Port (SSL) OracleAS Web Cache HTTP Listen (SSL)
4550 - 4599	OracleAS ProcessConnect Actional Listener
6003 - 6099	OPMN ONS Request
6100 - 6199	OPMN ONS Local
6200 - 6299	OPMN ONS Remote
7000 - 7099	Java Object Cache
7100 - 7199	DCM Java Object Cache
7200 - 7299	Oracle HTTP Server Diagnostic
7501 - 7599	Port Tunneling
7777 - 7877	Oracle HTTP Server Listen and Oracle HTTP Server Port OracleAS Web Cache HTTP Listen
8007 - 8107	JServ Servlet Engine
8777 - 8900	OracleAS ProcessConnect Integration Manager OracleAS ProcessConnect Adapter Framework
9100 - 9199	Wireless Notification Dispatcher Calendar
9901	OracleAS InterConnect RMI port for HTTP
14000 - 14010	OracleAS Reports Services Visigenics CORBA - Reports 9*i*
16001 - 16020	OracleAS Discoverer OSAgent

Table C–8 (Cont.) Port Numbers (Sorted by Port Number)

Port Number	Service
20300 - 20350	OracleAS ProcessConnect Actional Agent
44000 - 44099	Log Loader
53140 - 53999	Oracle Content Management Software Development Kit Domain Controller
	Oracle Content Management Software Development Kit Node Guardian
	Oracle Content Management Software Development Kit Node Manager

C.3 Guidelines for Changing Port Numbers (Sorted by Installation Type)

This section provides the following information about changing Oracle Application Server port numbers:

- **Can be changed?**: Indicates if the port number can be changed after its initial assignment during installation. If the answer to this is No, then Oracle does not support changing the port number.
- **Dependencies?**: Indicates if, after changing the port number, you must perform additional steps to register the change with other components.
- **Procedure**: The recommended procedure for changing the port number. The procedure includes the steps for changing the port number, plus the additional steps required to register the change with other components, if any.

The ports are sorted by the following installation types:

- J2EE and Web Cache Ports
- Portal and Wireless Ports
- Business Intelligence and Forms Ports
- Infrastructure Ports
- OracleAS ProcessConnect Ports
- Oracle Content Management Software Development Kit Ports

C.3.1 J2EE and Web Cache Ports

Table C–9 provides guidelines for changing port numbers in a J2EE and Web Cache installation.

Table C–9 J2EE and Web Cache Ports

Component / Service	Can be changed?	Dependencies?	Procedure
Oracle HTTP Server			
Listen	Yes	Yes	Section 5.3.3, "Changing Oracle HTTP Server Ports"
Port	Yes	Yes	Section 5.3.3, "Changing Oracle HTTP Server Ports"
Listen (SSL)	Yes	Yes	Section 5.3.3, "Changing Oracle HTTP Server Ports"
Port (SSL)	Yes	Yes	Section 5.3.3, "Changing Oracle HTTP Server Ports"
Diagnostic	Yes	No	Section 5.3.14, "Changing the Oracle HTTP Server Diagnostic Port"
OracleAS Web Cache			
HTTP Listen	Yes	Yes	Section 5.3.4, "Changing the Web Cache Non-SSL Listener Port (Middle-Tier Installations)"
HTTP Listen (SSL)	Yes	Yes	Section 5.3.5, "Changing the Web Cache SSL Listener Port (Middle-Tier Installations)"
Administration	Yes	Yes	Section 5.3.6, "Changing the Web Cache Administration Port"
Invalidation	Yes	Yes	Section 5.3.7, "Changing the Web Cache Invalidation Port"
Statistics	Yes	No	Section 5.3.8, "Changing the Web Cache Statistics Port"
OC4J			
AJP	Yes	No	Section 5.3.2, "Changing OC4J Ports"
JMS	Yes	No	Section 5.3.2, "Changing OC4J Ports"
RMI	Yes	No	Section 5.3.2, "Changing OC4J Ports"
IIOP	Yes	No	Section 5.3.2, "Changing OC4J Ports"

Table C–9 (Cont.) J2EE and Web Cache Ports

Component / Service	Can be changed?	Dependencies?	Procedure
IIOPS1 (Server only)	Yes	No	Section 5.3.2, "Changing OC4J Ports"
IIOPS2 (Server and client)	Yes	No	Section 5.3.2, "Changing OC4J Ports"
OPMN			
ONS Local	Yes	No	Section 5.3.13, "Changing OPMN Ports (ONS Local, Request, and Remote)"
ONS Remote	Yes	Yes	Section 5.3.13, "Changing OPMN Ports (ONS Local, Request, and Remote)"
ONS Request	Yes	No	Section 5.3.13, "Changing OPMN Ports (ONS Local, Request, and Remote)"
Oracle Enterprise Manager			
Application Server Control	No	N / A	N / A
Application Server Control (SSL)	No	N / A	N / A
Application Server Control RMI	No	N / A	N / A
Oracle Management Agent	No	N / A	N / A
Miscellaneous Ports			
DCM Java Object Cache	Yes	No	Section 5.3.9, "Changing the DCM Java Object Cache Port"
Java Object Cache	Yes	No	Section 5.3.10, "Changing the Java Object Cache Port"
JServ Servlet Engine	Yes	No	Section 5.3.11, "Changing the JServ Servlet Engine Port"
Log Loader	Yes	No	Section 5.3.12, "Changing the Log Loader Port"
Port Tunneling	Yes	No	Section 5.3.15, "Changing the Port Tunneling Port"

C.3.2 Portal and Wireless Ports

Guidelines for changing port numbers in a Portal and Wireless installation are listed in:

- Table C–9, " J2EE and Web Cache Ports"
- Table C–10, " Portal and Wireless Ports"

Table C–10 Portal and Wireless Ports

Component / Service	Can be changed?	Dependencies?	Procedure
Oracle Ultra Search			
RMI Daemon	No	N / A	N / A
RMI Registry	No	N / A	N / A
OracleAS Portal			
OracleAS Portal[1]	N / A	N / A	N / A
OracleAS Wireless			
OracleAS Wireless[1]	N / A	N / A	N / A
Wireless Notification Dispatcher Calendar	No	N / A	N / A

[1] This service does not have its own port. You can access it through the HTTP listener port.

C.3.3 Business Intelligence and Forms Ports

Guidelines for changing port numbers in a Business Intelligence and Forms installation are listed in:

- Table C–9, " J2EE and Web Cache Ports"
- Table C–10, " Portal and Wireless Ports"
- Table C–11, " Business Intelligence and Forms Ports"

Table C–11 Business Intelligence and Forms Ports

Component / Service	Can be changed?	Dependencies?	Procedure
OracleAS Discoverer			
OracleAS Discoverer[1]	N/A	N/A	N/A
OracleAS Discoverer OSAgent	No	N/A	N/A
OracleAS Forms Services			
OracleAS Forms Services[1]	N/A	N/A	N/A
OracleAS Reports Services			
SQL*Net *For 6i Backward Compatibility Only*	Yes	No	Section 5.5.3, "Changing the OracleAS Reports Services SQL*Net Port"
Visigenics CORBA - Reports 9*i*	No	N/A	N/A

[1] This service does not have its own port. You can access it through the HTTP listener port.

C.3.4 Infrastructure Ports

Guidelines for changing port numbers in an Infrastructure installation are listed in:

- Table C–9, " J2EE and Web Cache Ports"
- Table C–12, " Infrastructure Ports"

Table C–12 Infrastructure Ports

Component / Service	Can be changed?	Dependencies?	Procedure
Oracle Internet Directory			
Oracle Internet Directory	Yes	Yes	Section 5.6.2, "Changing Oracle Internet Directory Ports"
Oracle Internet Directory (SSL)	Yes	Yes	Section 5.6.2, "Changing Oracle Internet Directory Ports"
OracleAS Certificate Authority			
Server Authentication Virtual Host (SSL)	Yes	No	Section 5.6.4, "Changing OracleAS Certificate Authority Ports"
Mutual Authentication Virtual Host (SSL)	Yes	No	Section 5.6.4, "Changing OracleAS Certificate Authority Ports"
OracleAS Metadata Repository			
Oracle Net Listener	Yes	Yes	Section 5.6.1, "Changing the Metadata Repository Net Listener Port"
OracleAS Single Sign-On			
OracleAS Single Sign-On[1]	N / A	N / A	N / A

[1] This service does not have its own port. You can access it through the HTTP listener port.

C.3.5 OracleAS ProcessConnect Ports

Table C–13 provides guidelines for changing port numbers in an OracleAS ProcessConnect installation.

Table C–13 OracleAS ProcessConnect Ports

Service	Can be changed?	Dependencies?	Procedure
B2B Adapter RMI	Yes	No	Refer to *Oracle Application Server ProcessConnect User's Guide*
Integration Manager	Yes	No	Refer to *Oracle Application Server ProcessConnect User's Guide*
Adapter Framework	Yes	No	Refer to *Oracle Application Server ProcessConnect User's Guide*
Actional Agent	Yes	No	Refer to *Oracle Application Server ProcessConnect User's Guide*
Actional Listener	Yes	No	Refer to *Oracle Application Server ProcessConnect User's Guide*
Attunity Adapters (Legacy Adapters)	Yes	No	Refer to *Oracle Application Server ProcessConnect User's Guide*

C.3.6 OracleAS InterConnect Ports

Table C–13 provides guidelines for changing port numbers in an OracleAS InterConnect installation.

Table C–14 OracleAS InterConnect Ports

Service	Can be changed?	Dependencies?	Procedure
OracleAS InterConnect Adapters	Yes	No	You can change this port by manually configuring `repository.ini`
OracleAS InterConnect Repository	Yes	No	You can change this port by manually configuring `adapter.ini`
RMI port for HTTP	Yes	Yes	You can change this port by manually configuring `adapter.ini`. You must also update `web.xml` with the new port number.

C.3.7 Oracle Content Management Software Development Kit Ports

Table C–15 provides guidelines for changing port numbers in an Oracle Content Management Software Development Kit installation.

Table C–15 Oracle Content Management Software Development Kit Ports

Service	Can be changed?	Dependencies?	Procedure
AFP *(myhost.mydomain Node)*	No	N / A	N / A
CUP *(myhost.mydomain Node)*	Yes	No	Edit `CupServerConfiguration` and update `IFS.SERVER.PROTOCOL.CUP.Port`. Then reload the CUP server.
Domain Controller	No	N / A	N / A
FTP *(myhost.mydomain Node)*	Yes	No	Edit `FtpServerConfiguration` and update `IFS.SERVER.PROTOCOL.FTP.Port`. Then reload the FTP server.
IMAP *(myhost.mydomain Node)*	No	N / A	N / A
IMAP (SSL) *(myhost.mydomain Node)*	No	N / A	N / A
NB UDP *(myhost.mydomain Node)*	No	N / A	N / A
NFS *(myhost.mydomain Node)*	Yes	No	Edit `NfsServerConfiguration` and update `IFS.SERVER.PROTOCOL.NFS.Port`. Then reload the NFS Server. Refer to *Oracle Content Management SDK Administrator's Guide*.
NFS Mount Port *(myhost.mydomain Node)*	Yes	No	Edit `NfsServerConfiguration` and update `IFS.SERVER.PROTOCOL.NFS.MountPort`. Then reload the NFS Server. Refer to *Oracle Content Management SDK Administrator's Guide*.
Node Guardian *(myhost.mydomain Node)*	No	N / A	N / A

Table C–15 (Cont.) Oracle Content Management Software Development Kit Ports

Service	Can be changed?	Dependencies?	Procedure
Node Guardian *(myhost.mydomain HTTP Node)*	No	N / A	N / A
Node Manager *(myhost.mydomain Node)*	No	N / A	N / A
Node Manager *(myhost.mydomain HTTP Node)*	No	N / A	N / A
SMB *(myhost.mydomain Node)*	No	N / A	N / A
SMTP *(myhost.mydomain Node)*	No	N / A	N / A

D

Metadata Repository Schemas

A Metadata Repository is an Oracle database that is pre-seeded with additional schemas to support Oracle Application Server. This appendix provides information about those schemas.

It contains the following topics:

D.1 Metadata Repository Schema Descriptions

This section lists the Metadata Repository schemas and describes their contents.

The schemas are divided into three categories:

- Identity Management Schemas

  These schemas are used by Identity Management components, such as OracleAS Single Sign-On and Oracle Internet Directory.

- Product Metadata Schemas

  These schemas are used by middle-tier application components, such as OracleAS Portal and OracleAS Wireless.

- Management Schema

  This is a single schema that is used by Distributed Configuration Management (DCM).

There is one additional schema that does not fall into the previously listed categories: `INTERNET_APPSERVER_REGISTRY`. This schema contains release numbers for Metadata Repository schemas.

> **See Also:** Section H.5, "Viewing Metadata Repository Release Numbers" for information on using the `INTERNET_APPSERVER_REGISTRY` schema to query release numbers

D.1.1 Identity Management Schemas

Table D–1 lists the schemas used by Identity Management components, sorted alphabetically by component.

Table D–1 Identity Management Schemas

Component	Schema	Description
Oracle Internet Directory	ODS	For internal use
OracleAS Single Sign-On	ORASSO	For internal use
OracleAS Single Sign-On	ORASSO_DS	For internal use
OracleAS Single Sign-On	ORASSO_PA	For internal use
OracleAS Single Sign-On	ORASSO_PS	For internal use
OracleAS Single Sign-On	ORASSO_PUBLIC	For internal use
OracleAS Certificate Authority	OCA	For internal use
OracleAS Certificate Authority	ORAOCA_PUBLIC	For internal use

D.1.2 Product Metadata Schemas

Table D–2 lists the schemas used by middle-tier application components, sorted alphabetically by component.

Table D–2 Product Metadata Schemas

Component	Schema	Description
Oracle Ultra Search	WK_TEST	Oracle Ultra Search default instance schema—contains the document information and document index of the default Oracle Ultra Search instance
Oracle Ultra Search	WKPROXY	Oracle Ultra Search proxy database user—does not contain any data
Oracle Ultra Search	WKSYS	Oracle Ultra Search metadata repository—contains metadata information on data sources, crawler configuration, crawling schedules, trace logs, attribute mappings, authentication, and user privileges of Oracle Ultra Search instances

Table D–2 (Cont.) Product Metadata Schemas

Component	Schema	Description
Oracle Workflow	OWF_MGR	Contains design-time and runtime workflow tables, queues, PL/SQL code, directory service database views and local tables, and metadata for workflow processes and business events
OracleAS Discoverer	DISCOVERER5	Contains metadata for Discoverer Portlet Provider, portlet definitions for user portlets, and cached data obtained by running scheduled Discoverer queries. Has RESOURCE and CONNECT privileges.
OracleAS Portal	PORTAL	Contains Portal database objects and code. This schema also represents the proxy user account that mod_plsql uses to connect to the database through the credentials provided in the corresponding DAD.
OracleAS Portal	PORTAL_APP	Used for authentication of external JSP applications
OracleAS Portal	PORTAL_DEMO	Demonstration code
OracleAS Portal	PORTAL_PUBLIC	All lightweight users are mapped to this schema by default. All procedures publicly accessible through the Web are granted execute to PUBLIC, which makes them accessible through this schema.
OracleAS ProcessConnect	IP	Design and runtime repository. The design repository has modeling metadata and profile data for an integration. These describe the behavior of the integration and sequence of steps required to execute the business process. The modeling and profile metadata is the design of the integration prior to deployment and execution. Once the integration is deployed, the runtime repository contains the metadata required to execute the integration as well as the business process instance, event instances, role instances, and other data created during execution.
OracleAS Syndication Services	DSGATEWAY	Contains offer, subscription, and content provider information; channel portlet metadata; runtime system properties; escheduling information

Table D–2 (Cont.) Product Metadata Schemas

Component	Schema	Description
OracleAS UDDI Registry	UDDISYS	Contains UDDI entities such as business entities, business services, binding templates, tModels, and publisher assertions; taxonomy structures like North American Industy Classification System (NAICS), Universal Standard Products and Services Codes (UNSPSC), and ISO 3166 Geographic Taxonomy (ISO 3166); UDDI replication / subscription related internal tables; and other administration-related views and tables
OracleAS Web Clipping	WCRSYS	Web Clipping Repository for support with Wireless—contains clipping definitions, user customizations, and PL / SQL packages for their access
OracleAS Wireless	WIRELESS	Contains user content (folders, services, links, notifications, presets), user customization data, groups, roles, transient user information, style sheets, logical device definitions, Java transformers (serialized), adapters, location data, configuration data, process runtime state, and application metrics

D.1.3 Management Schema

Table D–3 lists the schema used by Distributed Configuration Management (DCM).

Table D–3 Management Schema

Component	Schema	Description
Distributed Configuration Management (DCM)	DCM	Contains configuration information for OC4J and Oracle HTTP Server instances, application server instances, clusters, and farms

D.2 Metadata Repository Schemas, Tablespaces, and Default Datafiles

Table D–4 lists the tablespace and default datafile for each Metadata Repository schema. It is sorted alphabetically by component.

Table D–4 Metadata Repository Tablespaces and Default Datafiles

Component	Schema	Tablespace	Default Datafile
Distributed Configuration Management (DCM)	DCM	DCM	dcm.dbf
Metadata Repository Version	INTERNET_APPSERVER_REGISTRY	IAS_META	ias_meta01.dbf
Oracle Internet Directory	ODS	OLTS_ATTRSTORE	attrs1_oid.dbf
Oracle Internet Directory	ODS	OLTS_BATTRSTORE	battrs1_oid.dbf
Oracle Internet Directory	ODS	OLTS_CT_STORE	gcats1_oid.dbf
Oracle Internet Directory	ODS	OLTS_DEFAULT	gdefault1_oid.dbf
Oracle Internet Directory	ODS	OLTS_SVRMGSTORE	svrmg1_oid.dbf
Oracle Ultra Search	WK_TEST	IAS_META	ias_meta01.dbf
Oracle Ultra Search	WKPROXY	IAS_META	ias_meta01.dbf
Oracle Ultra Search	WKSYS	IAS_META	ias_meta01.dbf
Oracle Workflow	OWF_MGR	IAS_META	ias_meta01.dbf
OracleAS Certificate Authority	OCA	OCATS	oca.dbf
OracleAS Certificate Authority	ORAOCA_PUBLIC	IAS_META	ias_meta01.dbf
OracleAS Discoverer	DISCOVERER5	DISCO_PTM5_META	discopltm1.dbf
OracleAS Discoverer	DISCOVERER5	DISCO_PTM5_CACHE	discopltc1.dbf
OracleAS Portal	PORTAL	PORTAL	portal.dbf
OracleAS Portal	PORTAL	PORTAL_DOC	ptldoc.dbf
OracleAS Portal	PORTAL	PORTAL_IDX	ptlidx.dbf
OracleAS Portal	PORTAL	PORTAL_LOG	ptllog.dbf
OracleAS Portal	PORTAL_APP	PORTAL	portal.dbf
OracleAS Portal	PORTAL_DEMO	PORTAL	portal.dbf
OracleAS Portal	PORTAL_PUBLIC	PORTAL	portal.dbf

Table D–4 (Cont.) Metadata Repository Tablespaces and Default Datafiles

Component	Schema	Tablespace	Default Datafile
OracleAS ProcessConnect	IP	IP_DT	ip_dt.dbf
OracleAS ProcessConnect	IP	IP_RT	ip_rt.dbf
OracleAS ProcessConnect	IP	IP_LOB	ip_lob.dbf
OracleAS ProcessConnect	IP	IP_IDX	ip_idx.dbf
OracleAS Single Sign-On	ORASSO	IAS_META	ias_meta01.dbf
OracleAS Single Sign-On	ORASSO_DS	IAS_META	ias_meta01.dbf
OracleAS Single Sign-On	ORASSO_PA	IAS_META	ias_meta01.dbf
OracleAS Single Sign-On	ORASSO_PS	IAS_META	ias_meta01.dbf
OracleAS Single Sign-On	ORASSO_PUBLIC	IAS_META	ias_meta01.dbf
OracleAS Syndication Services	DSGATEWAY	DSGATEWAY_TAB	oss_sys01.dbf
OracleAS UDDI Registry	UDDISYS	UDDISYS_TS	uddisys01.dbf
OracleAS Web Clipping	WCRSYS	WCRSYS_TS	wcrsys01.dbf
OracleAS Wireless	WIRELESS	IAS_META	ias_meta01.dbf

E

printlogs Tool Syntax and Usage

This appendix describes the `printlogs` command-line tool. You can use `printlogs` to print the contents of Oracle Application Server diagnostic log files to standard output.

It contains the following topics:

E.1 Introduction

The `printlogs` command-line tool reads logs generated by Oracle Application Server components and prints the content of the logs to standard output in a common format. `printlogs` supports many options for reading and filtering log files, and formatting the output.

> **See Also:** Chapter 4, "Managing Log Files" for more information on Oracle Application Server logging

Location

The `printlogs` command is located in:

ORACLE_HOME`/diagnostics/bin/printlogs`

Notes

- In order to run `printlogs`, you must log in as a user that has permission to read all of the log files in your Oracle home, for example, the user that installed Oracle Application Server.
- By default, `printlogs` operates on the Oracle home it resides in. You can override this with the `-home` option. Note that `printlogs` does not use the `ORACLE_HOME` environment variable.
- `printlogs` options are not case-sensitive.
- By default, `printlogs` uses the contents of the directory *ORACLE_HOME*`/diagnostics/config/registration` to determine which log files to read, the location of log files, and additional configuration information about each log file. You can override this with the `-repository`, `-registration`, and `-logs` options.

> **See Also:** Section 4.6.4, "Component Diagnostic Log File Registration" for more information

E.2 Basic Syntax

```
printlogs [input options] [filter options] [output options] [general options]
```

Input Options

```
[-home oracle_home_path] [-repository]

[-home oracle_home_path] [-registration registration_directory_path]
[filter options] [output options] [general options]
[-logs log_path [log_path ...]]
```

Filter Options

```
[-tail n] [-last n[s|m|h|d]] [-query expression]

expression:
    simple_expression
    -not simple_expression
    simple_expression -and simple_expression
    simple_expression -or simple_expression

simple_expression:
    field_name op value
    ( expression )
```

field_name:
An ODL log record field name. See Section E.4, "Log Record Fields" for a list of field names.

```
op:
    -eq | -eq_case | -contains | -contains_case |
    -startswith | -startswith_case | -from | -to
```

value:
A string or timestamp, depending on the operation (*op*)

Ouput Options

```
[-odl | -odl_complete | -text | -text_short | -text_full] [-orderBy
orderByFieldList]

[-count [groupByFieldList]]
```

General Options

```
[-help] [-f] [-sleep n] [-notailopt]
```

E.3 Detailed Option Descriptions

This section provides detailed descriptions of `printlogs` options. It contains the following sections:

- Input Options
- Filter Options
- Ouput Options
- General Options

E.3.1 Input Options

You can use input options to specify the location of logs and log definitions. The default is the local Oracle home. Table E–1 describes the input options in detail.

Table E–1 Input Options

Input Option	Description
`-home` *`oracle_home_path`*	Specify an alternate Oracle home directory from where to read logs and log definitions
`-repository`	Specify that log records should be read from the common repository instead of directly from each log. The common repository is updated by the Log Loader. The Log Loader must be running in order for the repository to contain the contents of Oracle Application Server component logs.
`-repos`	Same as -repository
`-registration` *`registration_directory_path`*	Specify an alternate registration directory that contains definitions of log files to be read by `printlogs`. The default registration directory is *`ORACLE_HOME`*`/diagnostics/config/registration`.
`-logs` *`log_path`* `[`*`log_path`* `...]`	Specify one or more logs to be read by `printlogs`. *`log_path`* is the full path to the log file, or the path relative to the current directory. The registration directory is used to find the definition of each log. If one of the specified logs is not defined in the registration directory, it is read by the default "UnformattedTextLogReader". Note: The `-logs` option must be at the end of the `printlogs` argument list, after the query options, output options, and general options.

E.3.2 Filter Options

You can use filter options to define which log records `printlogs` should print. The default is to print all records generated in the last 10 minutes. Table E–2 describes the filter options in detail.

Table E–2 Filter Options

Filter Option	Description
`-tail` *n*	Perform an operation similar to the UNIX "tail" command before reading a log. The *n* argument must be a positive number. The meaning of the *n* argument depends on the log type. For ODL logs, `printlogs` searches backwards from the end of the log for *n* occurrences of the pattern "<MESSAGE>" and starts reading the log from that point. For other log types, it reads the last *n* lines of the log.
`-last` *n*`[s|m|h|d]`	Print only logs generated in a specified period of time. The default is 10 minutes. You can use the *n* argument to specify a different period of time. The *n* argument must be a positive number. You can use a suffix to specify a unit of time: "`s`" for seconds, "`m`" for minutes, "`h`" for hours, and "`d`" for days. The default unit of time is minutes. If you would like to search through the logs generated over a large period of time, you can use a large value such as `100d`. The value of the `-last` option is used by `printlogs` to perform a "tail optimization" before it starts reading the logs. It performs an operation similar to the UNIX "tail" command to each log until it finds a timestamp that is within the desired range. This speeds up most inquiries significantly, but, if the log contains records out of timestamp order, it can cause `printlogs` to miss some records. It can also make queries slower in a few cases, for example, when you search the entire log. You can disable "tail optimization" with the -notailopt option.
`-query` *expression*	Apply *expression* to each log record to filter out undesirable records. See Table E–3 for a description of *expression*.

Table E–3 describes the query expressions you can use with the `-query` filter option in the `printlogs` command.

Table E–3 Query Expression Options

Query Expression Option	Description
`()`	You can use parenthesis as delimiters for complex sub-expressions. Parenthesis have special meaning to most UNIX command shells and you must use an escape character with them. This is not necessary on Windows.
`-not`	Logical negation
`-and`	Logical and
`-or`	Logical or
`fieldname`	An ODL log record field name. See Section E.4, "Log Record Fields" for a list of available field names.
`-eq`	Equality operation (case-insensitive). You can use this operation with all log record fields.
`-eq_case`	Same as -eq, except case-sensitive
`-contains`	Contains operation (case-insensitive). The result is true only if the log record field value contains the value operand string. You can use this operation only with "string" log record fields (all fields except `TSTZ_ORIGINATING` and `TSTZ_NORMALIZED`).
`-contains_case`	Same as -contains, except case-sensitive
`-startswith`	Starts with operation (case-insensitive). The result is true only if the log record field value starts with the value operand string. You can use this operation only with "string" log record fields (all fields except `TSTZ_ORIGINATING` and `TSTZ_NORMALIZED`).
`-startswith_case`	Same as -startswith, except case-sensitive
`-from`	This operation can only be used with timestamped log record fields (`TSTZ_ORIGINATING` and `TSTZ_NORMALIZED`). The result is true only if the log record timestamp is equal to or greater than the operand value. The operand value must be either in the ISO 8601 time format (for example: 2003-06-30T12:00:00.000-08:00), or in the date / time format of the default Java locale. By default, `printlogs` searches for timestamped records generated in the last 10 minutes. You can use the -last n[s | m | h | d] option in conjunction with the `-from` option to ensure the search period includes the specified timestamped records.

Table E–3 (Cont.) Query Expression Options

Query Expression Option	Description
`-to`	This operation can only be used with timestamped log record fields (TSTZ_ORIGINATING and TSTZ_NORMALIZED). The result is true only if the log record timestamp is less than or equal to the operand value. The operand value must be either in the ISO 8601 time format (for example: 2003-06-30T12:00:00.000-08:00), or in the date / time format of the default Java locale. By default, `printlogs` searches for timestamped records generated in the last 10 minutes. You can use the -last n[s | m | h | d] option in conjunction with the `-to` option to ensure the search period includes the specified timestamped records.

E.3.3 Ouput Options

You can use output options to specify an output format. The default is format is `-text_short`. Table E–4 describes the output options in detail.

Table E–4 Output Options

Output Option	Description
`-odl`	Specify that the output should be in ODL format. This option outputs an ODL document without the enclosing LOG tags. The generated output is not a complete XML document.
`-odl_complete`	Specify that the output should be in ODL format and that a complete XML document should be generated
`-text_short`	Specify that the output should be in a short text format including only the following fields: `TSTZ_ORIGINATING`, `COMPONENT_ID`, `MSG_TYPE`, `MODULE_ID`, `EXEC_CONTEXT_ID`, `MSG_TEXT`, and `SUPPL_DETAIL`. This is the default output format.
`-text`	Same as -text_short
`-text_full`	Specify that the output should be in full text format, including all message fields
`-orderBy` *`orderByFieldList`*	Sort the result in the specified order. The *`orderByFieldList`* argument is a list of log record field names separated by spaces. The field names can have an optional suffix of `:asc` or `:desc` to specify ascending or descending order. The default sort order is ascending. `printlogs` sorts the result in memory. If the result is large, it could run out of memory. In this case, you must provide additional filtering options to reduce the number of records in the result.
`-count [`*`groupByFieldList`*`]`	Report only the record count. The *`groupByFieldList`* argument is an optional list of log record field names separated by spaces. If you supply this argument, `printlogs` reports the record count for each supplied field.

E.3.4 General Options

You can use general options to obtain help, cause `printlogs` to loop, and disable optimization. Table E–5 describes the general options on detail.

Table E–5 General Options

General Option	Description
`-help`	Print detailed help.
`-f`	Follow. When you use this option, `printlogs` will not return after printing the result. Instead, it will go on an infinite loop where it sleeps for a number of seconds (specified with the -sleep `n` option), and then checks each log again and prints any new records that satisfy the query predicate.
`-sleep` *n*	Set the sleep time, in seconds, for the -f option. The default value is 20 seconds.
`-notailopt`	Disable the "tail optimization" that is usually performed with the -last option.

E.4 Log Record Fields

The `printlogs` command automatically translates the contents of any log file that it reads to the Oracle Diagnostic Logging (ODL) format. The ODL log record fields can be used to create a query expression, or to specify a group-by or order-by field list. Each field must be referred to by its names as described in Table E–6. Some of these fields are designated for future use, and currently are not used in any diagnostic messages generated by an Oracle Application Server

Table E–6 Log Record Fields

Log Record Field Name	Description
`COMPONENT_ID`	The component that originated the message
`DETAIL_PATH`	A URL for additional information about the message
`DOWNSTREAM_COMPONENT_ID`	The component that the originating component is working with on the downstream (server) side
`EID.SEQ`	The sequence number that is associated with the error instance
`EID.UNIQUE_ID`	A global unique identifier of an error instance associated with the message. This identifier can be used to correlate error messages from different components.
`EXEC_CONTEXT_ID.SEQ`	The sequence number that is associated with the execution context

Table E–6 (Cont.) Log Record Fields

Log Record Field Name	Description
EXEC_CONTEXT_ID.UNIQUE_ID	A global unique identifier of the thread of execution in which the originating component participates. This identifier can be used to correlate messages from several components that may be involved in the same thread of execution.
HOST_ID	The host name where the message originates
HOST_NWADDR	The network address of the host where the message originates
HOSTING_CLIENT_ID	An identifier for the client or security group to which the message relates
MODULE_ID	An identifier of the module that originated the message
MSG_ARG	A list of arguments to be bound with the message text. The argument is a list of an optional name and value. *Note: This field is not currently supported.*
MSG_GROUP	The name of the group to which the message belongs
MSG_ID	A message number, or some other value, that uniquely identifies the message within the component
MSG_LEVEL	The level qualifies the message type, indicating the degree of severity of the message. The value is an integer from 1 (highest severity) to 32 (lowest severity).
MSG_TEXT	A descriptive text for the message
MSG_TYPE	The type of the message. The defined message types are: INTERNAL_ERROR, ERROR, WARNING, NOTIFICATION, and TRACE. The value UNKNOWN may be used when the type is not known.
ORG_ID	The organization that wrote the component that originated the message
PROCESS_ID	An identifier of the process or execution unit that generated the message. For Java processes, the value can also include a thread identifier.
SUPPL_DETAIL	Supplemental information about the message
TSTZ_NORMALIZED	Date and time when the message was generated, adjusted for time difference between the host on which the message was generated and the host of the common repository. This field is only used if the log record is being read from a database repository.

Table E–6 (Cont.) Log Record Fields

Log Record Field Name	Description
TSTZ_ORIGINATING	Date and time when the message was generated
UPSTREAM_COMPONENT_ID	The component that the originating component is working with on the upstream (client) side
USER_ID	The user whose execution context originated the message

E.5 Environment Variable

You can use an environment variable to pass information to `printlogs`. Table E–7 describes the environment variable in detail.

Table E–7 Environment Variable

Environment Variable	Description
ORACLE_PRINTLOGS_JVM_ARGS	Provide additional arguments to the JVM that runs `printlogs`. Is is usually not necessary to provide additional JVM arguments, but this environment variable can be used in some situations, such as to set memory size, or provide additional properties to `printlogs`.

E.6 Examples

- To print records from all known logs in the last 10 minutes:

  ```
  printlogs
  ```

- To print records from all known logs in the last 10 minutes and follow:

  ```
  printlogs -f
  ```

  After reaching the end of all log files, `printlogs` will go into an infinite loop where it sleeps for 20 seconds, then reads and prints any new records that are added to the log files.

- To print records from the common repository in the last 2 hours:

  ```
  printlogs -repository -last 2h
  ```

- To print records from all known logs in the specified Oracle home in the last 2 days, in ODL format:

  ```
  printlogs -home /private/orahome2 -last 7d -odl
  ```

- To print records that are timestamped between 14:00 and 14:05 hours:

  ```
  printlogs -last 100d -query TSTZ_ORIGINATING -from 2003-07-15T14:00:00-07:00
  -and TSTZ_ORIGINATING -to 2003-07-15T14:05:00-07:00
  ```

  In this example, we assume that the specified time interval is more than 10 minutes before the current time. By default, `printlogs` searches logs generated in the last 10 minutes. We therefore need to use the `-last` option to increase the overall search length to include the timestamp interval. To save the trouble of calculating the amount of time to the timestamp interval, you can specify a very large value, such as `-last 100d`.

- To print records from OC4J logs that contain the word "exception" and are for the local Oracle home:

  ```
  printlogs -last 1d -query \( COMPONENT_ID -eq OC4J -and MODULE_ID
  -startswith home \)-and MSG_TEXT -contains exception
  ```

  Note: On the Windows platform the parenthesis should not be escaped.

- To print records in the last 10 minutes, sorted in ascending order by component id, and in descending order by time:

  ```
  printlogs -orderBy COMPONENT_ID TSTZ_ORIGINATING:desc
  ```

- To print the number of records from all known logs in the last 10 minutes, grouping by component and message type:

  ```
  printlogs -count COMPONENT_ID MESSAGE_TYPE
  ```

- To print records in the last hour from `daemon_logs` and `dcmctl_logs`:

  ```
  cd ORACLE_HOME/dcm/logs
  printlogs -last 1h -logs daemon_logs dcmctl_logs
  ```

  Note that this example uses log file names relative to the current directory.

- To print records in the last 10 minutes from `ipm.log` and `ons.log`:

  ```
  printlogs -logs ORACLE_HOME/opmn/logs/ipm.log ORACLE_HOME/opmn/logs/ons.log
  ```

  Note that this example uses the full path to the log files and can be run from any directory.

F

Auxiliary Procedures for Changing Infrastructure Services

This appendix contains auxiliary procedures that are referred to in Chapter 8, "Changing Infrastructure Services".

It contains the following topics:

- About LDAP-based Replicas
- Installing and Setting Up an LDAP-based Replica
- Migrating SSO and DIP Data
- Migrating Oracle Internet Directory Data

F.1 About LDAP-based Replicas

This section describes how to install and configure an LDAP-based Replica, specifically for use by the following procedures:

- Section 8.4, "Moving Identity Management to a New Host"
- Section 8.5, "Changing from a Test to a Production Environment"

F.1.1 What is an LDAP-based Replica?

Oracle Internet Directory replication is the process of copying and maintaining the same data (or naming context) on multiple directory servers. Simply put, replication is a means of having two identical directories that contain the same information. One directory is called the master (or supplier). This directory contains the master copy of the naming context. The other directory is called the replica (or consumer). The master supplies replication updates to the replica, which keeps the master and replica in sync.

There are different types of replicas. This procedure uses an LDAP-based Replica, which means the protocol for transferring data between the master and the replica is LDAP.

> **See Also:** *Oracle Internet Directory Administrator's Guide* for more information on directory replication and LDAP-based Replicas

For the purposes of this procedure, the master and replica directories are part of a larger environment that includes the Identity Management installations that contain the directories, and the Metadata Repositories that support them. This is called the LDAP-based Replica Environment, and it contains the following:

Master—The Identity Management installation containing the Oracle Internet Directory that holds the master copy of the naming context. It supplies replication updates to the Replica.

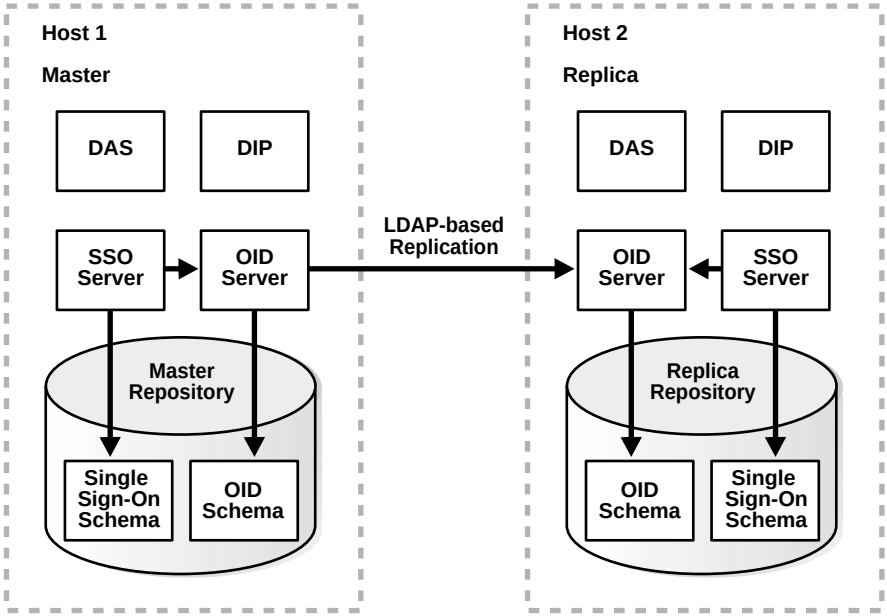
Master Repository—The Metadata Repository that the Master uses to store its Identity Management schemas.

Replica—The Identity Management installation containing the replicated Oracle Internet Directory.

Replica Repository—The Metadata Repository that the Replica uses to store its Identity Management schemas.

Figure F–1 illustrates the LDAP-based Replica environment.

Figure F–1 LDAP-based Replica Environment



F.1.2 How is the LDAP-based Replica Used for Changing Infrastructure Services?

Typically, an LDAP-based Replica is used to provide high availability and improved performance for directory users. For the purposes of changing Infrastructure services, the LDAP-based Replica is used as follows:

- For Section 8.4, "Moving Identity Management to a New Host", the LDAP-based Replica is created as a way of moving Identity Management from one host to another. The Master is the original Identity Management installation, and the Replica is the new Identity Management installation. In this case, replication is used to create an identical copy of the original Identity Management on a new host. You can then change your middle tiers from the old Identity Management (Master) to the new Identity Management (Replica) and discard the Master.
- For Section 8.5, "Changing from a Test to a Production Environment", the Replica is used to create a Test to Production environment. The Master is the Production Identity Management, and the Replica is the Test Identity Management. When you are ready to merge your Test Environment into your Production Environment, you can migrate data from your Test Identity

Management (Replica) to your Production Identity Management (Master) and change your middle-tiers from the Test Identity Management to the Production Identity Management. You can then discard the Test Identity Management or continue to use it for testing.

F.2 Installing and Setting Up an LDAP-based Replica

This section describes how to install and set up an LDAP-based Replica environment.

F.2.1 Things to Know Before You Start

You should be aware of these important items before you start the procedure:

- This procedure uses a single Infrastructure Oracle home that contains Identity Management and the Metadata Repository. However, it is fine to split the Infrastructure installation so Identity Management is in one Oracle home and the Metadata Repository is in another Oracle home. You can also distribute the Identity Management components (SSO, OID, DAS, DIP) across different hosts. If you do this, perform the operations on each component in their respective Oracle homes.
- The Replica always uses port 389 for the non-SSL OID port, and 636 for the SSL OID port, regardless of what is reported by Oracle Universal Installer, or printed in *ORACLE_HOME*`/install/portlist.ini`. Make sure no other processes are using ports 389 and 636 on the Replica host before you start the procedure.
- Make sure you use the `ldapsearch` and `ldapmodify` commands that are in *ORACLE_HOME*`/bin`. (Some operating systems ship their own version of these commands—do not use those.)
- The procedure contains many Oracle Internet Directory operations and requires a familiarity with Oracle Internet Directory administration and replication.
- The procedure contains many steps. It is important to follow each step precisely and not skip any steps.
- The procedure includes Validation Steps. You should perform these checks to verify that you are proceeding successfully.
- The procedure requires you to provide many parameters. Rather than describe these parameters multiple times throughout the procedure, they are listed in Table F–1, in the order in which they are first used. As you work through the

procedure, each time you encounter a new parameter, you can refer to the table to learn how to obtain its value. Make a note of each value as you obtain it, and refer back to your notes as you continue through the procedure.

Table F–1 Parameters for Setting Up an LDAP-based Replica

Document Convention	Description
REPLICA_HOME	Replica Oracle home

replica_db_name	Name of the entry for the Replica Repository in *REPLICA_HOME*/network/admin/tnsnames.ora. For example, the *replica_db_name* is asdb.myco.com if the entry looks like this:
	`ASDB.MYCO.COM =`
	`(DESCRIPTION = ....`

replica_ods_passwd	Password for the ODS schema in the Replica Repository. The default is "ods".
replica_orcladmin_passwd	Replica orcladmin password. The default is "welcome".
replica_oid_port	Replica non-SSL OID port number. This value is always 389.
master_host	Master hostname (you can use the plain or fully-qualified hostname)
master_oid_port	Master non-SSL OID port number This is listed as OIDport in *MASTER_HOME*/config/ias.properties
master_ods_passwd	Password for the ODS schema in the Master Repository. The default value is the ias_admin password you supplied while installing the Master.
replica_host	Replica hostname
MASTER_HOME	Master Oracle home
master_orcladmin_passwd	Replica orcladmin password. The default value is the ias_admin password you supplied while installing the Master.
master_replicaid	Master replica ID. You obtain this value during the procedure.
master_agreementid	Master agreement identifier. You obtain this value during the procedure.
replica_replicaid	Replica replica ID. You obtain this value during the procedure.
replica_repository_dn	Replica Repository dn. You obtain this value during the procedure.
replica_ssl_oid_port	Replica SSL OID port number. This value is always 636.
replica_http_port	Oracle HTTP Server Listen port on the Replica. This value is listed in *REPLICA_HOME*/install/portlist.ini. The default is 7777.
replica_em_port	Application Server Control port on the Replica. This value is listed in *REPLICA_HOME*/install/portlist.ini. The default is 1810.

F.2.2 Procedure

This section contains the procedure for setting up an LDAP-based Replica. It contains the following tasks:

- Task 1: Obtain the Master and Master Repository
- Task 2: Install Middle-Tier Instances (Optional)
- Task 3: Install and Configure the Replica
- Task 4: Configure and Start Replication
- Task 5: Register the Replica OID with Application Server Control
- Task 6: Enable SSO, DAS, and DIP on the Replica

Task 1: Obtain the Master and Master Repository

Most likely, you already have your Master and Master Repository.

- If you are following the procedure in Section 8.4, "Moving Identity Management to a New Host", the Master and Master Repository are the installations you would like to move to a new host, and the LDAP-base Replica will be the relocated installations.
- If you are following the procedure in Section 8.5, "Changing from a Test to a Production Environment", the Master and Master Repository are your Production environment, and the Replica will be your Test environment.

If you are starting from scratch, you can install a Master and Master Repository as follows:

1. Install Oracle Application Server using Oracle Universal Installer.
2. Choose the Infrastructure Installation.
3. Choose to install Identity Management and OracleAS Metadata Repository.
4. Choose to configure the following components: Oracle Internet Directory, OracleAS Single Sign-On, Delegated Administration Services, and Directory Integration and Provisioning

Task 2: Install Middle-Tier Instances (Optional)

Most likely, you already have middle-tier instances using the Master for Identity Management services. This is fine, and, if desired, you can install and configure additional instances to use the Master now, or at the end of this procedure after you have configured the Replica, or both.

These middle-tier instances can use the Master Repository for their product metadata, or they can use a different repository.

Task 3: Install and Configure the Replica

In this task, you install and configure the Replica and Replica Repository. The general procedure is to install an Infrastructure and choose Identity Management and Metadata Repository. However, you deselect all Identity Management components (OID, SSO, DAS, and DIP). After installation, you perform manual steps to configure and start up OID, SSO, DAS, and DIP.

1. Install the Replica.

   Be sure to install the Replica on a different host than the Master.

   a. Install Oracle Application Server using Oracle Universal Installer.

   b. Choose the Infrastructure Installation.

   c. Choose to install Identity Management and OracleAS Metadata Repository.

   d. Deselect all of the components that you can, so only OracleAS Metadata Repository, Oracle HTTP Server, and OracleAS Containers for J2EE are selected.

   e. When asked if you would like to register the Metadata Repository with Oracle Internet Directory, check **Yes** and supply the connection information for the Master Oracle Internet Directory.

2. Start OID on the Replica.

   a. Create a wallet for the ODS password:

   ```
   REPLICA_HOME/bin/oidpasswd connect=replica_db_name create_wallet=TRUE
   current_password=replica_ods_passwd
   ```

   b. Make sure OPMN is running:

   ```
   REPLICA_HOME/opmn/bin/opmnctl ping
   ```

   If OPMN is not running, start it:

   ```
   REPLICA_HOME/opmn/bin/opmnctl start
   ```

   c. Enable OID by editing the following file:

   ```
   REPLICA_HOME/opmn/conf/opmn.xml
   ```

Modify the `ias-component` entry for OID so the status is enabled, as follows:

```
<ias-component id="OID" status="enabled">
```

Save and close the file.

d. Run the following command:

```
REPLICA_HOME/dcm/bin/dcmctl updateConfig
```

e. Reload opmn.xml:

```
REPLICA_HOME/opmn/bin/opmnctl reload
```

f. Start OID:

```
REPLICA_HOME/opmn/bin/opmnctl startproc ias-component=OID
```

3. Validation Step: Make sure the Replica OID is started:

```
REPLICA_HOME/bin/ldapbind -D cn=orcladmin -w replica_orcladmin_passwd -p
replica_oid_port
```

If the command fails, check the following files for information on why the server did not start:

```
REPLICA_HOME/ldap/log/oidmon.log
REPLICA_HOME/ldap/log/oidldap01*.log
```

You can check the files manually, or use Log Viewer (refer to Section 4.2, "Listing and Viewing Log Files With Enterprise Manager")

See Also: *Oracle Internet Directory Administrator's Guide*, appendix on Syntax for LDIF and Command Line Tools, for more information

4. Enable SSL for OID.

a. On the Replica host, create a file named `mod.ldif` that contains the following lines:

```
dn:cn=configset0,cn=osdldapd,cn=subconfigsubentry
changetype:modify
replace:orclsslenable
orclsslenable:2
```

b. Run the following command:

```
REPLICA_HOME/bin/ldapmodify -D cn=orcladmin -w replica_orcladmin_passwd
-p replica_oid_port -v -f mod.ldif
```

c. Restart OID:

```
REPLICA_HOME/opmn/bin/opmnctl restartproc ias-component=OID
```

5. Validation Step: Make sure the SSL port is enabled on the Replica OID:

```
REPLICA_HOME/bin/ldapbind -D cn=orcladmin -w replica_orcladmin_passwd -U 1
-p replica_ssl_oid_port
```

If the command fails, perform Step 4, "Enable SSL for OID" again.

Task 4: Configure and Start Replication

In this task, you register the Replica with the Master.

1. Set environment variables.
   a. Make sure the ORACLE_HOME environment variable is set.
   b. Set the library path.
      – On HPUX systems, make sure the SHLIB_PATH environment variable includes $ORACLE_HOME/lib32
      – On all other UNIX systems, make sure the LD_LIBRARY_PATH environment variable includes $ORACLE_HOME/lib
2. Run the following command to configure replication:

```
REPLICA_HOME/ldap/bin/remtool -paddnode
```

The tool prompts for information, as shown Table F–2.

Table F–2 Prompts for the remtool Command

At this prompt...	Enter...
Enter supplier directory details: Enter hostname of host running OID server	Master hostname (***master_host***)
Enter port on which OID server is listening	Master non-SSL OID port number (***master_oid_port***)
Enter replication dn password	Master Repository ODS schema password (***master_ods_passwd***)

Table F–2 (Cont.) Prompts for the remtool Command

At this prompt...	Enter...
Enter consumer directory details: Enter hostname of host running OID server	Replica hostname (***replica_host***)
Enter port on which OID server is listening	Replica non-SSL OID port number (***replica_oid_port***)
Enter replication dn password	Replica Repository ODS schema password (***replica_ods_passwd***)
Enter naming context (e-end, q-quit)	***** (Enter the asterisk character.)
Enter naming context (e-end, q-quit)	**e**
Following naming contexts will be included for replication: 1. * Do you want to continue? [y / n]	**y**

3. Validation Step: Check if replication is configured:

   REPLICA_HOME`/bin/ldapsearch -D cn=orcladmin -w` ***replica_orcladmin_passwd*** `-h` ***replica_host*** `-p` ***replica_oid_port*** `-b "cn=replication configuration" -s sub "objectclass=orclreplnamectxconfig" dn orclincludednamingcontexts`

   This command should return two entries of the following types:

   ```
   orclincludednamingcontexts=cn=oraclecontext
   orclincludednamingcontexts=*
   ```

   If it only returns one entry, and it is of the first listed type, there was a problem configuring replication. To recover, delete the Replica and repeat step 2, "Run the following command to configure replication".

   To delete the Replica:

   REPLICA_HOME`/ldap/bin/remtool -pdelnode`

   > **See Also:** *Oracle Internet Directory Administrator's Guide*, appendix on Syntax for LDIF and Command Line Tools, for more information on `remtool`

4. Change the server on the Replica to read-write mode.

a. On the Replica host, create a file named `mod.ldif` that contains the following lines:

```
dn:
changetype:modify
replace:orclservermode
orclservermode:rw
```

b. Run the following command:

```
REPLICA_HOME/bin/ldapmodify -D cn=orcladmin -w replica_orcladmin_passwd
-p replica_oid_port -v -f mod.ldif
```

5. Obtain the Master replica ID by running the following command:

```
MASTER_HOME/bin/ldapsearch -h master_host -p master_oid_port -D cn=orcladmin
-w master_orcladmin_passwd -b "" -s base "objectclass=*" orclreplicaid
```

The replica ID will look something like "`myhost_asdb`".

6. Obtain the Master agreement identifier by running the following command:

```
MASTER_HOME/bin/ldapsearch -h master_host -p master_oid_port -D cn=orcladmin
-w master_orcladmin_passwd -b "orclreplicaid=master_replicaid,cn=replication
configuration" -s sub "objectclass=orclreplagreemententry" dn
```

Where ***master_replicaid*** is the Master replica ID you obtained in the previous step.

The agreement identifier will look something like "`000002`".

7. Perform this step on the Master.

a. Create a file named `mod.ldif` that contains the following lines:

```
dn:cn=includednamingcontext000001,cn=replication namecontext,
orclagreementid=master_agreementid,orclreplicaid=master_replicaid,cn=rep
lication configuration
changetype:modify
replace:orclexcludednamingcontexts
orclexcludednamingcontexts:orclapplicationcommonname=orasso_ssoserver,cn
=sso,cn=products,cn=oraclecontext
```

Where ***master_agreementid*** is the Master agreement identifier and ***master_replicaid*** is the Master replica ID you obtained in the previous steps.

Note that in the above code example, the first 3 lines should be a single line in your file; the next line is a single line; the next line is a single line; and the final two lines should be a single line in your file.

b. Run the following command:

```
MASTER_HOME/bin/ldapmodify -D cn=orcladmin -w master_orcladmin_passwd -p
master_oid_port -v -f mod.ldif
```

8. Obtain the Replica replica ID by running the following command:

```
REPLICA_HOME/bin/ldapsearch -h replica_host -p replica_oid_port -D
cn=orcladmin -w replica_orcladmin_passwd -b "" -s base "objectclass=*"
orclreplicaid
```

The replica ID will look something like "`myhost_asdb`".

9. On the Replica host, modify the replica subentry to configure bootstrap.

a. Create a file named `mod.ldif` that contains the following lines:

```
dn:orclreplicaid=replica_replicaid,cn=replication configuration
changetype:modify
replace:orclreplicastate
orclreplicastate:0
```

replica_replicaid is the Replica replica ID you obtained in the previous step.

b. Run the following command:

```
REPLICA_HOME/bin/ldapmodify -D cn=orcladmin -w replica_orcladmin_passwd
-p replica_port -v -f mod.ldif
```

10. Start the Replica:

```
REPLICA_HOME/bin/oidctl connect=replica_db_name server=oidrepld instance=1
flags='-p replica_oid_port' start
```

Wait for the Replica to bootstrap before proceeding to the next step. You can monitor the progress of the bootstrap by watching the messages appended to the oidrepld log file with the following command:

```
tail -f REPLICA_HOME/ldap/log/oidrepld00.log
```

For example:

```
Starting scheduler...
Start to BootStrap from supplier=pdsun-qa5_orcl to consumer=pdsun-qa8_repsid
```

```
gslrbssSyncDIT:Replicating namingcontext=cn=oraclecontext......
gslrbssSyncDIT:Sync done successfully for cn=oraclecontext, 266 entries
matched
gslrbssSyncDIT:Replicating namingcontext=dc=com ......
gslrbssSyncDIT:Sync done successfully for dc=com, 197 entries matched
gslrbssSyncDIT:Replicating namingcontext=cn=oracleschemaversion ......
gslrbssSyncDIT:Sync done successfully for cn=oracleschemaversion, 10 entries
matched
```

Note that if you cannot locate the above log file, the Replica may have failed to start. Check the command you used at the beginning of this step to start the Replica and retry if you find any problems.

11. Validation Step: Verify the Replica has bootstrapped successfully.

The following commands should each return entries:

```
REPLICA_HOME/bin/ldapsearch -D cn=orcladmin -w replica_orcladmin_passwd -h
replica_host -p replica_oid_port -b "dc=com" -s sub "objectclass=*" dn
```

```
REPLICA_HOME/bin/ldapsearch -D cn=orcladmin -w replica_orcladmin_passwd -h
replica_host -p replica_oid_port -b "cn=oraclecontext" -s sub
"objectclass=*" dn
```

If either of the above commands does not return entries then there was a problem with the bootstrap.

12. Validation Step: Verify the SSO server entry is excluded from replication.

The following search against the Replica should not return an entry. It should return two entries: "No such object" and a matched entry.

```
REPLICA_HOME/bin/ldapsearch -D cn=orcladmin -w replica_orcladmin_passwd -h
replica_host -p replica_oid_port -b
"orclapplicationcommonname=orasso_ssoserver, cn=sso, cn=products,
cn=oraclecontext" -s base "objectclass=*" dn
```

The same search, when performed against the Master, should return an entry.

```
MASTER_HOME/bin/ldapsearch -D cn=orcladmin -w master_orcladmin_passwd -h
master_host -p master_oid_port -b
"orclapplicationcommonname=orasso_ssoserver, cn=sso, cn=products,
cn=oraclecontext" -s base "objectclass=*" dn
```

If there are any problems, repeat steps 7, 8, and 9 in Task 4, then restart the Replica as follows:

```
REPLICA_HOME/bin/oidctl connect=replica_db_name server=oidrepld instance=1
flags='-p replica_oid_port' restart
```

Task 5: Register the Replica OID with Application Server Control

In this task, you enable the Replica OID to show up in Application Server Control.

1. Create the `ldaptarget.xml` file by making a copy of the template:

   ```
   cd REPLICA_HOME/ldap/templates
   cp ldaptarget.xml.template ldaptarget.xml
   ```

2. Edit the `ldaptarget.xml` file and replace the following variables with values for your installation:

   s_instanceName is the instance name of the Replica. You can obtain this name with the following command:

   ```
   REPLICA_HOME/dcm/bin/dcmctl whichInstance
   ```

   s_hostName is the fully qualified Replica host name—the same value as *replica_host*.

   ORACLE_HOME is the Replica Oracle home—the same value as *REPLICA_HOME*.

   s_odsPwd is the password for the Replica ODS schema—the same value as *replica_ods_passwd*.

   s_tnsAddress is the Net Description string for the Replica repository. You can obtain this from *REPLICA_HOME*`/network/admin/tnsnames.ora`. For example:

   ```
   (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=myhost.myco.com)
   (PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=infra.myco.com)))
   ```

   Note you should enter the entire string with no new-line characters and no white-space characters.

   For example:

   ```
   <Target TYPE="oracle_ldap" NAME="infra.myhost.myco.com_LDAP"
   DISPLAY_NAME="OID" VERSION="2.5" ON_HOST="myhost.myco.com">
     <Property NAME="OracleHome" VALUE="/home/infra"/>
     <Property NAME="password" VALUE="ods" ENCRYPTED="FALSE"/>
     <Property NAME="LDAPScriptsPath" VALUE="/sysman/admin/scripts"/>
     <Property NAME="host" VALUE="myhost.myco.com"/>
     <Property NAME="UserName" VALUE="ods" ENCRYPTED="FALSE"/>
     <Property NAME="LDAPBindDN" VALUE="cn=emd admin,cn=oracle internet
   ```

```
directory" ENCRYPTED="FALSE"/>
  <Property NAME="LDAPBindPwd" VALUE=""/>
  <Property NAME="version" VALUE="9.0.4"/>
  <Property NAME="ConnectDescriptor"
VALUE="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=myhost.myco.c
om)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=asdb.myco.com)))"/>
  <CompositeMembership>
     <MemberOf TYPE="oracle_ias" NAME="infra.myhost.myco.com" ASSOCIATION="
"/>
  </CompositeMembership>
</Target>
```

3. Upload the OID target using the following command (note that the following is a single command; type it all on one line):

   REPLICA_HOME`/bin/emctl config addtarget`
   REPLICA_HOME`/ldap/templates/ldaptarget.xml` ***REPLICA_HOME***

4. Verify that OID shows up in Application Server Control:

   a. Make sure Oracle Enterprise Manager Application Server Control is started:

      REPLICA_HOME`/bin/emctl startifdown iasconsole`

   b. Navigate to Application Server Control:

      `http://`***replica_host***`:`***replica_em_port***

      The `ias_admin` password on the Replica is set to the same value as the `ias_admin` password on the Master.

   c. Use Application Server Control to navigate to the Instance Home Page for the Replica instance.

   d. Verify that Oracle Internet Directory is listed in the System Components section.

5. Remove the `ldaptarget.xml` file; it contains secure information such as the ODS schema password:

   `rm` ***REPLICA_HOME***`/ldap/templates/ldaptarget.xml`

Task 6: Enable SSO, DAS, and DIP on the Replica

In this task, you enable SSO, DAS, and DIP on the Replica.

1. Modify the replication configuration for SSO.

a. Obtain the Replica Repository dn:

```
REPLICA_HOME/bin/ldapsearch -h replica_host -p replica_oid_port -D
cn=orcladmin -w replica_orcladmin_passwd -b "cn=oraclecontext" -s one
"objectclass=orcldbserver" dn
```

This command will return two DNs in the form of:

```
cn=short_gdbname,cn=oraclecontext
```

Find the one that corresponds to the Replica Repository.

Note that if this command returns the error "ldap_search: No such object" you should go back to the previous step and make sure the Replica was started properly.

b. On the Replica host, create a file named `mod.ldif` that contains the following lines:

```
dn:orclreplicaid=replica_replicaid,cn=replication configuration
changetype:modify
replace:seeAlso
seeAlso:replica_repository_dn
```

Where ***replica_repository_dn*** is the Replica Repository dn you obtained in the previous step.

c. Run the following command:

```
REPLICA_HOME/bin/ldapmodify -D cn=orcladmin -w replica_orcladmin_passwd
-p replica_oid_port -v -f mod.ldif
```

2. Edit *REPLICA_HOME*`/config/ias.properties` to reflect the Replica OID server host and port. Change the following lines:

```
OIDhost=replica_host
OIDport=replica_oid_port
OIDsslport=replica_ssl_oid_port
VirtualHostName=replica_host
```

3. Edit *REPLICA_HOME*`/network/admin/ldap.ora` to reflect the Replica OID server host and port. Change the following line:

```
DIRECTORY_SERVERS = (replica_host:replica_oid_port:replica_ssl_oid_port)
```

4. Configure SSO in Oracle Enterprise Manager Application Server Control.

a. Make sure Oracle Enterprise Manager Application Server Control is started:

```
REPLICA_HOME/bin/emctl startifdown iasconsole
```

b. Navagate to Application Server Control:

```
http://replica_host:replica_em_port
```

c. Use Application Server Control to navigate to the Instance Home Page for the Replica instance.

d. On the Instance Home Page, in the System Components section, click **Configure Component**.

e. On the Select Component screen, select **Single Sign-On Server** in the dropdown menu. Click **Continue**.

f. On the Login screen:

- In the User Name field, enter `cn=orcladmin`.
- In the Password field, enter the Replica `cn=orcladmin` password ("`welcome`").

g. Click **Finish**.

h. When the confirmation message appears, click **OK**.

5. Validation Step: If the confirmation message does not appear, or there is an error displayed, there are a few possible reasons. Check the following log files for errors:

```
REPLICA_HOME/sysman/log/emias.log
REPLICA_HOME/sso/log/ssoem.log
REPLICA_HOME/opmn/logs/OC4J~OC4J_SECURITY~default_island~1
```

- If the error messages on the screen or in the log files indicate an LDAP or OID error, check that the Replica OID server is running and that you supplied a valid password for cn=orcladmin. Also check that you updated ias.properties correctly in step 2 and that you configured the OID replica correctly. Then repeat step 4.
- If the error messages in the log files indicate a database error, check that the Replica Repository is running and that you updated the ldap.ora file correctly in step 3. Then repeat step 4.

6. Perform this step **only if your Replica is on an HPUX system**.

a. Edit the following file:

```
REPLICA_HOME/opmn/conf/opmn.xml
```

b. Locate the entry for OC4J_SECURITY.

c. In the environment element, replace LD_LIBRARY_PATH with SHLIB_PATH. For example, change:

```
<process-type id="OC4J_SECURITY" module-id="OC4J">
  <environment>
    <variable id="LD_LIBRARY_PATH" value="/private/oracleas/lib"/>
```

To:

```
<process-type id="OC4J_SECURITY" module-id="OC4J">
  <environment>
    <variable id="SHLIB_PATH" value="/private/oracleas/lib32"/>
```

d. Save and close the file.

e. Run the following command:

```
REPLICA_HOME/dcm/bin/dcmctl updateConfig
```

f. Reload OPMN:

```
REPLICA_HOME/opmn/bin/opmnctl reload
```

7. Register mod_osso.

a. Set environment variables.

- On HPUX systems, make sure the SHLIB_PATH environment variable includes $ORACLE_HOME/lib32
- On all other UNIX systems, make sure the LD_LIBRARY_PATH environment variable includes $ORACLE_HOME/lib

b. Run the following command:

```
REPLICA_HOME/jdk/bin/java -jar REPLICA_HOME/sso/lib/ossoreg.jar
-oracle_home_path REPLICA_HOME
-site_name replica_host
-config_mod_osso TRUE
-mod_osso_url http://replica_host:replica_http_port
-u user
```

Note that *user* is the user that starts Oracle HTTP Server. By default, this is the user that installed Oracle Application Server. If you have changed the

Oracle HTTP Server listen port number to a value < 1024, then this user is root.

8. Configure DAS in Oracle Enterprise Manager Application Server Control.

   a. Navagate to Application Server Control:

      `http://`***`replica_host`***`:`***`replica_em_port`***

   b. Use Application Server Control to navigate to the Instance Home Page for the Replica instance.

   c. On the Instance Home Page, in the System Components section, click **Configure Component**.

   d. On the Select Component screen, select **Delegated Administration Service** in the dropdown menu. Click **Continue**.

   e. On the Login screen:

      – In the User Name field, enter `cn=orcladmin`.

      – In the Password field, enter the Replica `cn=orcladmin` password ("`welcome`").

   f. Click **Finish**.

   g. When the confirmation message appears, click **OK**.

9. Update the DAS URL entry.

   a. On the Replica host, create a file named `mod.ldif` with the following lines:

      ```
      dn:cn=OperationURLs,cn=DAS,cn=Products,cn=OracleContext
      changetype:modify
      replace:orcldasurlbase
      orcldasurlbase:http://replica_host:replica_http_port/
      ```

      Note the slash at the end of the URL.

   b. Run the following command:

      ```
      REPLICA_HOME/bin/ldapmodify -D cn=orcladmin -w replica_orcladmin_passwd
      -p replica_oid_port -v -f mod.ldif
      ```

10. Restart the Replica instance:

    ```
    REPLICA_HOME/opmn/bin/opmnctl stopall
    REPLICA_HOME/opmn/bin/opmnctl startall
    ```

11. Validation Step: Verify that SSO was configured successfully.

Navigate to the following URL and click **Login**:

```
http://replica_host:replica_http_port/pls/orasso
```

Log in as `orcladmin` and use the password you specified during the installation of the Master. If the page does not appear or the login fails, check the following log files:

```
REPLICA_HOME/Apache/Apache/logs/error_log.most_recent_timestamp
REPLICA_HOME/sso/log/ssoServer.log
```

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

12. Validation Step: Verify that DAS was configured successfully.

Using Application Server Control, navigate to the Instance Home Page where DAS is running. Verify that `OC4J_SECURITY` is listed in the System Components section. Verify that the Farm value displayed on the page is the Replica Repository.

Verify DAS is running properly:

a. Log in to DAS using the following URL:

```
http://replica_host:replica_http_port/oiddas
```

b. Click the My Profile tab

c. Make sure the correct login user information is shown on this page

d. Click on the Directory tab

e. Type in a keyword in the "Search for user" field and click the Go button

f. Make sure the correct list of users is shown on the search result table

If these steps fail, turn on DAS debugging mode by setting the DEBUG flag to true in the following file:

```
REPLICA_HOME/ldap/das/das.properties
```

and restart DAS as follows:

```
REPLICA_HOME/opmn/bin/opmnctl stopproc process-type=OC4J_SECURITY
REPLICA_HOME/opmn/bin/opmnctl startproc process-type=OC4J_SECURITY
```

Repeat the steps for verifying DAS is running properly to reproduce the problem. Examine the errors in the DAS log file:

REPLICA_HOME/ldap/log/das.log

13. Migrate the DIP data:

    MASTER_HOME/bin/dipassistant reassociate -src_ldap_host ***master_host*** -src_ldap_port ***master_oid_port*** -dst_ldap_host ***replica_host*** -dst_ldap_port ***replica_oid_port*** -src_ldap_passwd ***master_orcladmin_passwd*** -dst_ldap_passwd ***replica_orcladmin_passwd***

    This command prints log messages to:

    MASTER_HOME/ldap/odi/log/reassociate.log

14. Configure DIP in Oracle Enterprise Manager Application Server Control.

    a. Navagate to Application Server Control:

       http://***replica_host***:***replica_em_port***

    b. Use Application Server Control to navigate to the Instance Home Page for the Replica instance.

    c. On the Instance Home Page, in the System Components section, click **Configure Component**.

    d. On the Select Component screen, select **Directory Integration and Provisioning** in the dropdown menu. Click **Continue**.

    e. On the Login screen:

       – In the User Name field, enter `cn=orcladmin`.

       – In the Password field, enter the Replica `cn=orcladmin` password ("`welcome`").

    f. Click **Finish**.

    g. When the confirmation message appears, click **OK**.

15. Start the DIP server on the Replica:

    REPLICA_HOME/bin/oidctl server=odisrv instance=1 flags='port=***replica_oid_port***' start

16. Validation Step: Verify that DIP was configured successfully.

Navigate to the Directory Integration Page on Application Server Control. The DIP server instance "1" should have a status of "UP", the DIP host should be the Replica host, and the OID node should be the Replica host. If this is not the case, the DIP server was not registered and brought up on the Replica host successfully. To debug this problem, check the DIP server log file:

REPLICA_HOME/ldap/log/odisrv01.log

All provisioning profiles should be getting executed successfully. If any of the profiles show a "Database connection error" in the errors field, then the reassociation of the profiles was not successful. To debug this problem, check the application-specific trace file in this directory:

REPLICA_HOME/ldap/odi/log

The trace file names are of the form *application_name_realm_name*_E.trc or *application_name_realm_name*_E.aud.

You have finished setting up an LDAP-based Replica. You can return the main procedure you are following in either Section 8.4, "Moving Identity Management to a New Host" or Section 8.5, "Changing from a Test to a Production Environment".

F.3 Migrating SSO and DIP Data

This procedure describes how to migrate SSO and DIP data from a source Infrastructure to a target Infrastructure.

- If you are using this procedure in conjunction with Section 8.4, "Moving Identity Management to a New Host", you should migrate the SSO and DIP data from the Master (old host) to the Replica (new host).

  In this case, the Master is the source and the Replica is the target. You can convert the parameters in the procedure as follows:

  - Convert ***SOURCE_param*** to ***MASTER_param***
  - Convert ***TARGET_param*** to ***REPLICA_param***

- If you are using this procedure in conjunction with Section 8.5, "Changing from a Test to a Production Environment", you should migrate the SSO and DIP data from the Replica (Test) to the Master (Production).

  In this case, the Replica is the source and the Master is the target. You can convert the parameters in the procedure as follows:

- Convert ***SOURCE_param*** to ***REPLICA_param***
- Convert ***TARGET_param*** to ***MASTER_param***

Refer to Table F–1 to obtain the values for the various parameters used in this procedure.

This procedure contains the following tasks:

- Task 1: Migrate the SSO Data
- Task 2: Migrate the DIP Data

Task 1: Migrate the SSO Data

1. Obtain the ORASSO schema password on the source:

   ```
   SOURCE_HOME/bin/ldapsearch -p source_oid_port -h source_host -D
   "cn=orcladmin" -w source_orcladmin_password -b "orclresourcename=orasso,
   orclreferencename=source_db_name, cn=ias infrastructure databases, cn=ias,
   cn=products, cn=oraclecontext" -s base "objectclass=*" orclpasswordattribute
   ```

   This command prints the ORASSO password in a line like the following:

   ```
   orclpasswordattribute=LAetjdQ5
   ```

2. Export the SSO data from the source:

   ```
   SOURCE_HOME/sso/bin/ssomig -export -s orasso -p source_orasso_passwd -c
   source_db_name -log_d $SOURCE_HOME/sso/log
   ```

   source_orasso_passwd is the ORASSO password obtained in the previous step.

3. Copy the `ssomig.dmp` and `ssoconf.log` files from the source to the target, preserving the exact full path for each file:

   ```
   cp SOURCE_HOME/sso/log/ssomig.dmp TARGET_HOME/sso/log/ssomig.dmp
   cp SOURCE_HOME/sso/log/ssoconf.log TARGET_HOME/sso/log/ssoconf.log
   ```

4. Obtain the ORASSO schema password on the target:

   ```
   TARGET_HOME/bin/ldapsearch -p target_oid_port -h target_host -D
   "cn=orcladmin" -w target_orcladmin_password -b "orclresourcename=orasso,
   orclreferencename=target_db_name, cn=ias infrastructure databases, cn=ias,
   cn=products, cn=oraclecontext" -s base "objectclass=*" orclpasswordattribute
   ```

5. Import the SSO data to the target:

```
TARGET_HOME/sso/bin/ssomig -import -overwrite -s orasso -p
target_orasso_password -c target_db_name -log_d $TARGET_HOME/sso/log
-discoforce
```

target_orasso_passwd is the ORASSO password obtained in the previous step.

6. Validation Step: Verify that the export and import of SSO succeeded.

   Verify that the SSO migration tool reported success. You can also check the following log files for errors:

   ```
   SOURCE_HOME/sso/log/ssomig.log
   TARGET_HOME/sso/log/ssomig.log
   ```

   See Also: *Oracle Application Server Single Sign-On Administrator's Guide* for information on interpreting messages in the log files

Task 2: Migrate the DIP Data

1. Stop the DIP server on the source:

   ```
   SOURCE_HOME/bin/oidctl server=odisrv instance=1 stop
   ```

2. Migrate the DIP data:

   ```
   SOURCE_HOME/bin/dipassistant reassociate -src_ldap_host source_host
   -src_ldap_port source_oid_port -dst_ldap_host target_host -dst_ldap_port
   target_oid_port -src_ldap_passwd source_orcladmin_passwd -dst_ldap_passwd
   target_orcladmin_passwd
   ```

   This command prints log messages to:

   ```
   SOURCE_HOME/ldap/odi/log/reassociate.log
   ```

3. Register the DIP server on the target:

   ```
   TARGET_HOME/bin/odisrvreg -D "cn=orcladmin" -w target_orcladmin_password -h
   target_host -p target_oid_port
   ```

4. Start the DIP server on the target:

   ```
   TARGET_HOME/bin/oidctl server=odisrv instance=1 flags='port=target_oid_port'
   start
   ```

F.4 Migrating Oracle Internet Directory Data

This section describes how to migrate Oracle Internet Directory data from an Replica (Test) to the Master (Production). This procedure is used in conjunction with the procedure in Section 8.5, "Changing from a Test to a Production Environment".

Refer to Table F–1 to obtain the values for the various parameters used in this procedure.

1. End the Pilot Mode on the Replica.

   a. Obtain the Replica replica ID by running the following command:

      ```
      REPLICA_HOME/bin/ldapsearch -h replica_host -p replica_oid_port -D
      cn=orcladmin -w replica_orcladmin_passwd -b "" -s base "objectclass=*"
      orclreplicaid
      ```

      The replica ID will look something like "`myhost_asdb`".

   b. On the Replica host, create a file named `mod.ldif` that contains the following lines:

      ```
      dn:orclreplicaid=replica_replicaid,cn=replication configuration
      changetype:modify
      replace:orclpilotmode
      orclpilotmode:0
      ```

      Where ***replica_replicaid*** is the Replica replica ID obtained in the previous step.

   c. Run the following command:

      ```
      REPLICA_HOME/bin/ldapmodify -p replica_oid_port -D cn=orcladmin -w
      replica_orcladmin_passwd -v -f mod.ldif
      ```

   d. Restart OID:

      ```
      REPLICA_HOME/opmn/bin/opmnctl stopproc ias-component=OID
      REPLICA_HOME/opmn/bin/opmnctl startproc ias-component=OID
      ```

2. (Optional) Clean up entries in the Replica OID.

   You can clean up (delete) the data that is modified or added on the Test (Replica) OID so that it is not migrated to the Production (Master) OID. This might be a requirement of a middle-tier component or might be desired by the administrator who maintains OID consistency in the Production OID.

To clean up the data, use the `ldapdelete` command-line utility and delete entries that should not be migrated.

> **See Also:** *Oracle Internet Directory Administrator's Guide* for more information on the `ldapdelete` command

3. Quiesce the Distributed Directory Environment.

   It is very important to quiesce the Distributed Directory environment while the data migration from the Replica (Test) to the Master (Production) takes place. This ensures that there are no conflicting updates, and therefore no data loss or corruption.

   However, if you feel the data operated on by middle-tier components is isolated and cannot be modified by any processes in the Master (Production) environment, then it is safe to skip this step and proceed to the next step.

   To quiesce the Distributed Directory Environment:

   a. Make sure all the Replica and Master are up and running.

   b. Change the ldapserver on the Replica (Test) to read-only mode.

      On the Replica host, create a file named `mod.ldif` that contains the following lines:

      ```
      dn:
      changetype:modify
      replace:orclservermode
      orclservermode:r
      ```

      Run the following command:

      ```
      REPLICA_HOME/bin/ldapmodify -p replica_oid_port -D cn=orcladmin -w
      replica_orcladmin_passwd -v -f mod.ldif
      ```

   c. Wait until all the pending changes are applied to both nodes and the nodes are completely in sync. There is no tool to automatically detect this, but you can monitor the replication log files and make sure there are no new changes being processed by any node in the Directory Replication Group (DRG), which ensures that the DRG is in a quiesced state.

4. Make a Backup of the Middle-Tier Data in the Replica (Test)

   Once middle-tier component testing is complete, you must identify the Database Access Descriptor (DAD) that has been modified or added locally at the Replica (Test) directory and move this data to the Master (Production)

directory. This step describes how to back up the data from the Replica into a flat file.

a. Catalog the `modifytimestamp` and `modifiersname` attributes:

```
REPLICA_HOME/ldap/bin/catalog.sh -connect replica_db_name -add -attr
modifytimestamp

REPLICA_HOME/ldap/bin/catalog.sh -connect replica_db_name -add -attr
modifiersname
```

Enter "ODS" when the script requests the OID Database user name.

b. Restart OID:

```
REPLICA_HOME/opmn/bin/opmnctl stopproc ias-component=OID
REPLICA_HOME/opmn/bin/opmnctl startproc ias-component=OID
```

c. Retrieve the Pilot Start Time:

```
REPLICA_HOME/bin/ldapsearch -h replica_host -p replica_oid_port -D
cn=orcladmin -w replica_orcladmin_passwd -b
"orclreplicaid=replica_replicaid,cn=replication configuration" -s base
"objectclass=*" pilotstarttime
```

Where ***replica_replicaid*** is the Replica replica ID you obtained earlier in the procedure.

This command returns something like:

```
orclreplicaid=myhost_asdb,cn=replication configuration
pilotstarttime=20031119120647z
```

d. Perform the following search against the Replica to back up the data (this step creates a file called `migrate.ldif`). Note that the following command should be typed all on one line.

```
REPLICA_HOME/bin/ldapsearch -L -h replica_host -p replica_oid_port
-D cn=orcladmin -w replica_orcladmin_passwd -b ""
-s sub "(&(modifytimestamp >= pilot_start_time)
(!(modifiersname=cn=replicationdn, orclreplicaid=replica_replicaid,
cn=replication configuration)))" \* orclguid > migrate.ldif
```

pilot_start_time is the Pilot Start Time obtained in a previous step.

replica_replicaid is the Replica replica ID obtained at the beginning of this procedure.

5. Migrate OID Data to the Master (Production)

   Run the following command to migrate data to the Master. Make sure you use the `-r` flag. Specify the `migrate.ldif` file created in the previous step.

   ```
   MASTER_HOME/bin/ldapaddmt -h master_host -p master_oid_port -D
   "cn=orcladmin" -w master_orcladmin_passwd -r -f migrate.ldif
   ```

6. Validation Step: Verify that the migration of OID data succeeded.

   Verify that `ldapaddmt` reported success. You can check the `add.log` file for errors, which is created in the directory from which you ran the `ldapaddmt` command.

   If the command succeeded, `add.log` will be empty. If `add.log` contains errors, preserve it by renaming it.

   > **See Also:** *Oracle Internet Directory Administrator's Guide* for information on interpreting messages in log files

   If necessary, repeat steps 4, 5, and 6.

7. Migrate SSO and DIP data from the Replica (Test) to the Master (Production).

   > **See Also:** Section F.3, "Migrating SSO and DIP Data"

8. (Optional) Post-Migration Cleanup Tasks

   Some middle-tier components might have special cleanup requirements after you have changed to the Master (Production). You can perform these cleanup tasks on the Replica (Test) after the middle-tier instances have been changed to the Production Node.

G

Examples of Administrative Changes

This appendix provides examples of administrative changes that can be performed on an Oracle Application Server environment. It is a companion to Part IV, "Backup and Recovery" in this book, and to the Disaster Recovery and Active Failover Cluster sections in *Oracle Application Server 10g High Availability Guide*.

It contains the following topics:

- How to Use This Appendix
- Examples of Administrative Changes (by Component)

G.1 How to Use This Appendix

Some administrative operations cause configuration changes to your Oracle Application Server environment. These are called *administrative changes*, and include deploying and undeploying applications, changing the topology, changing ports, creating and deleting users, and changing passwords. As an administrator, you should be aware when administrative changes occur, because you may need to back up your environment or perform some synchronization procedures.

This appendix provides examples of administrative changes, listed by component. You can use this as a guide for performing the following procedures:

- Backup and Recovery

  Oracle recommends you perform a backup after each administrative change to your environment. You can use this appendix to determine the types of administrative changes that require you to back up your environment.

  See Also: Part IV, "Backup and Recovery"

- Disaster Recovery Synchronization Between the Primary and Standby Sites

  When you implement Disaster Recovery, you must update standby sites when you make an administrative change to your environment. You can use this appendix to determine the types of administrative changes that require you to update your standby sites.

  See Also: *Oracle Application Server 10g High Availability Guide*

- Active Failover Cluster (AFC) Infrastructure File Synchronization Between Different Nodes of the Hardware Cluster

  If you use Active Failover Cluster, you must keep the files in the different nodes in the AFC in sync. You can use this appendix to determine the types of administrative changes that require to you to synchronize your AFC nodes.

  See Also: *Oracle Application Server 10g High Availability Guide*

G.2 Examples of Administrative Changes (by Component)

Table G–1 provides examples of administrative changes, by component. Consult your component documentation to learn more about these operations.

Table G–1 Examples of Administrative Changes

Component	Examples of Administrative Changes
Delegated Administration Services (DAS)	Manual edits to DAS configuration files, such as `das.properties`
Directory Integration and Provisioning (DIP)	DIP administrative and configuration operations, such as running the `odisrvreg` or `remtool` utilities (password management)
Distributed Configuration Management (DCM)	DCM administrative and configuration operations performed using Application Server Control
	Manual edits to DCM configuration files
	DCM administrative and configuration operations using `dcmctl`, such as `configrepositoryssl`, `joincluster`, `joinfarm`, `leavecluster`, `leavefarm`, `repositoryrelocated`, `resetDCMcacheport`, `resethostinformation`, `restoreinstance`, and `set` operations
	DCM administrative and configuration operations performed using the `dcmctl` utility, such as deploying and undeploying applications and making configuration changes
Dynamic Monitoring Service (DMS)	DMS administrative and configuration operations performed using Application Server Control
	Manual edits to DMS configuration files, such as `dms.conf`
Log Loader	Log Loader administrative and configuration operations performed using Application Server Control
	Manual edits to Log Loader configuration files, such as `loglоader.properties`, `logloader.xml`, and files in *`ORACLE_HOME`*`/diagnostics/config/registration`
Oracle Application Server Containers for J2EE (OC4J)	OC4J administrative and configuration operations performed using Application Server Control
	Manual edits to OC4J configuration files
	OC4J administrative and configuration operations using the `dcmctl` utility, such as deploying and undeploying applications, and creating OC4J instances

Table G–1 (Cont.) Examples of Administrative Changes

Component	Examples of Administrative Changes
Oracle Application Server Java Authentication and Authorization Service (JAZN)	JAZN administrative and configuration operations performed using Application Server Control
	JAZN administrative and configuration operations performed using the `admintool` utility, such as adding and removing users, and changing roles, permissions, privileges, and passwords
Oracle Enterprise Manager Application Server Control	Application server-wide or component-specific administrative and configuration operations performed using Application Server Control, such as changing the `ias_admin` password, changing port numbers, deploying and undeploying applications, and operations that result in configuration file changes
Oracle HTTP Server	Oracle HTTP Server administrative and configuration operations performed using Application Server Control, such as modifying the number of VMs and creating virtual hosts
	Manual edits to Oracle HTTP Server configuration files
	Oracle HTTP Server administrative and configuration operations using the `dcmctl` utility
Oracle Internet Directory (OID)	Oracle Internet Directory administrative and configuration operations, such as running the `oidpasswd` or `remtool` utilities (password management), and installing and removing components
Oracle Process Manager and Notification Server (OPMN)	OPMN administrative and configuration operations performed using Application Server Control
	Manual edits to OPMN configuration files, such as `opmn.xml`
	OPMN administrative and configuration operations using the `dcmctl` utility
Oracle Ultra Search	Manual edits to Oracle Ultra Search configuration files, such as `crawler.dat`, `data-sources.xml`, `truststore.dat`, and `ultrasearch.properties`
OracleAS Certificate Authority (OCA)	OCA administrative and configuration operations using the `ocactl` utility with the following options: `setpasswd`, `generatewallet`, `convertwallet`, `importwallet`, `revokecert`, `renewcert`, `updateconnection`, and `changesecurity`
	Using the administrative interface to enroll the OCA Web administrator
OracleAS Forms Services	OracleAS Forms Services administrative and configuration operations performed using Application Server Control, such as operations on the "Forms / Configuration", "Forms / Environment Property", and "Forms / Overview" pages

Table G–1 (Cont.) Examples of Administrative Changes

Component	Examples of Administrative Changes
OracleAS Portal	OracleAS Portal administrative and configuration operations performed using Application Server Control
	OracleAS Portal administrative and configuration operations using the Administration screen in the Portal User Interface
	Manual edits to OracleAS Portal configuration files
	Running the `ptlconfig` script
	Running any Portal-specific scripts that modify the database-side configuration for Portal, for example, disabling OracleAS Web Cache or changing some background job frequencies in Portal
OracleAS ProcessConnect	OracleAS ProcessConnect administrative and configuration operations performed using Application Server Control
OracleAS Reports Services	OracleAS Reports Services administrative and configuration operations performed using Application Server Control, such as operations on the "Reports / Configuration" page
	Manual edits to OracleAS Reports Services configuration files
	When the Reports server receives a job insert or update, such as when adding a new job or moving a job from one queue to another. *Note: Oracle recommends that you perform backup and file synchronization more frequently when running OracleAS Reports Services.*
OracleAS Single Sign-On (SSO)	SSO administrative and configuration operations performed using Application Server Control, such as changing the `ORASSO` schema password
	Configuration changes such as adding or removing an SSO middle-tier instance, changing SSO to use SSL, and performing Windows Native Authentication configuration changes
OracleAS Web Cache	OracleAS Web Cache administrative and configuration operations performed using Web Cache Manager, such as changes in the following areas: "Operations", "Properties", "Logging and Diagnostics", "Ports", "Origin Servers, Sites, and Load Balancing", and "Rules and Rule Association"
	Manual edits to OracleAS Web Cache configuration files, such as `webcache.xml`
	Other administrative or configuration operations, such as deploying new Web servers into the farm, changing port numbers, performing security changes, and deploying or undeploying an application or site

Table G–1 (Cont.) Examples of Administrative Changes

Component	Examples of Administrative Changes
OracleAS Wireless	OracleAS Wireless administrative and configuration operations performed using Application Server Control, such as deploying and undeploying applications, changing ports, making changes to groups or users, and changing configuration parameters

H

Viewing Oracle Application Server Release Numbers

This appendix describes how to view Oracle Application Server release numbers.

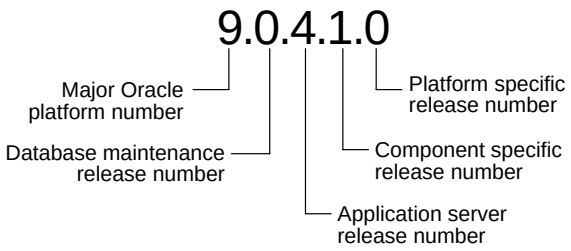
It contains the following topics:

> **Note:** Oracle recommends you keep a log of all one-off patches applied to your Oracle Application Server installations.

H.1 Release Number Format

To understand the release level nomenclature used by Oracle, examine the example of an Oracle release number shown in Figure H–1.

Figure H–1 Example of an Oracle Release Number



Major Oracle Platform Number

This is the most general identifier. It represents a major new edition (or version) of the Oracle database server, Oracle Application Server, or Oracle9*i*DS, and indicates that the release contains significant new functionality.

Database Maintenance Release Number

This digit represents a maintenance release level. Some new features may also be included.

Application Server Release Number

This digit reflects the release level of Oracle Application Server.

Component Specific Release Number

This digit identifies a release level specific to a component. Different components can have different numbers in this position depending upon, for example, component patch sets or interim releases.

Platform Specific Release Number

This digit identifies a platform specific release.

H.2 Viewing Oracle Application Server Installation Release Numbers

All Oracle Application Server installations have a release number. This number is updated when you apply a patch set release or upgrade the installation.

You can view the release number of an Oracle Application Server installation using Oracle Universal Installer, as follows:

1. Launch Oracle Universal Installer:

   ```
   ORACLE_HOME/oui/bin/runInstaller.sh
   ```

2. Click **Installed Products** to open the Inventory Page.
3. In the Inventory Page, expand **Oracle Homes**. You will see entries for all installations on your host.
4. Expand the Oracle Home entry for the installation you are interested in.
5. You will see an entry with the release number for your original installation, followed by entries for any patch sets that have been applied.

H.3 Viewing Component Release Numbers

All Oracle Application Server components have a release number and many contain services that have release numbers. These numbers *may* be updated when you apply a patch set release or upgrade the installation.

You can view the release number of components and their services in the following ways:

- On the Filesystem
- Using Oracle Universal Installer

On the Filesystem

You can view component release numbers as follows:

```
cd ORACLE_HOME/inventory
ls -d Components*/*/*
```

Using Oracle Universal Installer

If you installed Oracle Application Server using Oracle Universal Installer, you can view component release numbers as follows:

1. Launch Oracle Universal Installer:

ORACLE_HOME/oui/bin/runInstaller.sh

2. Click **Installed Products** to open the Inventory Page.
3. In the Inventory Page, expand **Oracle Homes**. You will see entries for all installations on your host.
4. Expand the Oracle Home entry for the installation you are interested in.
5. You will see an entry with the release number for your original installation, followed by entries for any patch sets that have been applied.
6. Expand the initial entry to view the component release numbers at installation time. If you have subsequent patch set entries, expand them to see the component release numbers updated for each patch set.

H.4 Viewing Oracle Internet Directory Release Numbers

Oracle Internet Directory has a server release number, which is the version of the binaries. It also has schema and context versions. All of these numbers correspond to the Oracle Application Server installation release number up through the third digit. These numbers *may* be updated when you apply a patch set release or upgrade the installation.

Viewing the Oracle Internet Directory Server Release Number

The Oracle Internet Directory server release number is the version of the binaries. You can view the Oracle Internet Directory server release number as follows:

1. Make sure the ORACLE_HOME environment variable is set.
2. Run the following command:

   ORACLE_HOME/bin/oidldapd -version

Viewing the Oracle Internet Directory Schema and Context Versions

You can view the Oracle Internet Directory schema and context versions in this file:

ORACLE_HOME/ldap/schema/versions.txt

The contents of this file are kept up-to-date, however, you can also query the schema and context release from Oracle Internet Directory, just to be sure.

To view the schema version:

1. Make sure the ORACLE_HOME environment variable is set.

2. Run the following command:

```
ORACLE_HOME/bin/ldapsearch -h oid_host -p oid_port -D "cn=orcladmin" -w
orcladmin_password -b "cn=base,cn=oracleschemaversion" -s base
"objectclass=*" orclproductversion
```

The output will be in this form:

```
cn=BASE,cn=OracleSchemaVersion
orclproductversion=90400
```

To view the context version:

1. Make sure the ORACLE_HOME environment variable is set.
2. Run the following command:

```
ORACLE_HOME/bin/ldapsearch -h oid_host -p oid_port -D "cn=orcladmin" -w
orcladmin_password -b "cn=oraclecontext" -s base "objectclass=*" orclversion
```

The output will be in this form:

```
cn=oraclecontext
orclversion=90400
```

H.5 Viewing Metadata Repository Release Numbers

Metadata Repositories have the following release numbers:

- Database release number

  This is the Oracle9*i* database release number.

- Metadata Repository Container release number

  This is the release number for the Metadata Repository—this number is equal to the Oracle Application Server installation release number.

- Schema release numbers

  The Oracle Application Server schemas in the Metadata Repository have release numbers. These numbers do not necessarily correspond to Oracle Application Server release numbers or database release numbers.

Viewing the Database Release Number

The Metadata Repository is an Oracle9*i* database that has a release number. This number is updated when you apply a patch set release or upgrade the database.

You can view the Metadata Repository release number using SQL*Plus as follows (you can be connected to the database as any user to issue these commands):

```
SQL> COL PRODUCT FORMAT A35
SQL> COL VERSION FORMAT A15
SQL> COL STATUS FORMAT A15
SQL> SELECT * FROM PRODUCT_COMPONENT_VERSION;

PRODUCT                             VERSION         STATUS
----------------------------------------------------- ----------------
NLSRTL                              9.0.1.5.0       Production
Oracle9i Enterprise Edition         9.0.1.5.0       Production
PL/SQL                              9.0.1.5.0       Production
TNS for Solaris:                    9.0.1.4.0       Production
```

Viewing Metadata Repository Container and Schema Release Numbers

You can view the Metadata Repository Container release number, as well as schema release numbers, using SQL*Plus as follows (you must log in as a user with SYSDBA privileges):

```
SQL> COL COMPONENT_NAME FORMAT A35
SQL> COL ID FORMAT A15
SQL> COL VERSION FORMAT A15
SQL> SELECT * FROM IAS_VERSIONS;

COMPONENT_NAME                      ID              VERSION
----------------------------------------------------- ----------------
Metadata Repository Container       mrc             9.0.4.0.0
Oracle Ultrasearch                  ultrasearch     9.0.4
Oracl9i Workflow                    workflow        2.6.3
```

`IAS_VERSIONS` is a public synonym to a view owned by the `INTERNET_APPSERVER_REGISTRY` user. If the above query returns an error, it may be because:

- There was an error in seeding one or more components
- Not all of the components whose underlying tables are read by the view are present in the database

Either case indicates that the database is not properly seeded to be a Metadata Repository.

To get the same result by querying the underlying table:

```
SQL> SELECT * FRIM INTERNET_APPSERVER_REGISTRY.SCHEMA_VERSIONS;
```

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W