

Oracle® Application Server

Quick Administration Guide

10g Release 2 (10.1.2)

B14126-02

July 2005

Oracle Application Server Quick Administration Guide, 10g Release 2 (10.1.2)

B14126-02

Copyright © 2003, 2005, Oracle. All rights reserved.

Primary Author: Helen Grembowicz

Contributing Authors: Mary Beth Roeser, Pavana Jain, Lypp-Tek Khoo-Ellis, Peter LaQuerre, Theresa Bandy, Andrew Salt, Thomas Van Raalte, Pavi Sandhu

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documentation	viii
Conventions	viii
1 Getting Started After Installing Oracle Application Server	
1.1 Setting Environment Variables	1-1
1.2 Using the Oracle Application Server Welcome Page	1-3
1.3 Checking Your Port Numbers	1-3
1.4 Getting Started with Managing Components	1-5
1.4.1 Common Components	1-5
1.4.2 Optional Components	1-6
1.5 Changing the ias_admin Password	1-7
1.5.1 Using the Application Server Control Console	1-7
1.5.2 Using the emctl Command-line Tool	1-7
2 Using the Administration Tools	
2.1 Understanding Oracle Enterprise Manager 10g	2-1
2.1.1 Oracle Enterprise Manager 10g Application Server Control	2-1
2.1.2 Oracle Enterprise Manager 10g Grid Control	2-3
2.2 Understanding Command-line Tools	2-3
2.3 Understanding the Application Server Control Console	2-4
2.3.1 Displaying the Application Server Control Console	2-5
2.3.2 Using the Application Server Home Page	2-6
2.3.3 Using the Oracle Application Server Farm Home Page	2-7
2.3.4 Using an Oracle Application Server Component Home Page	2-8
2.3.5 Monitoring and Diagnosing with the Application Server Control Console	2-8
2.4 Managing the OracleAS Metadata Repository Database with Database Control	2-11
3 Starting and Stopping	
3.1 Starting and Stopping Application Server Instances	3-1
3.1.1 Starting an Application Server Instance	3-1
3.1.2 Stopping an Application Server Instance	3-2
3.1.3 Starting OracleAS Infrastructure	3-3

3.1.4	Stopping OracleAS Infrastructure.....	3-3
3.1.5	Starting a Middle-Tier Instance	3-3
3.1.6	Stopping a Middle-Tier Instance	3-4
3.2	Starting and Stopping Components.....	3-4
3.2.1	Starting and Stopping Using opmnctl	3-5
3.2.2	Starting and Stopping Using the Application Server Control Console	3-5
3.3	Enabling and Disabling Components	3-5
3.4	Starting and Stopping an Oracle Application Server Environment.....	3-6
3.4.1	Starting an Oracle Application Server Environment.....	3-6
3.4.2	Stopping an Oracle Application Server Environment.....	3-6

4 Changing the HTTP Listener Ports

4.1	Changing the HTTP Server Listen Port on Middle-Tier Instances.....	4-1
4.1.1	Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024.....	4-1
4.1.2	Using the portconfig Command to Change the Oracle HTTP Server Listen Port	4-2
4.2	Changing the HTTP Server Listen Port on Identity Management Installations.....	4-5

5 Viewing and Managing Log Files

5.1	Introducing Oracle Application Server Logging.....	5-1
5.1.1	Understanding Log File Data and Naming	5-1
5.1.2	Using a Log Repository.....	5-3
5.1.3	Configuring Component Logging Options	5-3
5.2	Listing and Viewing Log Files With Enterprise Manager	5-3
5.2.1	Listing Log Files	5-4
5.2.2	Listing Log Files for Selected Components.....	5-4
5.2.3	Listing Log Files from Oracle Application Server Components Pages	5-5
5.2.4	Using Log Files Advanced Search.....	5-5
5.2.5	Viewing Log File Details and Log File Contents.....	5-5
5.3	Using Oracle Application Server Log Loader.....	5-6
5.3.1	Starting and Stopping Log Loader	5-6
5.3.2	Enabling and Disabling Log Loader	5-7
5.3.3	Updating the Log Configuration.....	5-7
5.3.4	Setting Log Loader Properties	5-7
5.3.5	Understanding Log Loader Diagnostic Messages	5-8

6 Changing Network Configurations

6.1	Overview of Procedures for Changing Network Configurations	6-1
6.2	Changing Your Hostname, Domain Name, or IP Address	6-1
6.2.1	Changing the Hostname or Domain Name of a Middle-Tier Installation	6-2
6.2.2	Changing the IP Address of an Infrastructure Containing a Metadata Repository ..	6-8
6.2.3	Special Topics for Changing Your Hostname or Domain Name.....	6-11
6.3	Moving Between Off-Network and On-Network.....	6-13
6.3.1	Moving from Off-Network to On-Network (Static IP Address).....	6-13
6.3.2	Moving from Off-Network to On-Network (DHCP)	6-13
6.3.3	Moving from On-Network to Off-Network (Static IP Address).....	6-13
6.3.4	Moving from On-Network to Off-Network (DHCP)	6-14

6.4	Changing Between a Static IP Address and DHCP	6-14
6.4.1	Changing from a Static IP Address to DHCP	6-14
6.4.2	Changing from DHCP to a Static IP Address.....	6-14
7	Enabling SSL	
7.1	Overview of SSL.....	7-1
7.2	Using the SSL Configuration Tool.....	7-1
7.2.1	Command Line Interface	7-2
7.3	SSL Communication Paths in the Infrastructure.....	7-3
7.4	Common SSL Configuration Tasks for the Infrastructure.....	7-5
7.4.1	Configuring SSL for OracleAS Single Sign-On and Oracle Delegated Administration Services.....	7-6
7.4.2	Configuring SSL for Oracle Internet Directory	7-6
7.4.3	Configuring SSL for Oracle Internet Directory Replication Server and Oracle Directory Integration and Provisioning	7-6
7.4.4	Configuring SSL in the Identity Management Database	7-6
7.5	SSL Communication Paths in the Middle Tier	7-6
7.6	Common SSL Configuration Tasks for the Middle Tier	7-8
7.6.1	Enabling SSL in OracleAS Web Cache	7-8
7.6.2	Enabling SSL in the Oracle HTTP Server	7-8
7.6.3	Enabling SSL in Oracle Application Server Containers for J2EE (OC4J).....	7-8
7.6.4	Enabling SSL in J2EE and Web Cache Installations.....	7-9
7.6.5	Enabling SSL in Virtual Hosts.....	7-9
7.6.6	Enabling SSL in OracleBI Discoverer.....	7-9
7.6.7	Enabling SSL in OracleAS Wireless	7-9
7.6.8	Enabling SSL in OracleAS Portal.....	7-10
7.6.9	Configuring SSL for Oracle Enterprise Manager 10g.....	7-11
8	Cloning an Application Server Instance	
8.1	Introduction to Cloning	8-1
8.1.1	Installation Types Supported.....	8-1
8.1.2	General Considerations and Limitations for Cloning.....	8-2
8.2	Procedure for Cloning.....	8-3
8.2.1	Prerequisites for Cloning.....	8-3
8.2.2	Preparing the Source	8-3
8.2.3	Cloning the Instance.....	8-5
8.2.4	Locating and Viewing Log Files.....	8-7
9	Backup and Recovery	
9.1	Locating the OracleAS Backup and Recovery Tool	9-1
9.1.1	Manually Installing the OracleAS Backup and Recovery Tool	9-2
9.2	Configuring the OracleAS Backup and Recovery Tool.....	9-3
9.3	Customizing the Tool for Your Configuration Files.....	9-5
9.4	OracleAS Backup and Recovery Tool Usage Summary.....	9-6
9.4.1	Prerequisites for Running the Tool	9-6
9.4.2	Syntax	9-6

9.4.3	Usage Examples	9-12
9.5	Backup Procedures	9-14
9.5.1	Enabling Block Change Tracking	9-14
9.5.2	Enabling ARCHIVELOG Mode	9-14
9.5.3	Creating a Record of Your Oracle Application Server Configuration	9-16
9.5.4	Performing a Complete Oracle Application Server Environment Backup	9-17
9.5.5	Performing a Configuration and Metadata Backup	9-21

A OPMN Commands

B DCM Commands

C Metadata Repository Schemas

C.1	Metadata Repository Schema Descriptions	C-1
C.1.1	Identity Management Schemas.....	C-1
C.1.2	Product Metadata Schemas	C-2
C.1.3	Management Schemas.....	C-3
C.2	Metadata Repository Schemas, Tablespaces, and Default Datafiles	C-3

Index

Preface

This guide describes some of the more common administrative tasks for Oracle Application Server.

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documentation](#)
- [Conventions](#)

Audience

This 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. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documentation

For more information, refer to these Oracle resources:

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

Conventions

The following text conventions are used in this document:

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

Getting Started After Installing Oracle Application Server

This chapter describes the tasks that you need to perform after installing Oracle Application Server. It contains the following topics:

- [Setting Environment Variables](#)
- [Using the Oracle Application Server Welcome Page](#)
- [Checking Your Port Numbers](#)
- [Getting Started with Managing Components](#)
- [Changing the ias_admin Password](#)

1.1 Setting Environment Variables

Log in as the user who installed Oracle Application Server. To use Oracle Application Server, you should set environment variables, as shown in the following tables:

- [Table 1-1, "Oracle Application Server Environment Variables for UNIX"](#)
- [Table 1-2, "Oracle Application Server Environment Variables for Windows"](#)

Table 1-1 Oracle Application Server Environment Variables for UNIX

Environment Variable	Value
DISPLAY	<i>hostname:display_number.screen_number</i> Beginning with Oracle Application Server 10g, very few tools require the DISPLAY variable. Only a few tools, such as oidadmin, require it.
LD_LIBRARY_PATH	On Solaris, ensure this contains the following directory: \$ORACLE_HOME/lib32 On HP-UX, ensure this contains the following directory: \$ORACLE_HOME/lib On IBM AIX, ensure this environment variable is unset.
(Solaris only) LD_LIBRARY_PATH_64	Ensure this contains the following directory: \$ORACLE_HOME/lib
(HP-UX only) SHLIB_PATH	Ensure this contains the following directory: \$ORACLE_HOME/lib32

Table 1–1 (Cont.) Oracle Application Server Environment Variables for UNIX

Environment Variable	Value
(IBM AIX only) LIBPATH	If the calling application is a 32-bit application, then ensure this contains the following directory: \$ORACLE_HOME/lib32 If the calling application is a 64-bit application, then ensure 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 OracleAS Metadata Repository SID you supplied during installation. The default is <code>orcl</code> .
PATH	Ensure 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.

Table 1–2 Oracle Application Server Environment Variables for Windows

Environment Variable	Value
ORACLE_HOME	Set to the full path of the installation's Oracle home. This is automatically set by Oracle Universal Installer.
ORACLE_SID (Infrastructure installations only)	Set to the OracleAS Metadata Repository SID you supplied during installation. The default is <code>orcl</code> . This is automatically set by Oracle Universal Installer.
TEMP	Set to your temp directory, for example, <code>C:\temp</code> .
TMP	Set to your temp directory, for example, <code>C:\temp</code> .

Best Practices for Multiple Installations on a UNIX Host

Some Oracle Application Server commands use the `ORACLE_HOME` environment variable to determine which installation to operate on, whereas others use the directory location of the command. Therefore, it is not sufficient to simply reset your environment variables or `cd` into a different Oracle home to move between installations. If you want to use an installation made by a different user, then you must log in as that user and then set the environment variables, as described in [Table 1–1](#).

Note: You can also use the `su -` command to switch to the user. For example, `su - username`.

If you have installed multiple installations as the same user, then ensure that you are in the correct Oracle home and have set the correct environment variables when working on a particular installation.

1.2 Using the Oracle Application Server Welcome Page

The Oracle Application Server Welcome page is a quick access point to manage your application server as shown in [Figure 1-1](#).

Figure 1-1 Oracle Application Server Welcome Page

Oracle Application Server

Welcome | What's Next | Demonstrations

Welcome
to Oracle Application Server 10g Release 2 (10.1.2)

Overview

Oracle Application Server 10g Release 2 (10.1.2) is an integrated, standards-based application platform suite that allows organizations of all sizes to respond better to changing business requirements.

The Oracle Application Server application platform suite can improve your organization's ability to predict and respond to market dynamics, enhance productivity, and simplify your information technology environment, all while allowing you to use your existing investments to their full potential. Oracle Application Server 10g Release 2 (10.1.2) achieves these goals through:

- **Service-Oriented Computing:** Oracle Application Server uses a service-oriented computing architecture to facilitate the development of enterprise applications as business services, which enables you to build a flexible enterprise application infrastructure.
- **Grid Computing:** The Oracle Application Server architecture coordinates the use of large numbers of low

Release Notes
Read the latest Release Notes on Oracle Technology Network for important information about Oracle Application Server 10g Release 2 (10.1.2).

New Features
For details about new features for Oracle Application Server 10g Release 2 (10.1.2), visit [Oracle Technology Network](#).

Oracle Application Server Logins
To manage and monitor Oracle Application Server, [log on to Oracle Enterprise Manager 10g Application Server Control](#):
username: ias_admin
password: specified during install

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

```
(UNIX) ORACLE_HOME/install/setupinfo.txt
(Windows) ORACLE_HOME\install\setupinfo.txt
```

If you cannot access the Welcome page, then perform the following steps:

1. Check `setupinfo.txt` to ensure you are using the correct URL.
2. Restart Oracle HTTP Server by using the following commands:

```
opmnctl stopproc ias-component=HTTP_Server
opmnctl startproc ias-component=HTTP_Server
```

3. If OracleAS Web Cache is configured, then restart it using the following commands:

```
opmnctl stopproc ias-component=WebCache
opmnctl startproc ias-component=WebCache
```

1.3 Checking Your Port Numbers

During installation, Oracle Application Server assigns port numbers to various components and services. Check these port numbers to manage your application

server and to ensure that a port number assignment doesn't conflict with a non-Oracle Application Server process.

See Also: [Chapter 4, "Changing the HTTP Listener Ports"](#) for information about changing port numbers

Every component and service has an allotted port range. Oracle Application Server first checks the lowest port number in the port range for a component.

You can find the complete list of port numbers in the `ORACLE_HOME/install/portlist.ini` file. The following example displays a sample copy of the `portlist.ini` file. Another file that displays two important ports, the Application Server Control Console port and the HTTP Server port is the `ORACLE_HOME/Oracle/Http/Http/setinfo.txt` file.

```
;OracleAS Components reserve the following ports at install time.
;As a postinstallation 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 = 8250
Oracle HTTP Server Diagnostic port = 7200
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 Discovery port = 7101
Application Server Control port = 1156
Enterprise Manager Agent port = 1830
Web Cache HTTP Listen port = 7777
Web Cache HTTP Listen (SSL) port = 8250
Web Cache Administration port = 9400
Web Cache Invalidation port = 9401
Web Cache Statistics port = 9402
```

The `portlist.ini` file contains port numbers for components that are not installed, 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.

Note: The `portlist.ini` file is not updated if you modify port numbers after installation. After you start managing the application server, use the Application Server Control Console Ports page for viewing port numbers, because it displays the current port numbers. View the Ports page by clicking the ports link on the Application Server Home page. It also contains links to pages that allow you to change port numbers.

1.4 Getting Started with Managing Components

This section provides an introduction to managing components. It includes instructions for accessing component administration tools and post-installation notes about components. Components are installed according to the topology selected.

See Also: *Oracle Application Server Installation Guide*

1.4.1 Common Components

Some components are installed by default for every installation. These include the following:

- [Oracle Process Manager and Notification Server \(OPMN\)](#)
- [Distributed Configuration Management \(DCM\)](#)
- [Oracle HTTP Server](#)
- [Oracle Application Server Containers for J2EE \(OC4J\)](#)

1.4.1.1 Oracle Process Manager and Notification Server (OPMN)

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. Use OPMN to start and stop your application server, monitor components, and configure event scripts.

See Also:

- *Oracle Process Manager and Notification Server Administrator's Guide*
- [Appendix A, "OPMN Commands"](#)

1.4.1.2 Distributed Configuration Management (DCM)

With DCM, you can 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 (JAAS) Provider (JAZN), and OPMN. You can use DCM to save and restore configuration information, deploy applications, and manage clusters.

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 DCM schema in OracleAS Metadata Repository. It is used by Portal and Wireless, and Business Intelligence and Forms installations.
- **File Based:** This repository is stored in the file system of your Oracle home.

J2EE and Web Cache installations use the database repository if you choose Managed OracleAS Clusters during installation. If you chose File-based clusters, then installations use the file-based repository.

During installation, DCM creates a copy of your initial configuration. If you wish to return to the initial configuration, you can use the `dcmctl restoreInstance` command.

See Also:

- *Distributed Configuration Management Administrator's Guide*
- [Appendix B, "DCM Commands"](#)

1.4.1.3 Oracle HTTP Server

Oracle HTTP Server is installed and configured with every middle-tier and Infrastructure installation. You can access Oracle HTTP Server at `http://hostname.domain:port`, where `port` is the Oracle HTTP Server Listener port number in the `portlist.ini` file.

1.4.1.4 Oracle Application Server Containers for J2EE (OC4J)

OC4J is a complete J2EE environment. When you install OC4J, at least one OC4J instance, called `home`, is installed. Depending on the configuration, additional OC4J instances may also be installed.

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

1.4.2 Optional Components

Depending on the installation type you have chosen, some components may be installed. [Table 1–3](#) describes how to access each component.

Table 1–3 Accessing Optional Components

Component	URL
OracleAS Web Cache	<code>http://hostname.domain:port</code> Log in as <code>ias_admin</code> or <code>administrator</code> .
OracleAS Portal	<code>http://hostname.domain:port/pls/portal</code> Log in as <code>portal</code> using the <code>ias_admin</code> password you supplied during installation.
OracleAS Wireless	<code>http://hostname.domain:port/webtool/login.uix</code> Log in as <code>orcladmin</code> .
OracleBI Discoverer	Discoverer Viewer: <code>http://hostname.domain:port/discoverer/viewer</code> Discoverer Plus: <code>http://hostname.domain:port/discoverer/plus</code> Discoverer Portlet Provider: <code>http://hostname.domain:port/discoverer/portletprovider</code>
Oracle Internet Directory Manager	On UNIX, use the following command: <code>\$ORACLE_HOME/bin/oidadmin</code> — On Windows, select Start, Programs, Oracle - Oracle_Home, Integrated Management Tools, Oracle Directory Manager .
OracleAS Single Sign-On Administration pages	<code>http://host:7777/pls/orasso</code> Log in as <code>orcladmin</code> using the <code>ias_admin</code> password supplied during installation.
OracleAS Certificate Authority Administration Interface	<code>http://host:4400/oca/admin</code> Log in as OracleAS Certificate Authority Administrator using the password supplied during installation.
OracleAS Forms Services	<code>http://hostname.domain:port/forms/frmservlet</code> Log in as <code>portal</code> using the <code>ias_admin</code> password you supplied during installation.
OracleAS Reports Services	<code>http://hostname.domain:port/reports/rwservlet/getserverinfo</code> Log in as <code>orcladmin</code> with the <code>orcladmin</code> password.

1.5 Changing the ias_admin Password

Use the `ias_admin` password to log in to the Oracle Application Server Control Console. You can change the `ias_admin` user password in the following ways:

- [Using the Application Server Control Console](#)
- [Using the emctl Command-line Tool](#)

Caution: If you use Infrastructure Services, then you must adhere to the Oracle Internet Directory password policy when setting the `ias_admin` password. For more information, refer to the *Oracle Internet Directory Administrator's Guide*

1.5.1 Using the Application Server Control Console

To change the `ias_admin` user password:

1. Navigate to the Application Server home page and select **Preferences**. Then, click **Change Password**. The Change Password page is displayed.
2. Change the password, and click **OK** to reset the password for the current instance.

1.5.2 Using the emctl Command-line Tool

To change the `ias_admin` user password:

1. Enter the following command in the Oracle home of your Oracle Application Server installation:

```
(UNIX) ORACLE_HOME/bin/emctl set password old_password new_password
(Windows) ORACLE_HOME\bin\emctl set password old_password new_password
```

2. Restart the Oracle Application Server Control Console.

```
(UNIX) ORACLE_HOME/bin/emctl stop iasconsole
(UNIX) ORACLE_HOME/bin/emctl start iasconsole
```

```
(Windows) ORACLE_HOME\bin\emctl stop iasconsole
(Windows) ORACLE_HOME\bin\emctl start iasconsole
```

Using the Administration Tools

This chapter describes the Oracle Application Server administration tools for managing Oracle Application Server. It contains the following topics:

- [Understanding Oracle Enterprise Manager 10g](#)
- [Understanding Command-line Tools](#)
- [Understanding the Application Server Control Console](#)
- [Managing the OracleAS Metadata Repository Database with Database Control](#)

2.1 Understanding Oracle Enterprise Manager 10g

The primary tool for managing Oracle Application Server, as well as your entire Oracle environment, is Oracle Enterprise Manager 10g (Enterprise Manager).

Enterprise Manager has two main components:

- [Oracle Enterprise Manager 10g Application Server Control](#)
You can manage individual Oracle Application Server instances with Oracle Enterprise Manager 10g Application Server Control.
- [Oracle Enterprise Manager 10g Grid Control](#)
You can centrally manage all the components of your network and your enterprise with Oracle Enterprise Manager 10g Grid Control .

When used together, Application Server Control and Grid Control provide a complete set of efficient tools to reduce the cost and complexity of managing your enterprise.

Note: If you select the OracleAS Metadata Repository-only installation type, the Application Server Control is installed, but not configured. This installation type does not need the Application Server Control Console.

See [Section 2.4, "Managing the OracleAS Metadata Repository Database with Database Control"](#) for more information about managing OracleAS Metadata Repository.

2.1.1 Oracle Enterprise Manager 10g Application Server Control

Application Server Control is installed with every instance of Oracle Application Server and you can manage your application server and its components from your Web browser.

The Application Server Control consists of:

- [The Application Server Control Console](#)
- [The Underlying Software Technologies](#)

2.1.1.1 The Application Server Control Console

Application Server Control Console organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for each application server component. You can monitor and administer a single Oracle Application Server instance, a farm of application server instances, or OracleAS Cluster.

The Web-based home pages, called the **Enterprise Manager home pages**, help you to locate commonly used administrative functions, using your Web browser. Enterprise Manager home pages provide you with a high-level view of your Oracle Application Server environment.

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 may want to manage Oracle Application Server from different levels of detail.

For example, you may want to manage a single application server instance or you may find it efficient to combine multiple instances into an OracleAS Cluster. At other times, you will want to manage a specific application server component.

To support these multiple levels of management, use the 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. Enterprise Manager home pages also provide tools for configuring your Oracle Application Server components.

The following home pages are available when you use the Application Server Control Console:

- Use the OracleAS Farm 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. See [Section 2.3.3, "Using the Oracle Application Server Farm Home Page"](#) for more information.
- Use the Application Server Home page to manage all aspects of an individual application server instance. See [Section 2.3.2, "Using the Application Server Home Page"](#) for more information.
- Use 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. Similarly, use the Oracle Containers for J2EE (OC4J) Home page to deploy a custom Web-based application. See [Section 2.3.4, "Using an Oracle Application Server Component Home Page"](#) for more information.

2.1.1.2 The Underlying Software Technologies

The Application Server Control Console 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 the Application Server Control Console.

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

Technology	Description
Dynamic Monitoring Service (DMS)	The Application Server Control Console uses DMS to gather performance data about your Oracle Application Server components. Refer to <i>Oracle Application Server Performance Guide</i> .
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. Refer to Section 1.4.1.1, "Oracle Process Manager and Notification Server (OPMN)" .
Distributed Configuration Management (DCM)	The Application Server Control Console uses DCM to make configuration changes and to propagate configuration changes and deployed applications across the cluster. Refer to Section 1.4.1.2, "Distributed Configuration Management (DCM)" .
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 Console to ensure both processes are running and available at all times.

2.1.2 Oracle Enterprise Manager 10g Grid Control

If you have an environment that includes other Oracle products and applications in addition to Oracle Application Server, then consider using Oracle Enterprise Manager 10g Grid Control.

Grid Control, when used with Application Server Control, provides a wider view of your Oracle environment beyond the application server. From a central location, you can use the Grid Control Console to manage databases, application servers, and Oracle applications across your entire network.

The Grid Control Console offers advanced management features, such as a Notification system to notify administrators of changes in your environment and a Job system to automate standard and repetitive tasks, such as executing a SQL script or executing an operating system command.

Grid Control is installed separately from the Oracle Enterprise Manager 10g installation CD-ROM. The Grid Control Console provides a wider view of your network so you can manage multiple Oracle Application Server instances. In addition, the Grid Control Console provides a robust feature set designed to help you manage all aspects of your enterprise, including your Oracle databases, hosts, listeners, and other components.

See Also: Chapter 2 in the *Oracle Application Server Administrator's Guide*

2.2 Understanding Command-line Tools

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 most important administration command-line tools are:

- `runstartupconsole`, which starts and stops Application Server instances. You can use `runstartupconsole` to:

- Start and stop entire Application Server instances, including the Infrastructure, middle tier, and Enterprise Manager, at the same time when they are installed on the same host.
- Start and stop either the Infrastructure or the middle tier.
- Start and stop Enterprise Manager in the Infrastructure or middle-tier instances, or both at the same time.

See Also: [Section 3.1, "Starting and Stopping Application Server Instances"](#)

- `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:**
 - *Oracle Process Manager and Notification Server Administrator's Guide*
 - [Appendix A, "OPMN Commands"](#)
- `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:

- *Distributed Configuration Management Administrator's Guide*
- [Appendix B, "DCM Commands"](#)

In addition to these commands, Oracle Application Server provides many other command-line tools for performing specific tasks.

Note: 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 Console. These built-in performance metrics are measured continuously using performance instrumentation inserted into the implementations of Oracle Application Server components.

2.3 Understanding the Application Server Control Console

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

This section describes how to use the Application Server Control Console. It contains the following topics:

- [Displaying the Application Server Control Console](#)
- [Using the Application Server Home Page](#)
- [Using the Oracle Application Server Farm Home Page](#)
- [Using an Oracle Application Server Component Home Page](#)
- [Monitoring and Diagnosing with the Application Server Control Console](#)

2.3.1 Displaying the Application Server Control Console

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

- [Using the Application Server Control Console URL](#)
- [Understanding the Initial Application Server Control Console Home Page](#)

2.3.1.1 Using the Application Server Control Console URL

The URL for the Application Server Control Console 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:

```
(UNIX) ORACLE_HOME/install/setupinfo.txt  
(Windows) ORACLE_HOME\install\setupinfo.txt
```

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

```
http://mgmthost1.acme.com:1156
```

Note: The default port for the Application Server Control Console is usually 1156 on UNIX. However, if that port is in use, the installation 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 Understanding the Initial Application Server Control Console Home Page

When you first display the Application Server Control Console, 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 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 the Application Server Control Console.

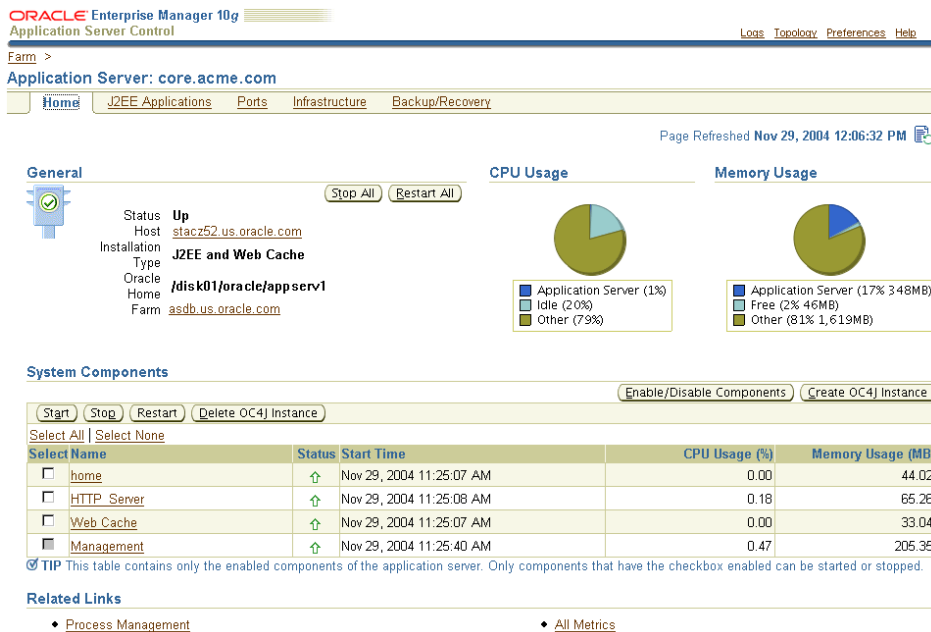
Table 2–2 Enterprise Manager Home Pages for Managing Oracle Application Server

Home Page	Description
Application Server Home page	<p>Use this home page to monitor and configure a single application server instance.</p> <p>The Application Server Home page is the first page you see if you have installed a single application server instance that does not use an OracleAS Metadata Repository.</p> <p>See Section 2.3.2, "Using the Application Server Home Page" for more information.</p>
OracleAS Farm page	<p>Use this home page to view a list of all the application server instances that use a common OracleAS Metadata Repository.</p> <p>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 OracleAS Metadata Repository.</p> <p>See Section 2.3.3, "Using the Oracle Application Server Farm Home Page" for more information.</p>

2.3.2 Using the Application Server Home Page

From the Application Server Home page, shown in [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 configure individual components and examine their performance.

Figure 2–1 Application Server Home page



The page contains a **System Components** table that lists the components of the application server. This table provides a snapshot of how each individual component is performing. You can also 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 **Topology** to view the Topology Viewer, which provides a graphical view of the application server processes managed by OPMN.

See Also: [Section 2.3.5.1, "Reviewing the Application Server Component Topology"](#)

- 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 **Backup/Recovery** to perform backup and recovery operations for the selected Oracle Application Server instance.

See Also: [Chapter 9, "Backup and Recovery"](#) and the Enterprise Manager online help for more information about backup and recovery procedures.

- 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**.

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

2.3.3 Using the Oracle Application Server Farm Home Page

If your application server instance uses an OracleAS Metadata Repository, then your start page for the Application Server Control Console is the OracleAS Farm page as shown in [Figure 2-2](#).

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

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

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

Using the Oracle Application Server Farm Home page, you can perform the following tasks:

- View multiple application server instances on multiple hosts
- Drill down to the Application Server Home page for each instance

- Create and manage OracleAS Clusters

See Also: *Oracle Application Server High Availability Guide* for more information about using OracleAS Clusters

Figure 2–2 The OracleAS Farm page

ORACLE Enterprise Manager 10g
Application Server Control

Topology Preferences Help

Farm: orcl.us.oracle.com

Instances can be grouped and managed together by configuring standalone instances in a common repository. This collection of instances is known as an Oracle Application Server Farm.

Repository Type Database

Clusters

Create Cluster

Select Name Status Instances

There are no clusters in the farm.

Standalone Instances

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

Join Cluster

Select Name	Host	Oracle Home
apserv1.acme.com	pc-host1.acme.com	C:\oracle\101202_bughunt_bif
apserv2.acme.com	solaris-host2.acme.com	/private/101202_shiphomes/bughunt_infra

Copyright © 1996, 2005, Oracle. All rights reserved.
About Oracle Enterprise Manager 10g Application Server Control

Topology | Preferences | Help

2.3.4 Using an Oracle Application Server Component Home Page

Component home pages vary from one component to another because each component has different monitoring and configuration requirements. However, most 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.

2.3.5 Monitoring and Diagnosing with the Application Server Control Console

The Application Server Control Console 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 the Application Server Component Topology](#)
- [Reviewing General Information and Resource Usage](#)
- [Reviewing the Resources of the Application Server Host](#)
- [Monitoring Application Server Components](#)
- [Monitoring Your J2EE Applications](#)

2.3.5.1 Reviewing the Application Server Component Topology

You can click **Topology** at the top of any page in Application Server Control Console to display Topology Viewer (Figure 2–3). The Topology Viewer provides a graphical, real-time representation of application server processes managed by OPMN. You can use this viewer to better understand the component relationships of the application server.

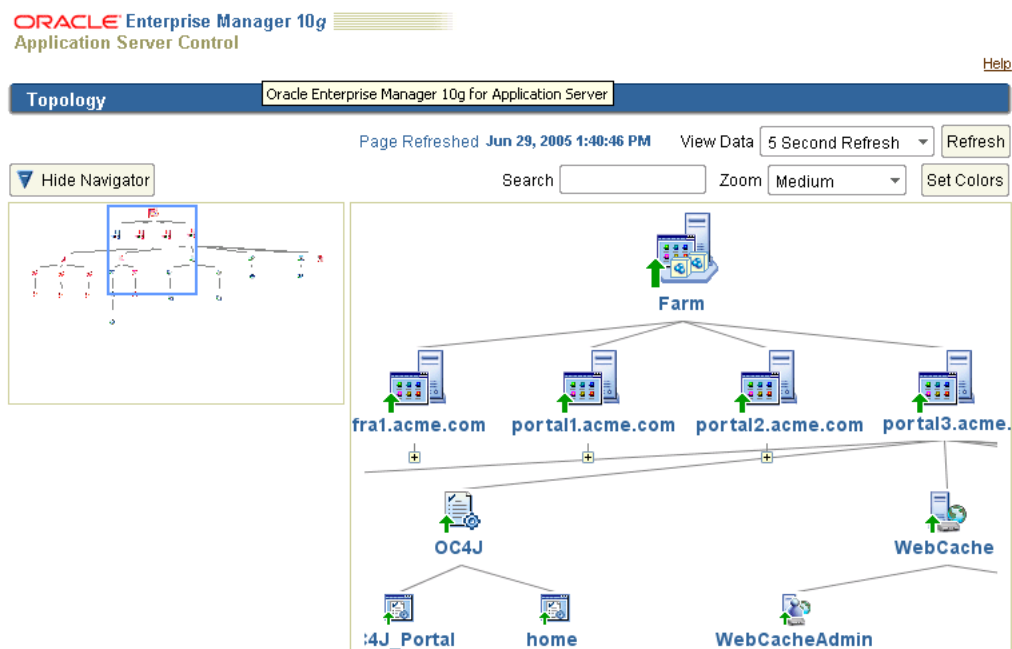
The Topology Viewer identifies each component of the application server with an icon. The position of each icon on the page and the connections between the icons represent the relationships between each component. Visual clues in the Topology Viewer help you quickly identify components that are down or performing poorly.

If you are managing multiple application servers as part of an OracleAS Farm, then the viewer also shows the relationships between the application server instances, including any OracleAS Cluster you have created.

From Topology Viewer, you can perform the following tasks:

- View the status of components
- Start, stop, or restart processes
- Monitor performance across the application server environment
- Drill down to component home pages for details

Figure 2–3 Topology Viewer



See Also: "About Topology Viewer" in the Enterprise Manager online help

2.3.5.2 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.

If you suspect that the application server is using too many resources, then review the resource usage by each component.

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

2.3.5.3 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.

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.

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, then 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.

2.3.5.4 Monitoring Application Server Components

After you review the high-level performance metrics and the resources available on the application server host computer, you can 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.

2.3.5.5 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. Click **J2EE Applications** on the Application Server Home page to display a list of the applications deployed from this application server instance.

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

See Also: For more complete information about monitoring, refer to the Application Server Control Console online help and the *Oracle Application Server Performance Guide*.

2.4 Managing the OracleAS Metadata Repository Database with Database Control

Many features of Oracle Application Server depend upon the OracleAS Metadata Repository, which uses an Oracle database to contain the OracleAS Metadata Repository. When you install the OracleAS Metadata Repository, you can choose to install a preconfigured instance of Oracle Database 10g for the OracleAS Metadata Repository.

If you have installed and deployed Oracle Enterprise Manager 10g Grid Control, then you can use the Grid Control Console to manage the OracleAS Metadata Repository.

See Also: [Section 2.1.2, "Oracle Enterprise Manager 10g Grid Control"](#)

However, if you are not centrally managing your environment with Grid Control, the OracleAS Metadata Repository database comes with Oracle Enterprise Manager 10g Database Control, which is provided with Oracle Database 10g.

To display the Database Control:

1. Use a Web browser to access the Database Control URL:

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

In this example:

- *hostname* is the name of the computer on which you installed Oracle Database.
- *port* is the port number reserved for the Database Control during installation.

If you do not know the correct port number, then look for the following line in the `portlist.ini` file, which is stored in the `install` directory of your OracleAS Metadata Repository Oracle home:

```
Enterprise Manager Console HTTP Port (db_name) = 5500
```

The installation reserves the first available port from the range 5500 to 5519. For example, if you installed Oracle Database on host `mgmt42`, and the Database Control uses port 5500, then enter the following URL:

```
http://mgmt42.acme.com:5500/em
```

Oracle Enterprise Manager displays the Database Control login page.

2. Log in to the database using the user name `SYS` and connect as `SYSDBA`.

Use the password that you specified for the `SYS` account during the installation.

3. Enterprise Manager displays the Database Home page.

From the Database Home page, you can review the current state of your database and access a wide range of monitoring and administration features.

See Also: *Oracle 2 Day DBA* in the Oracle Database 10g documentation library for an introduction to database management with the Database Control Console

Starting and Stopping

This chapter describes various procedures for starting and stopping Oracle Application Server and its components. It contains the following topics:

- [Starting and Stopping Application Server Instances](#)
- [Starting and Stopping Components](#)
- [Enabling and Disabling Components](#)
- [Starting and Stopping an Oracle Application Server Environment](#)

Oracle Application Server is a flexible product that you can start and stop in different ways, depending on your requirements.

3.1 Starting and Stopping Application Server Instances

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

- [Starting an Application Server Instance](#)
- [Stopping an Application Server Instance](#)
- [Starting OracleAS Infrastructure](#)
- [Stopping OracleAS Infrastructure](#)
- [Starting a Middle-Tier Instance](#)
- [Stopping a Middle-Tier Instance](#)

3.1.1 Starting an Application Server Instance

To start an entire application server instance, including the Infrastructure and the middle tier, such as when you have restarted your host, you can use the `runstartupconsole` command.

If the Infrastructure and middle tier is installed on the same host, run the following command from the middle-tier Oracle home:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh start all  
(Windows) ORACLE_HOME\bin\runstartupconsole.bat start all
```

The command starts the following in the Infrastructure Oracle home:

- The OracleAS Metadata Repository instance
- The Net Listener

- OracleAS Infrastructure processes such as Oracle Identity Management components, Oracle Internet Directory, OC4J_Security, DCM, and OPMN
- Enterprise Manager, including Application Server Control Console and Database Control

The command starts the following in the middle-tier Oracle home:

- OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and OracleAS Web Cache, OracleAS Forms Services, and OracleAS Reports Services
- Enterprise Manager Application Server Control Console

If you want to start the Infrastructure and middle tier, but not Enterprise Manager, run the following command from the middle-tier Oracle home:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh start allas
(Windows) ORACLE_HOME\bin\runstartupconsole.bat start allas
```

If you want to start only Enterprise Manager, but in both the Infrastructure and middle tier, run the following command from the middle-tier Oracle home:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh start allem
(Windows) ORACLE_HOME\bin\runstartupconsole.bat start allem
```

If the Infrastructure and middle tier are installed on separate hosts, see [Section 3.1.3, "Starting OracleAS Infrastructure"](#) and [Section 3.1.5, "Starting a Middle-Tier Instance"](#).

3.1.2 Stopping an Application Server Instance

To stop an entire application server instance, including the Infrastructure and the middle tier, such as when you are preparing to shut down your host, you can use the `runstartupconsole` command.

If the Infrastructure and middle tier is installed on the same host, run the following command from the middle-tier Oracle home:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh stop all
(Windows) ORACLE_HOME\bin\runstartupconsole.bat stop all
```

The command stops the following in the Infrastructure Oracle home:

- The OracleAS Metadata Repository instance
- The Net Listener
- OracleAS Infrastructure processes such as Oracle Identity Management components, Oracle Internet Directory, OC4J_Security, DCM, and OPMN
- Enterprise Manager, including Application Server Control Console and Database Control

The command stops the following in the middle-tier Oracle home:

- OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and OracleAS Web Cache, OracleAS Forms Services, and OracleAS Reports Services
- Enterprise Manager Application Server Control Console

If you want to stop the Infrastructure and middle tier, but not Enterprise Manager, run the following command from the middle-tier Oracle home:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh stop allas
```

```
(Windows) ORACLE_HOME\bin\runstartupconsole.bat stop allas
```

If you want to stop only Enterprise Manager, but in both the Infrastructure and middle tier, run the following command from the middle-tier Oracle home:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh stop allem
(Windows) ORACLE_HOME\bin\runstartupconsole.bat stop allem
```

If the Infrastructure and middle tier are installed on separate hosts, see [Section 3.1.4, "Stopping OracleAS Infrastructure"](#) and [Section 3.1.6, "Stopping a Middle-Tier Instance"](#).

3.1.3 Starting OracleAS Infrastructure

To start all processes in an OracleAS Infrastructure, such as when you have restarted your host, use the following command:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh start
(Windows) ORACLE_HOME\bin\runstartupconsole.bat start
```

When you run this command in the Infrastructure home, it starts the following:

- The OracleAS Metadata Repository instance
- The Net Listener
- OracleAS Infrastructure processes such as Oracle Identity Management components, Oracle Internet Directory, OC4J_Security, DCM, and OPMN
- Oracle Enterprise Manager 10g, including Application Server Control Console and Database Control

Alternatively, on Windows, you can start the Infrastructure from the Programs menu: **Start > Programs > Oracle Application Server Infrastructure - *Infra_name* > Start *instanceName***.

3.1.4 Stopping OracleAS Infrastructure

To stop all processes in an OracleAS Infrastructure, such as when you are preparing to shut down the host, use the following command:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh stop
(Windows) ORACLE_HOME\bin\runstartupconsole.bat stop
```

When you run this command in the Infrastructure home, it stops the following:

- The OracleAS Metadata Repository instance
- The Net Listener
- OracleAS Infrastructure processes such as Oracle Identity Management components, Oracle Internet Directory, OC4J_Security, DCM, and OPMN
- Oracle Enterprise Manager 10g, including Application Server Control Console and Database Control

Alternatively, on Windows, you can stop the Infrastructure from the Programs menu: **Start > Programs > Oracle Application Server Infrastructure - *Infra_name* > Stop *instanceName***.

3.1.5 Starting a Middle-Tier Instance

To start all processes in a middle-tier instance, take the following steps:

1. If the middle-tier instance uses OracleAS Infrastructure services, such as Oracle Identity Management or OracleAS Metadata Repository, make sure they are started.

If they are not started, use the command described in [Section 3.1.3, "Starting OracleAS Infrastructure"](#), or start both the middle-tier instance and its associated Infrastructure, using the procedure described in [Section 3.1.1, "Starting an Application Server Instance"](#).

2. Start the middle-tier instance by using the following command:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh start
(Windows) ORACLE_HOME\bin\runstartupconsole.bat start
```

When you run this command in a middle-tier Oracle home, it starts the following:

- OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and OracleAS Web Cache, OracleAS Forms Services, and OracleAS Reports Services
- Oracle Enterprise Manager 10g Application Server Control Console

Alternatively, on Windows, you can start the middle tier from the Programs menu: **Start > Programs > Oracle Application Server - Oracle_Home > Start > instanceName.**

3.1.6 Stopping a Middle-Tier Instance

To stop all processes in a middle-tier instance, use the following command:

```
(UNIX) ORACLE_HOME/bin/runstartupconsole.sh stop
(Windows) ORACLE_HOME\bin\runstartupconsole.bat stop
```

When you run this command in a middle-tier Oracle home, it stops the following:

- OPMN and all OPMN-managed processes such as DCM, Oracle HTTP Server, OC4J instances, and OracleAS Web Cache, OracleAS Forms Services, and OracleAS Reports Services
- Oracle Enterprise Manager 10g Application Server Control Console

Alternatively, on Windows, you can stop the middle tier from the Programs menu: **Start > Programs > Oracle Application Server - Oracle_Home > Stop > instanceName.**

3.2 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 Console: a Web-based tool

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

Although the two tools can be used interchangeably, they offer different features. With the `opmnctl` command, you can start and stop subprocesses within components, as well as the entire component. For example, you can start and stop OracleAS Web Cache, or you can start and stop only the OracleAS Web Cache Admin subprocess.

With the Application Server Control Console, you can 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.

3.2.1 Starting and Stopping Using opmnctl

You can start, stop, or restart a component, using the following commands:

```
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
```

The commands are shown in UNIX format. For Windows, invert the slashes.

You can start, stop, or restart the subprocess of a component, using the following commands:

```
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
```

The commands are shown in UNIX format. For Windows, invert the slashes.

You can check the status of components and processes, using the following command:

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

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

3.2.2 Starting and Stopping Using the Application Server Control Console

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

1. Open the Application Server Home page from the Application Server Control Console. 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.

3.3 Enabling and Disabling Components

If you want a component to start every time the application server instance is started, then you must enable the component. On the other hand, if you disable a component, it will no longer start when the application server instance is started.

You can enable and disable components using the Application Server Control Console. On the Application Server Home page, click **Enable/Disable Components**. 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, then you must run `bkp_restore.pl -m config` after you enable or disable components so that these are registered with the OracleAS Backup and Recovery Tool.

3.4 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 you must 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 to apply a patch.

3.4.1 Starting an Oracle Application Server Environment

You can start an Oracle Application Server environment as follows:

1. Start any OracleAS Infrastructure that contains only OracleAS Metadata Repository.

If your environment has OracleAS Infrastructure installations that contain only OracleAS Metadata Repository, then start them in any order. For these installation types, you only need to start OracleAS Metadata Repository. You do not need to start any processes with `opmnctl` and you do not need to start the Application Server Control Console. See [Section 3.1.3, "Starting OracleAS Infrastructure"](#) for more information.

2. Start the OracleAS Infrastructure that contains Oracle Identity Management.

If your environment uses Oracle Identity Management, then start the OracleAS Infrastructure that contains Oracle Internet Directory. See [Section 3.1.3, "Starting OracleAS Infrastructure"](#) for more information.

3. Start OracleAS Clusters.

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

See Also: *Oracle Application Server High Availability Guide* for more information

4. Start middle-tier instances.

If your environment contains middle-tier instances that are not part of OracleAS Cluster, then start them in any order. See [Section 3.1.5, "Starting a Middle-Tier Instance"](#) for more information.

3.4.2 Stopping an Oracle Application Server Environment

You can stop all processes in an Oracle Application Server environment as follows:

1. Stop OracleAS Clusters.
2. Stop middle-tier instances. See [Section 3.1.6, "Stopping a Middle-Tier Instance"](#) for more information.

3. Stop the OracleAS Infrastructure that contains Oracle Identity Management. See [Section 3.1.4, "Stopping OracleAS Infrastructure"](#) for more information.
4. Stop any OracleAS Infrastructure instances that contain only OracleAS Metadata Repository.

See Also: *Oracle Application Server High Availability Guide*

Changing the HTTP Listener Ports

This chapter describes how to change the port numbers. It contains the following topics:

- [Changing the HTTP Server Listen Port on Middle-Tier Instances](#)
- [Changing the HTTP Server Listen Port on Identity Management Installations](#)

See Also: Refer to [Section 1.3, "Checking Your Port Numbers"](#) to view port numbers

4.1 Changing the HTTP Server Listen Port on Middle-Tier Instances

This section describes how to change port numbers in middle-tier instances and update any other affected components. It contains the procedure to change the Oracle HTTP Server listen port (SSL or Non-SSL).

When you change the Oracle HTTP Server Listen directive, there are often dependencies that must also be set. For example, if you are using OracleAS Web Cache to improve the performance of your Oracle Application Server instance, then you must modify the OracleAS Web Cache origin server settings whenever you modify the Oracle HTTP Server Listen ports.

To be sure the port dependencies are modified correctly, you can use a single command to change the Oracle HTTP Server Listen port. The `portconfig` command automatically modifies the necessary configuration files within the Oracle home and optionally restarts the required components within the Oracle home.

The following sections describe how to define the `portconfig` command and then use it to modify the Oracle HTTP Server Listen SSL or non-SSL port:

- [Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 \(UNIX only\)](#)
- [Using the portconfig Command to Change the Oracle HTTP Server Listen Port](#)

4.1.1 Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024

If you are on a UNIX system and you are changing the Listen port to a number less than 1024, perform these steps before you change the Oracle HTTP Server Listen port.

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

1. Log in as the `root` user.

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

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

4.1.2 Using the portconfig Command to Change the Oracle HTTP Server Listen Port

Use the following procedure to change the Oracle HTTP Server SSL or non-SSL Listen port:

1. Set the ORACLE_HOME environment variable to the home directory of the Oracle Application Server instance where the Oracle HTTP Server resides.

For example:

```
(UNIX) setenv ORACLE_HOME /dev0/private/oracle/appserv1/
(Windows) set ORACLE_HOME=D:\oracle\appserv1\
```

2. On UNIX systems, set the LD_LIBRARY_PATH, LD_LIBRARY_PATH_64, LIB_PATH, or SHLIB_PATH environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you must set depend on the type of your UNIX operating system.
3. Create an alias (on UNIX systems) or a DOSKEY macro (on Windows systems) to represent the portconfig command.

For example, to execute the command as an alias on UNIX systems, enter the following command:

```
alias portconfig '$ORACLE_HOME/jdk/bin/java -cp
$ORACLE_HOME/sysman/webapps/emd/WEB-INF/lib/emd.jar:
$ORACLE_HOME/dcm/lib/dcm.jar:
$ORACLE_HOME/sso/lib/ossoreg.sh
oracle.sysman.ias.sta.tools.PortConfigCmdLine \!*
```

Similarly, to execute the command as DOSKEY macro on Windows systems, enter the following at the DOS command line:

```
doskey portconfig=%ORACLE_HOME%\jdk\bin\java -cp
%ORACLE_HOME%\sysman\webapps\emd\WEB-INF\lib\emd.jar;
%ORACLE_HOME%\dcm\lib\dcm.jar;
%ORACLE_HOME%\sso\lib\ossoreg.bat
oracle.sysman.ias.sta.tools.PortConfigCmdLine $*
```

4. Use the newly created portconfig command as follows:

```
portconfig -oracleHome ORACLE_HOME
-oldPort old_port
-newPort new_port
[-sso -url http://sso_host:port -user http_server_admin_user
 [-site name_of_sso_partner_application]
 [-admin mod_osso_admin_user]
 [-vHost path_to_mod_osso_configuration_file]]
[-webCache]
{-start | -restart}
```

For example, on UNIX systems:

```
portconfig -oracleHome $ORACLE_HOME -oldPort 7777 -newPort 7778 -webCache
```

For example, on Windows systems:

```
portconfig -oracleHome %ORACLE_HOME% -oldPort 7777 -newPort 7778 -webCache
```

Table 4–1 describes the arguments available when you use the `portconfig` command to automatically change the Oracle HTTP Server Listen port.

Table 4–1 Arguments for the `portconfig` Command

Argument	Description
<code>-oracleHome</code>	The Oracle home of the Oracle Application Server instance. The <code>portconfig</code> command modifies only components that are part of the selected Oracle home. You can use an environment variable to represent the Oracle home.
<code>-oldPort</code>	The old (current) value of the Oracle HTTP Server Listen port.
<code>-newPort</code>	The new value for the Oracle HTTP Server Listen port.
<code>-webCache</code>	<p>Use this optional argument if you are using OracleAS Web Cache to improve the performance and reliability of your Web server. When this argument is included on the command line, the dependent OracleAS Web Cache port assignment is changed automatically.</p> <p>Specifically, the port number of the origin server is updated automatically so that it points to the new Oracle HTTP Server listen port.</p> <p>Note: The <code>portconfig</code> command updates the OracleAS Web Cache instance only if it resides in the current Oracle home.</p>
<code>-start</code>	<p>Use this optional argument to stop and start the application server instance after the <code>portconfig</code> command performs the configuration changes. The Oracle Application Server instance must be stopped and started—or restarted—before the port changes take effect.</p> <p>Note that during startup, all enabled components of the application server are started, even those that were originally down before you ran the <code>portconfig</code> command to change the Oracle HTTP Server Listen port.</p> <p>Compare with the <code>-restart</code> argument. Each time you run the command you can use the <code>-restart</code> or <code>-start</code> options, but not both.</p>
<code>-restart</code>	<p>Use this optional argument to stop and start the application server instance after the <code>portconfig</code> command performs the configuration changes. The Oracle Application Server instance must be restarted—or stopped and started—before the port changes take effect.</p> <p>With this option, only already running components are restarted after the configuration changes are complete. Components that were down before you ran the <code>portconfig</code> command to change the Oracle HTTP Server Listen port will remain down.</p> <p>Compare with the <code>-start</code> argument. Each time you run the command you can use the <code>-restart</code> or <code>-start</code> options, but not both.</p>
<code>-debug</code>	Use this optional argument to display debugging information as the command executes. This argument can be useful if you are troubleshooting a problem or working with Oracle Support.
<code>-sso</code>	<p>Use this optional argument when the Listen port you are changing is protected by OracleAS Single Sign-On.</p> <p>When you use this argument, the <code>portconfig</code> command re-registers <code>mod_osso</code> with the new Oracle HTTP Server Listen port value.</p> <p>When you use the <code>-sso</code> argument, then you must include the <code>-url</code> and <code>-user</code> arguments. In addition, you can optionally use the <code>-site</code>, <code>-admin</code>, and <code>-vHost</code> arguments.</p> <p>For more information about registering <code>mod_osso</code>, see "Configuring and Administering Partner Applications" in the <i>Oracle Application Server Single Sign-On Administrator's Guide</i>.</p>

Table 4–1 (Cont.) Arguments for the portconfig Command

Argument	Description
-url	<p>This argument is required when you use the <code>-sso</code> argument.</p> <p>Use this argument to provide the new Oracle HTTP Server URL, which is also used by OracleAS Single Sign-On and uses the new Listen port. For example:</p> <pre>http://sso42.acme.com:7778</pre> <p>This URL is passed as the <code>-mod_osso_url</code> parameter in the <code>ssoreg.sh</code> and <code>ssoreg.bat</code> scripts.</p>
-user	<p>This argument is required when you use the <code>-sso</code> argument.</p> <p>Use this argument to enter the name of the account that is used to start Oracle HTTP Server. On UNIX systems, this is usually <code>root</code>. On Windows, it is usually <code>SYSTEM</code>.</p> <p>The value provided with this argument is passed as the <code>-u</code> parameter in the <code>ssoreg.sh</code> and <code>ssoreg.bat</code> scripts.</p>
-site	<p>This argument is optional; however, it can be used only when you use the <code>-sso</code> argument.</p> <p>Use this argument to enter the site name of OracleAS Single Sign-On partner application. The site name is displayed by the OracleAS Single Sign-On administration pages.</p> <p>The value of this argument is passed as the <code>-site_name</code> parameter in the <code>ssoreg.sh</code> and <code>ssoreg.bat</code> scripts. If the <code>-site</code> argument is not specified, the application server instance name is passed to <code>ssoreg.sh</code> and <code>ssoreg.bat</code> scripts as the value of the <code>-site_name</code> parameter.</p>
-admin	<p>This argument is optional; however, it can be used only when you use the <code>-sso</code> argument.</p> <p>Use this argument to enter the account name of the <code>mod_osso</code> administrator. This value is displayed in the OracleAS Single Sign-On administration pages. In most cases, this value should be the same as the distinguished name (dn) of the user who installed Oracle Application Server. The value of this argument is passed as the <code>-admin_info</code> parameter in the <code>ssoreg.sh</code> and <code>ssoreg.bat</code> scripts.</p>
-vHost	<p>This argument is optional; however, it can be used only when you use the <code>-sso</code> argument.</p> <p>Use this argument to enter the path to the <code>osso.conf</code> file for the virtual host being configured. For example:</p> <pre>\$ORACLE_HOME/Apache/Apache/conf/osso/vh_name/osso.conf</pre> <p>Use this argument only when you are registering an HTTP virtual host with the OracleAS Single Sign-On server. The value of this argument is passed as the <code>-config_file</code> parameter, along with the <code>-virtualhost</code> parameter, in the <code>ssoreg.sh</code> and <code>ssoreg.bat</code> scripts.</p>

5. Restart the application server instance:

UNIX:

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/opmn/bin/opmnctl startall
ORACLE_HOME/bin/emctl start iasconsole
```

Windows:

```
ORACLE_HOME\bin\emctl stop iasconsole
ORACLE_HOME\opmn\bin\opmnctl stopall
ORACLE_HOME\opmn\bin\opmnctl startall
ORACLE_HOME\bin\emctl start iasconsole
```


4.2 Changing the HTTP Server Listen Port on Identity Management Installations

This section describes how to change the Oracle HTTP Server HTTP or HTTPS listen port on an Identity Management installation. When you change this port number, you also effectively change the OracleAS Single Sign-On port number. This means you must update any middle-tier instances that use the OracleAS Single Sign-On port.

Task 1: Prepare the Middle-Tier Instances

Perform this task only if the Identity Management installation is being used by middle-tier instances. On each middle-tier instance that uses Oracle Identity Management, stop the middle-tier instance as follows:

1. On the Application Server Home page of the Application Server Control Console, click **Stop All**.
2. Leave the Application Server Control Console running.

It is important that you leave the Application Server Control Console running in each of the middle-tier instances while you perform this procedure.

Task 2: Prepare the Infrastructure Instances

1. Ensure that Oracle Identity Management and its associated OracleAS Metadata Repository are started 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, then ensure that those are up. In short, ensure all Metadata Repositories in your environment are up.

Task 3: Modify the Oracle HTTP Server Listen and Port Directives

If you are changing the HTTP port, change both the non-SSL Listen and Port directives to the new port number. Perform the following steps:

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.

Note: You can manually update the port numbers in the `httpd.conf` file. Update the non-SSL listen and port directives that are not enclosed in an SSL virtual host container with the same new port number. Save the file, and then run the following command:

```
dcmctl updateConfig -ct ohs
```

If you are changing the HTTPS port, change both the SSL Listen and SSL Port directives to the new port number, perform the following steps:

1. Edit the following file:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/ssl.conf  
(Windows) 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.
3. Save and close the file.
4. Run the following command:

```
(UNIX) ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct ohs  
(Windows) ORACLE_HOME\dcm\bin\dcmctl updateConfig -ct ohs
```

Task 4: Enable Oracle HTTP Server to Run as Root for Ports Less Than 1024 on UNIX

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, then 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
```

Task 5: Update the Application Server Control Console

Update the Application Server Control Console with the new port number:

1. Edit the following file:

```
(UNIX) ORACLE_HOME/sysman/emd/targets.xml  
(Windows) ORACLE_HOME\sysman\emd\targets.xml
```

2. Update each occurrence of the old Oracle HTTP Server listen port number with the new port number.
3. Save and close the file.
4. Reload the Application Server Control Console:

```
(UNIX) ORACLE_HOME/bin/emctl reload  
(Windows) ORACLE_HOME\bin\emctl reload
```

Task 6: Update OracleAS Single Sign-On

In the example, *hostname* is the host on which OracleAS Single Sign-On is running and *new_port_number* is the new SSL Oracle HTTP Server listen port number.

Perform this task if OracleAS Single Sign-On is configured to use the Oracle HTTP Server HTTP listen port in the installation where you are changing the port.

1. On UNIX systems, set the LD_LIBRARY_PATH, LD_LIBRARY_PATH_64, LIB_PATH, or SHLIB_PATH environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you must set depend on the type of your UNIX operating system.

2. Run one or both of the following commands in the OracleAS Single Sign-On Oracle home:

To change the non-SSL port:

```
(UNIX) ORACLE_HOME/sso/bin/ssocfg.sh http hostname new_non_ssl_port_number
(Windows) ORACLE_HOME\sso\bin\ssocfg.bat http hostname new_non_ssl_port_number
```

To change the SSL port:

```
(UNIX) ORACLE_HOME/sso/bin/ssocfg.sh https hostname new_ssl_port_number
(Windows) ORACLE_HOME\sso\bin\ssocfg.bat https hostname new_ssl_port_number
```

In the examples:

- *hostname* is the host on which OracleAS Single Sign-On is running.
- *new_non_ssl_port_number* is the new non-SSL Oracle HTTP Server listen port number.
- *new_ssl_port_number* is the new SSL Oracle HTTP Server listen port number.

Task 7: Re-register mod_osso

To re-register mod_osso, perform the following steps:

1. On UNIX systems, set the LD_LIBRARY_PATH, LD_LIBRARY_PATH_64, LIB_PATH, or SHLIB_PATH environment variables to the proper values, as shown in [Table 1-1](#).
2. On Windows systems, set the path, for example: PATH=%PATH%;%ORACLE_HOME%\bin;%ORACLE_HOME%\lib.
3. If you are changing the non-SSL listen port, then re-register mod_osso to take care of the default partner applications by running the following command in Oracle Identity Management Oracle home:

UNIX:

```
ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path identity_management_oracle_home
-site_name identity_management_hostname:new_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
```

Windows:

```
ORACLE_HOME\sso\bin\ssoreg.bat
-oracle_home_path middle_tier_oracle_home
-site_name identity_management_hostname:new_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
```

For example, 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
```

4. If you are changing the Oracle HTTP Server SSL listen port, perform the following steps.

- a. Re-register `mod_osso` with the new port number by running the following command in the middle-tier Oracle home:

UNIX:

```
ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path identity_management_oracle_home
-site_name identity_management_hostname:new_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-config_file path/osso-https.conf
```

Windows:

```
ORACLE_HOME\sso\bin\ssoreg.bat
-oracle_home_path identity_management_oracle_home
-site_name identity_management_hostname:new_port_number
-config_mod_osso TRUE
-mod_osso_url mod_osso_url
-config_file path\osso-https.conf
```

For example, if you want to change the Oracle HTTP Server SSL listen port to 7778 on myhost on UNIX:

```
$ORACLE_HOME/sso/bin/ssoreg.sh
-oracle_home_path /disk1/oracleas
-site_name myhost:4445
-config_mod_osso TRUE
-mod_osso_url http://myhost.mydomain:7778
-config_file $ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf
```

- b. Edit the `mod_osso.conf` file, which is located at:

```
(UNIX) ORACLE_HOME/Apache/Apache/conf/mod_osso.conf
(Windows) ORACLE_HOME\Apache\Apache\conf\mod_osso.conf
```

In the `mod_osso.conf` file, comment the following directive, if you have not previously done so:

On UNIX:

```
LoadModule osso_module libexec/mod_osso.so
```

On Windows:

```
LoadModule osso_module modules\ApacheModuleOsso.dll
```

- c. In the `httpd.conf` file, which is found in the same (`conf`) directory, add the directive that you just commented in the preceding step (if you have not previously done so). In a default setup, place the directive right after:

```
LoadModule wchandshake_module libexec/mod_wchandshake.so
```

5. Restart the Oracle HTTP Server:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=HTTP_Server
(Windows) ORACLE_HOME\opmn\bin\opmnctl restartproc process-type=HTTP_Server
```

6. Re-register any additional partner applications that you configured or modified.

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

Task 8: Update Oracle Delegated Administration Services

If you have Oracle Delegated Administration Services configured, and Oracle Delegated Administration Services uses the SSL and non-SSL port numbers, take the following steps to update the Oracle Delegated Administration Services URL entry in Oracle Internet Directory.

Note: To find out what port Oracle Delegated Administration Services uses, enter the following command:

```
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:

```
ldapmodify -D cn=orcladmin -w password -p oid_port -f mod.ldif
```

Task 9: Update Oracle Application Server Certificate Authority

If you are using OracleAS Certificate Authority:

1. Re-register OracleAS Certificate Authority with the OracleAS Single Sign-On server by running the following command in the OracleAS Certificate Authority Oracle home:

```
(UNIX) ORACLE_HOME/oca/bin/ocactl changesecurity -server_auth_port portnum
(Windows) ORACLE_HOME\oca\bin\ocactl changesecurity -server_auth_port portnum
```

In the example, `port_number` is the OracleAS Certificate Authority Server Authentication Virtual Host (SSL) port. The default value is 4400.

See Also: *Oracle Application Server Certificate Authority Administrator's Guide* for more information

2. If OracleAS Certificate Authority is located in a different Oracle home than the OracleAS Single Sign-On server, then restart Oracle HTTP Server and the `oca` instance in the OracleAS Certificate Authority Oracle home. For example, on UNIX:

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

Task 10: Restart the Identity Management Instance

Restart the Identity Management instance. For example, on UNIX:

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
ORACLE_HOME/opmn/bin/opmnctl startall
ORACLE_HOME/bin/emctl start iasconsole
```

Task 11: Restart OracleAS Certificate Authority

If OracleAS Certificate Authority is configured in this instance, then restart it:

```
(UNIX) ORACLE_HOME/oca/bin/ocactl start
(Windows) ORACLE_HOME\oca\bin\ocactl start
```

Task 12: Update the Middle-Tier Instances to Use the New Port Number

After you change the Oracle HTTP Server non-SSL port on the Identity Management installation, you must update all middle-tier instances to use the new port number.

1. Update each middle-tier instance using the Change Identity Management wizard in the Application Server Control Console.

On each middle-tier instance that uses Identity Management:

- a. Using the Application Server Control Console, navigate to the Application Server Home page for the middle-tier instance.
 - b. Click the **Infrastructure** link.
 - c. On the Infrastructure page, in the Identity Management section, click **Change**.
 - d. Follow the steps in the wizard.
 - e. When the wizard is finished, navigate to the Application Server Home page and start the middle-tier instance by clicking **Start All**.
2. Refresh the Oracle Internet Directory cache in your applications:
 - a. Log in to the Portal.
 - b. Click the global settings link.
 - c. Click the **SSO/OID** tab.
 - d. Check the refresh Oracle Internet Directory cache settings and click **Apply**.

Viewing and 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, and access information about HTTP requests. 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:

- [Introducing Oracle Application Server Logging](#)
- [Listing and Viewing Log Files With Enterprise Manager](#)
- [Using Oracle Application Server Log Loader](#)

5.1 Introducing Oracle Application Server Logging

With the Application Server Control Console, you can list and search log files across Oracle Application Server components. You can view log files from the Application Server Control Console pages or download a log file to your local client and view the log files using another tool.

This section contains the following topics:

- [Understanding Log File Data and Naming](#)
- [Using a Log Repository](#)
- [Configuring Component Logging Options](#)

5.1.1 Understanding Log File Data and Naming

Several Oracle Application Server components use Oracle Diagnostic Logging (ODL). ODL ensures that the log file naming and log file content formats conform to an Oracle standard. ODL writes the diagnostic messages in XML. Components that do not use ODL write their diagnostic messages using a component-specific text format.

You can view log files of any format by using the Application Server Control Console. You can also download log files to your local client and view them using a text editor or another file viewing utility.

5.1.1.1 Log File Messages by Component

[Table 5–1](#) lists the supported message formats for each Oracle Application Server component.

Table 5–1 Diagnostic Message Format By Component

Component	Default Format	ODL Support	Location ¹
Oracle ADF (ADF)	ODL	Yes	<i>ORACLE_HOME</i> /bc4j/logs/ <i>OC4J_Name</i>
BPEL Process Manager	Text	No	<i>ORACLE_HOME</i> /integration/orabpel/system/logs
CM SDK	Text	No	<i>ORACLE_HOME</i> /ifs/cmsdk/log/ <i>cmsdk_domain_name</i> /DomainController.log <i>ORACLE_HOME</i> /ifs/cmsdk/log/ <i>cmsdk_domain_name</i> / <i>node_name</i> .log
DCM	ODL	Yes	<i>ORACLE_HOME</i> /dcm/logs
Discoverer	Text	No	<i>ORACLE_HOME</i> /discoverer/logs Discoverer Viewer is an OC4J application. The log file is named <i>application.log</i> and is found in the directory <i>ORACLE_HOME</i> /j2ee/OC4J_BI_FORMS.
Enterprise Manager	Text	No	<i>ORACLE_HOME</i> /sysman/log
Forms	Text	No	<i>ORACLE_HOME</i> /j2ee/OC4J_BI_FORMS/application-deployments/formsapp/ <i>island</i> /application.log
HTTP Server	Text	Yes	<i>ORACLE_HOME</i> /Apache/Apache/logs/error_log.time
InterConnect	Text	No	<i>ORACLE_HOME</i> /oai/10.1.2/adapters/ <i>adapter_name</i> /logs
Integration B2B	ODL	Yes	<i>ORACLE_HOME</i> /ip/log
Oracle BPEL Process Analytics	Text	No	<i>ORACLE_HOME</i> /integration/bam/log
Log Loader	ODL	Yes	<i>ORACLE_HOME</i> /diagnostics/logs
OC4J <i>instance_name</i>	Text	Yes	<i>ORACLE_HOME</i> /j2ee/ <i>instance_name</i> /log <i>ORACLE_HOME</i> /j2ee/ <i>instance_name</i> /application-deployments/ <i>application_name</i> /application.log
OCA	Text	No	From the command line, for administrator use only, messages are stored at: <i>ORACLE_HOME</i> /oca/logs/admin.log Logging for user and administrator usage, other than command line, is stored in the database and accessed through the OracleAS Certificate Authority (OCA) Administrator web interface.
Oracle Internet Directory	Text	No	<i>ORACLE_HOME</i> /ldap/log
OPMN	Text	No	<i>ORACLE_HOME</i> /opmn/logs <i>ORACLE_HOME</i> /opmn/logs/ <i>component_type</i> ~...
Port Tunneling	Text	No	<i>ORACLE_HOME</i> /iaspt/logs
Reports Server	Text	No	<i>ORACLE_HOME</i> /reports/logs
Single Sign-On	Text	No	<i>ORACLE_HOME</i> /sso/log
TopLink	Text	No	As specified with the log_path configuration option in the TopLink installation directory, as: config/toplink.xml
Universal Installer	Text	No	<i>ORACLE_HOME</i> /cfgtoollogs/
Web Cache	Text	No	<i>ORACLE_HOME</i> /webcache/logs
Wireless	Text	Yes	<i>ORACLE_HOME</i> /wireless/logs

¹ Locations are shown in UNIX format. Invert the slashes for Windows format.

5.1.2 Using a Log Repository

The Application Server Control Console supports viewing diagnostic messages from a Log Repository. A Log Repository:

- Stores error logs, but does not store access logs.
- Contains diagnostic messages collected from multiple log files across components.
- Consolidates Oracle Application Server log file data, which enables you to use the Application Server Control Console to easily search and view log file data generated by multiple components.
- Speeds up the diagnostic process and reduces the resources required to support Oracle Application Server.

A Log Repository is updated by the Oracle Application Server Log Loader component.

See Also: [Section 5.3, "Using Oracle Application Server Log Loader"](#)

5.1.3 Configuring Component Logging Options

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

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

The logging configuration options include:

- Specifying log file names and pathnames
- Limiting log file size
- Using log file archiving
- Setting component logging levels

The logging configuration options are component dependent. Not all components support the logging configuration options.

See Also: Oracle Application Server component documentation for information about setting logging configuration options

5.2 Listing and Viewing Log Files With Enterprise Manager

You can use the Application Server Control Console to list log files. On the Application Server Control Console, click the **Logs** link to display the View Logs page.

This section describes the following:

- [Listing Log Files](#)
- [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](#)

5.2.1 Listing Log Files

To list the log files, perform the following steps:

1. From the View Logs page, click **Move** or **Move All** to move the selected or all available components to the **Selected Components** box.
2. Click **Search** 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 5–1 shows the Application Server Control Console View Logs page after a search.

Figure 5–1 Enterprise Manager View Logs Search Results

The screenshot shows the Oracle Enterprise Manager 10g Application Server Control console. The page title is "Application Server Control" and the breadcrumb is "Farm > Application Server: oracleas1.hqoracle.com > View Logs". The page was refreshed on Apr 6, 2005 at 1:29:18 PM. The "Log Files" tab is active, and the "Search Log Repository" button is visible. Below the search bar, there are sections for "Available Components" and "Selected Components". The "Selected Components" list includes: ADF Business Components, ASCLONE, DCM, Discoverer, Enterprise Manager, Forms, HTTP_Server, LogLoader, OC4J_BI_Forms, and OC4J_Portal. A "Search" button is located below the component lists. The search results section shows "Results: 75 Log Entries Retrieved" and a table with the following data:

Component Type	Component Name	Log Type	Log File	Modified	Size (bytes)	OC4J Island	Pr
DCM	Command-line Utility	Error	log.xml	March 22, 2005 9:01:44 AM EST	12411		
DCM	Daemon Process	Error	log.xml	April 5, 2005 1:22:10 PM EDT	27066		
DCM	Enterprise Manager Website	Error	log.xml	March 22, 2005 9:14:12 AM EST	24146		

When you click the **Logs** link, the Application Server Control Console displays the View Logs page and runs a search for the component’s log files. You can then view the log files by selecting the **Log File** links shown in the Results section.

5.2.2 Listing Log Files for Selected Components

Using the Application Server Control Console, 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 click **Move** to move the selected component to the **Selected Components** box (some browsers support double clicking to move components between the boxes).
2. Click **Search** 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 5–1 shows the View Logs page with the Results after a search.

5.2.3 Listing Log Files from Oracle Application Server Components Pages

After you select a system component link on the Application Server Control Console Home page, you can view the component log files by selecting the **Logs** link. When you select this link, the Application Server Control Console 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.

5.2.4 Using Log Files Advanced Search

On the View Logs page, click **Advanced Search** to display the View Logs Advanced Search page. On the Advanced Search page, you can list log files for Oracle Application Server components and filter the search for log files by certain log file attributes.

Perform the following steps:

1. Select a component and click **Move**, or click **Move All** to move the components to the **Selected Components** box.
2. Select a field from the **Log File Attribute** list.
3. Click **Add Row** 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, click **Add Another Row** and enter additional values.
6. Click **Search** to perform the search. When the search returns, the **Results** section displays the log files with matching fields.

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

5.2.5 Viewing Log File Details and Log File Contents

After you click **Search** 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.

5.3 Using Oracle Application Server Log Loader

The Oracle Application Server **Log Loader** component initializes and updates 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 contains 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](#)

5.3.1 Starting and Stopping Log Loader

You can use the controls on the Application Server Control Console Log Loader page to start and stop the Log Loader.

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

To start the log loader, perform the following steps:

1. Click the **Logs** link on the Application Server Control Console page.
2. On the View Logs page, click the **Search Log Repository** link.
3. Click **Log Loader** on the View Logs page.
4. On the Log Loader page, click **Start**. The Confirmation page is displayed.
If the log loader is already running, click **Stop** to stop it.
5. Click **Start** or click **Start and Load Existing Logs** to start and initialize the log repository with the existing log messages.

5.3.2 Enabling and Disabling Log Loader

On the Log Loader page, click **Enable** to enable the Log Loader. When you first install Oracle Application Server, the Log Loader is enabled. When you disable the Log Loader, its log files are not displayed in the component lists on the View Logs page.

5.3.3 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. These messages are stored in the Log Repository, which includes information about the location and format of the log files. The instance is reconfigured after the Log Loader is started. For example, when a new component is added, click **Update Log Configuration** to update the Log Loader configuration. Updating the log configuration allows the Log Loader to reread configuration files to locate and load all the component log files into the Log Repository.

5.3.4 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 Console page.
2. From the View Logs page, select the **Search Log Repository** link.
3. Click **Log Loader** 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. Click **Apply** to apply the new values.

[Figure 5–2](#) shows the Application Server Control Console Log Loader Properties page.

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

Figure 5–2 Log Loader Properties Page

ORACLE Enterprise Manager 10g
Application Server Control

Topology Preferences Help

Farm > Application Server_oracleas1_hqoracle.com > View Logs > Log Loader >

Log Loader Properties

Page Refreshed Apr 6, 2005 1:42:39 PM

These properties can be used to control the behavior of the Log Loader and the size of the Log Repository it updates.

Location of Log Repository	<input type="text" value="diagnostics/repository"/>	(This property identifies the directory where the Log Repository is located.)
Maximum size of Log Repository (MB)	<input type="text" value="50"/>	(The total size of the Log Repository is controlled by this property.)
Size of each segment (MB)	<input type="text" value="5"/>	(The Log Repository is a set of files called segments. Segments are reused to control the size the the repository.)
Interval between loads (Minutes)	<input type="text" value="5"/>	(This property defines how often the Log Loader reads component log files and updates the Log Repository.)
Maximum load size (KBytes)	<input type="text" value="51200"/>	(The Log Loader may skip the loading of some log entries if a log file has grown very large since it was last loaded. This property controls the maximum number of bytes that may be loaded from a file or set of ODL files during a run of the Loader.)
Log Loader Port	<input type="text" value="44000"/>	(This property identifies the communication port used by the Log Loader.)

5.3.5 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:

- 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.
- 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:
 - XML syntax errors that prevent the file from being parsed. If such errors are encountered, then the Log Loader completely ignores the contents of the file.
 - A wrong path specified for a configuration file. If the Log Loader cannot find a log file at the specified path, then 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.
- 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.

- 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.
- 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 about the name of the log file */logfile*, and the number of bytes skipped *y_skipped*.

Changing Network Configurations

This chapter provides procedures for changing the network configuration of an Oracle Application Server host.

It contains the following topics:

- [Overview of Procedures for Changing Network Configurations](#)
- [Changing Your Hostname, Domain Name, or IP Address](#)
- [Moving Between Off-Network and On-Network](#)
- [Changing Between a Static IP Address and DHCP](#)

6.1 Overview of Procedures for Changing Network Configurations

The following procedures for changing network configurations are presented in this chapter:

- [Changing Your Hostname, Domain Name, or IP Address](#)

This section describes how to update Oracle Application Server when changing the hostname, domain name, or IP address of a host.

- [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.

6.2 Changing Your Hostname, Domain Name, or IP Address

After you have installed Oracle Application Server, there may come a time when you want to change the hostname, domain name, or IP address of the host. Depending on your installation type, you may perform some or all of these operations.

[Table 6–1](#) summarizes the installation types that support hostname, domain name, and IP address changes, and provides pointers to the appropriate procedures.

Table 6–1 Supported Procedures for Hostname, Domain Name, and IP Address Changes

Installation Type	Changing the Hostname or Domain Name	Changing the IP Address
Middle tier	Supported Refer to Section 6.2.1, "Changing the Hostname or Domain Name of a Middle-Tier Installation"	Supported Simply change the address in your operating system. No updates to Oracle Application Server are required
Infrastructure: Identity Management and Metadata Repository	Not supported	Supported Refer to Section 6.2.2, "Changing the IP Address of an Infrastructure Containing a Metadata Repository"
Infrastructure: Metadata Repository only	Not supported	Supported Refer to Section 6.2.2, "Changing the IP Address of an Infrastructure Containing a Metadata Repository"
Infrastructure: Identity Management only Applies to Identity Management containing the following in any configuration: Oracle Internet Directory, OracleAS Single Sign-On, Oracle Delegated Administration Services, Oracle Directory Integration and Provisioning	Supported Refer to <i>Oracle Application Server Administrator's Guide</i>	Supported Refer to <i>Oracle Application Server Administrator's Guide</i>
OracleAS Certificate Authority	Supported Refer to <i>Oracle Application Server Administrator's Guide</i>	Supported Simply change the address in your operating system. No updates to Oracle Application Server are required

6.2.1 Changing the Hostname or Domain Name of a Middle-Tier Installation

This section describes how to change the hostname, domain name, or both, of a host that contains any of the following middle-tier installation types:

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

Note: This procedure is not supported for OracleAS Developer Kits.

The following sections describe the procedure:

- [Things to Know Before You Start](#)
- [Task 1: Prepare Your Host](#)
- [Task 2: Change the Hostname](#)
- [Task 3: Run the chgiphost Command](#)
- [Task 4: Restart Your Environment](#)
- [Task 5: Update OracleAS Portal, OracleAS Wireless, OracleAS Single Sign-On, and Oracle Ultra Search](#)

- [Task 6: Manually Update the Hostname in Files](#)

Things to Know Before You Start

Review the following items before you start:

- If any installations contain Oracle Content Management Software Development Kit, then you must perform additional steps. Refer to *Oracle Content Management SDK Administrator's Guide* before starting this procedure.
- If the middle-tier instance is registered with Oracle Internet Directory, then you must supply the `cn=orcladmin` password during the procedure.
- Consider changing the log level before running the `chgiphost` command so you can view more detailed information. See [Section 6.2.3.1, "Setting the Log Level for chgiphost"](#) for more information.
- If your old hostname is a string that is likely to appear in a configuration file, then the `chgiphost` script may encounter problems when trying to update the configuration files. Refer to [Section 6.2.3.2, "Customizing the chgiphost Script"](#) for information about how to avoid this problem.
- Write down the old hostname and IP address before you begin. You will be prompted for these values.
- Oracle recommends that you perform a backup of your environment before you start this procedure. Refer to [Chapter 9, "Backup and Recovery"](#).

Task 1: Prepare Your Host

Prepare your host for the change by removing instances from OracleAS Clusters and stopping all processes:

1. If the host contains a middle-tier instance that is part of an OracleAS Cluster, then remove the instance from the OracleAS Cluster. You can add the instance back into the cluster at the end of the procedure.

See Also: *Oracle Application Server High Availability Guide* for instructions on removing instances from an OracleAS Cluster

2. If the host contains an instance that stores the file-based repository used by an OracleAS File-Based farm, you must remove all instances from that farm, even if they reside on other hosts. This is because the repository ID will change when you change the hostname. As a result, you must remove all instances from the farm, change the hostname (which will change the repository ID), then add the instances back to the farm at the end of this procedure using the new repository ID.

To remove an instance from an OracleAS File-Based Farm, run the following command in the instance Oracle home:

- On UNIX systems:

```
ORACLE_HOME/dcm/bin/dcmctl leavefarm
```

- On Windows systems:

```
ORACLE_HOME\dcm\bin\dcmctl leavefarm
```

3. If the host contains a J2EE and Web Cache instance that is part of an OracleAS File-Based Farm (that uses a repository on another host) or an OracleAS Database-Based Farm, then remove the instance from the farm:
 - On UNIX systems:

```
ORACLE_HOME/dcm/bin/dcmctl leavefarm
```

- On Windows systems:

```
ORACLE_HOME\dcm\bin\dcmctl leavefarm
```

You can add the instance back to the farm at the end of the procedure.

4. If the host contains a middle-tier instance that is part of an OracleAS Web Cache cluster, then remove the instance from the cache cluster. You can add the instance back into the cache cluster at the end of the procedure.

See Also: *Oracle Application Server Web Cache Administrator's Guide* for instructions on removing caches from a cache cluster

5. Shut down each middle-tier instance on the host by running the following commands in each Oracle home:

- On UNIX systems:

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
```

- On Windows systems:

```
ORACLE_HOME\bin\emctl stop iasconsole
ORACLE_HOME\opmn\bin\opmnctl stopall
```

6. If the middle-tier instance was part of an OracleAS File-Based Farm, then ensure the DCM daemon is running in the file-based repository instance. This applies whether the repository instance is on the same host or a different host.

To verify if the DCM daemon is running, then run the following command in the file-based repository Oracle home:

- On UNIX systems:

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

- On Windows systems:

```
ORACLE_HOME\opmn\bin\opmnctl status
```

To start the DCM daemon:

- On UNIX systems:

```
ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=dcm-daemon
```

- On Windows systems:

```
ORACLE_HOME\opmn\bin\opmnctl startproc ias-component=dcm-daemon
```

7. Ensure Oracle Application Server processes will not start automatically after restarting the host by disabling any automated startup scripts you may have set up, such as `/etc/init.d` scripts.
8. Ensure the Oracle Internet Directory that is used by the middle-tier is running.

Task 2: Change the Hostname

Update your operating system with the new hostname, domain name, or both. Consult your operating system documentation for more information about how to perform the following steps. You can also change the IP address, if desired.

1. Make the updates to your operating system to properly change the hostname, domain name, or both.
2. Restart the host, if necessary for your operating system.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new hostname to ensure everything is resolving properly.

Task 3: Run the `chgiphost` Command

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. Ensure your `ORACLE_HOME` environment variable is set to the middle-tier Oracle home.
3. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, `LIB_PATH`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1–1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.
4. Run the following commands in the middle-tier Oracle home:

- On UNIX systems:

```
cd ORACLE_HOME/chgip/scripts
./chgiphost.sh -mid
```

- On Windows systems:

```
cd ORACLE_HOME\chgip\scripts
cmd /c chgiphost.bat -mid
```

The `chgiphost` command prompts for information, as shown in [Table 6–2](#). Note that the prompts may provide values in parentheses. You can enter a different value, or press the return key to accept the suggested value.

Table 6–2 Prompts and Actions for `chgiphost -mid`

Prompt	Action
Enter fully qualified hostname (hostname.domainname) of destination	Enter the new fully-qualified hostname. This may be a new hostname, domain name, or both.
Enter valid IP Address of destination	If you changed the IP address of the host, then enter the new IP address. Otherwise, enter the current IP address.
Enter valid IP Address of source	If you changed the IP address of the host, then enter the old IP address. Otherwise, enter the current IP address.
OIDAdmin Password:	Enter the <code>cn=orcladmin</code> password for the Oracle Internet Directory in which this middle-tier instance is registered.

5. Verify that the tool ran successfully by checking for errors in the files in the following directory:
 - On UNIX systems:


```
ORACLE_HOME/chgip/log
```
 - On Windows systems:

```
ORACLE_HOME\chgip\log
```

Task 4: Restart Your Environment

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:

- On UNIX systems:

```
ORACLE_HOME/opmn/bin/opmnctl startall  
ORACLE_HOME/bin/emctl start iasconsole
```

- On Windows systems:

```
ORACLE_HOME\opmn\bin\opmnctl startall  
ORACLE_HOME\bin\emctl start iasconsole
```

2. If you removed any instances from an OracleAS Web Cache cluster at the beginning of this procedure, then 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

3. If the host contained an instance that stored the file-based repository used by an OracleAS File-Based farm:

- a. Obtain the new repository ID for the new farm by running the following command in the Oracle home of that instance:

On UNIX systems:

```
ORACLE_HOME/dcm/bin/dcmctl getRepositoryID
```

On Windows systems:

```
ORACLE_HOME\dcm\bin\dcmctl getRepositoryID
```

- b. Recreate the OracleAS File-Based Farm by adding that instance to the new farm using the new repository ID obtained in the preceding step. The `repository_ID` is of the form `hostname:port`.

On UNIX systems:

```
ORACLE_HOME/dcm/bin/dcmctl joinfarm -r repository_ID
```

On Windows systems:

```
ORACLE_HOME\dcm\bin\dcmctl joinfarm -r repository_ID
```

- c. Add all instances on other hosts back to the new farm using the command in the preceding step.

4. If you removed any J2EE and Web Cache instances from an OracleAS File-Based Farm (that uses a repository on another host) at the beginning of this procedure, then add each one back as follows:

- On UNIX systems:

```
ORACLE_HOME/dcm/bin/dcmctl joinfarm -r repository_ID
```

- On Windows systems:

```
ORACLE_HOME\dcm\bin\dcmctl joinfarm -r repository_ID
```

In the preceding command, *repository_ID* is the hostname:port value returned by running the following command in the file-based repository Oracle home:

- On UNIX systems:

```
ORACLE_HOME/dcm/bin/dcmctl getRepositoryID
```

- On Windows systems:

```
ORACLE_HOME\dcm\bin\dcmctl getRepositoryID
```

5. If you removed any J2EE and Web Cache instances from an OracleAS Database-based Farm at the beginning of this procedure, then add each one back as follows:

- On UNIX systems:

```
ORACLE_HOME/dcm/bin/dcmctl joinfarm
```

- On Windows systems:

```
ORACLE_HOME\dcm\bin\dcmctl joinfarm
```

6. If you removed any instances from an OracleAS Cluster at the beginning of this procedure, then add them back to the cluster.

See Also: *Oracle Application Server High Availability Guide* for instructions on adding instances to an OracleAS Cluster

7. If you disabled any processes for automatically starting Oracle Application Server at the beginning of this procedure, then enable them.

Task 5: Update OracleAS Portal, OracleAS Wireless, OracleAS Single Sign-On, and Oracle Ultra Search

You must update OracleAS Portal, OracleAS Wireless, OracleAS Single Sign-On, and Oracle Ultra Search when you change the hostname.

1. Update OracleAS Portal with the new OracleAS Wireless service URL.

If you change the hostname, the OracleAS Wireless server URL will also change to use this new hostname. Therefore, you must update OracleAS Portal with the new OracleAS Wireless service URL. For more information, refer to "Updating the OracleAS Wireless Portal Service URL Reference" in *Oracle Application Server Portal Configuration Guide*.

2. Update OracleAS Single Sign-On (SSO) server with the new OracleAS Wireless SSO Partner URL.

If you change the hostname, the OracleAS Wireless SSO Partner URL uses the new hostname. Therefore, you must update OracleAS Single Sign-On with the new OracleAS Wireless SSO Partner URL.

Rather than manually changing the SSO settings, Oracle recommends that you re-register the OracleAS Wireless server with SSO using the following command line tool:

```
(UNIX) Oracle_Home/wireless/bin/reRegisterSSO.sh
(Windows) Oracle_Home\wireless\bin\reRegisterSSO.bat
```

This tool, which prompts you through the registration process, not only updates the OracleAS Wireless URL in the SSO server, but it also updates the SSO URL in the OracleAS Wireless server.

3. Re-register OracleAS Portal as an Oracle Ultra Search Content Source.

If you change the hostname, the OracleAS Portal URL will also change to use this new hostname. Therefore, you must update Oracle Ultra Search with the new OracleAS Portal URL. In Oracle Ultra Search, the OracleAS Portal URL is used to register OracleAS Portal as a crawlable content source. For more information, refer to "Registering OracleAS Portal as a Content Source" in *Oracle Application Server Portal Configuration Guide*.

Task 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, then the hostname is not automatically updated by running the `chgiphost` script. To update the hostname in such cases, you need to edit the files manually. For example, the `plsq1.conf` file may contain an NFS path including the hostname, such as: `/net/dsun1/private/...`

The `chgiphost` 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`

6.2.2 Changing the IP Address of an Infrastructure Containing a Metadata Repository

This section describes how to change the IP address of a host that contains either of the following Infrastructure installation types:

- Metadata Repository only
- Identity Management and Metadata Repository

The following sections describe the procedure:

- [Things to Know Before You Start](#)
- [Task 1: Shut Down Middle-Tier Instances](#)
- [Task 2: Prepare Your Host](#)
- [Task 3: Change the IP Address](#)
- [Task 4: Update the Infrastructure](#)
- [Task 5: Restart Your Environment](#)

Things to Know Before You Start

Review the following items before you start the procedure:

- Write down the old IP address before you begin. You will be prompted for this during the procedure.
- Oracle recommends that you perform a backup of your environment before you start this procedure. Refer to [Chapter 9, "Backup and Recovery"](#).

Task 1: Shut Down Middle-Tier Instances

Shut down all middle-tier instances that use the Infrastructure installation, even if they are on other hosts, using Application Server Control Console.

Task 2: Prepare Your Host

Prepare your host for the change by stopping all processes.

1. Set the `ORACLE_HOME` and `ORACLE_SID` environment variables.
2. Shut down the Infrastructure:

- On UNIX systems:

```
ORACLE_HOME/bin/emctl stop iasconsole
ORACLE_HOME/opmn/bin/opmnctl stopall
```

- On Windows Systems:

```
ORACLE_HOME\bin\emctl stop iasconsole
ORACLE_HOME\opmn\bin\opmnctl stopall
```

Shut down the listener and database:

```
lsnrctl stop
```

```
sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
```

3. Verify that all Oracle Application Server processes have stopped.
4. Ensure Oracle Application Server processes will not start automatically after a restarting the host by disabling any automated startup scripts you may have set up, such as `/etc/init.d` scripts.

Task 3: Change the IP Address

Update your operating system with the new IP address, restart the host, and verify that the host is functioning properly on your network. Consult your operating system documentation for more information about how to do this.

1. Make the updates to your operating system to properly change the IP address.
2. Restart the host, if required by your operating system.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new IP address to ensure everything is resolving properly.

Task 4: Update the Infrastructure

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. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, `LIB_PATH`, or `SHLIB_PATH` environment variables to the proper values, as shown in [Table 1-1](#). The actual environment variables and values that you have to set depend on the type of your UNIX operating system.

4. Start the database and listener:

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

```
lsnrctl start
```

5. Start OPMN:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl start
(Windows) ORACLE_HOME\opmn\bin\opmnctl start
```

6. Start Oracle Internet Directory:

```
(UNIX) ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=OID
process-type=OID
(Windows) ORACLE_HOME\opmn\bin\opmnctl startproc ias-component=OID
process-type=OID
```

7. Run the following commands in the Infrastructure Oracle home:

```
(UNIX)
cd ORACLE_HOME/chgip/scripts
./chgiphost.sh -infra
```

```
(Windows)
cd ORACLE_HOME\chgip\scripts
cmd /c chgiphost.bat -infra
```

The `chgiphost` command prompts for the old and new IP address.

8. Verify that the tool ran successfully by checking for errors in the files in the following directory:

```
(UNIX) ORACLE_HOME/chgip/log
(Windows) ORACLE_HOME\chgip\log
```

Task 5: Restart Your Environment

Start the remaining components of the Infrastructure and start any middle-tier instances that use it:

1. Start the Infrastructure:

- On UNIX systems:

```
ORACLE_HOME/opmn/bin/opmnctl startall
ORACLE_HOME/bin/emctl start iasconsole
```

- On Windows Systems:

```
ORACLE_HOME\opmn\bin\opmnctl startall
ORACLE_HOME\bin\emctl start iasconsole
```

2. If a middle-tier instance is on the same host as the Infrastructure, then you need to run the `chgiphost` command on the middle-tier instance before restarting the middle-tier processes.

3. If you disabled any processes for automatically starting Oracle Application Server at the beginning of this procedure, enable them.

6.2.3 Special Topics for Changing Your Hostname or Domain Name

This section contains the following special topics that apply to changing the hostname or domain name of an Oracle Application Server host:

- [Setting the Log Level for chgiphost](#)
- [Customizing the chgiphost Script](#)
- [Changing your Hostname after Upgrading from Windows 2000 to Windows 2003](#)
- [Recovering from Errors When Changing Your Hostname](#)

6.2.3.1 Setting the Log Level for chgiphost

By default, the console log level for the `chgiphost` command is SEVERE. This causes only critical information to be printed while running `chgiphost`. If you would like to view additional progress information, then set the console log level to CONFIG as follows:

1. Edit the following file:

```
(UNIX) ORACLE_HOME/chgip/config/chgip.log.properties
(Windows) ORACLE_HOME\chgip\config\chgip.log.properties
```

2. Change the `java.util.logging.ConsoleHandler.level` parameter to CONFIG:

```
java.util.logging.ConsoleHandler.level = CONFIG
```

6.2.3.2 Customizing the chgiphost Script

By default, the `chgiphost` script updates key configuration files in the Oracle home with the new hostname. If any of the following cases apply to your installation, then you may want to consider customizing the behavior of the `chgiphost` script:

- You have created additional configuration files that contain the hostname and would like the `chgiphost` script to update those files.

To update these files, add their full path name to the following file before running `chgiphost`:

```
(UNIX) ORACLE_HOME/chgip/config/hostname.lst
(Windows) ORACLE_HOME\chgip\config\hostname.lst
```

- Your old hostname is very short (one or two letters) or is a string that is likely to appear in a configuration file

Before running `chgiphost`, examine each of the files listed in `hostname.lst` to determine if the old hostname exists in any settings in those files. If you find a match, then you can correct those settings after you run `chgiphost`.

- Your Oracle home contains the hostname in its full path.

In this case, the `chgiphost` script may not update your configuration files properly. You can avoid this problem by using a Java utility called `FileFixer`, which searches for specific text strings in a file by matching regular expressions, and updates them to their new values. Note that `FileFixer` searches for patterns one line at a time. It cannot match patterns across lines.

To use `FileFixer`:

1. Make a copy of the following file:
 - On UNIX systems:
`ORACLE_HOME/chgip/config/hostname_short_sample.lst.xml`
 - On Windows systems:
`ORACLE_HOME\chgip\config\hostname_short_sample.lst.xml`
2. Edit your copy of the file to specify the regular expression matching required for your old and new hostnames. The file contains an example of how to do this.
3. Specify the file when running the `chgiphost` script. For example, on UNIX:
`./chgiphost option -hostnameShortXml full_path_to_your_xml_file`

For example, if you named your file `/mydir/my_sample.lst.xml`, and you are updating a middle-tier installation on UNIX, then run `chgiphost` as follows:

```
./chgiphost -mid -hostnameShortXml /mydir/my_sample.lst.xml
```

6.2.3.3 Changing your Hostname after Upgrading from Windows 2000 to Windows 2003

When you upgrade from Windows 2000 to Windows 2003, lower-case letters in your hostname may be changed to upper-case letters. For example, if your hostname is `myhost` before the upgrade, then it may be changed to `MYHOST`. If this occurs, then some Oracle Application Server processes may not function properly.

To resolve this problem, you do not need to run the `chgiphost` command to update Oracle Application Server. You can simply add an entry with the lower-case hostname to the hosts file:

```
OS_path\system32\drivers\etc\hosts
```

For example, if your fully-qualified hostname was `myhost.mydomain` before the upgrade, and your IP address is `1.2.3.4`, then add the following line:

```
1.2.3.4 myhost.mydomain myhost
```

6.2.3.4 Recovering from Errors When Changing Your Hostname

This section describes how to recover from typical errors you might encounter when using the `chgiphost` 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` script but specified the wrong destination name. In this case, you can remedy the error by running `chgiphost` 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`

For example, you will get an error message if you enter the wrong password for Oracle Internet Directory. In this case, you should run `chgiphost` again, with the same source and destination hostnames as before, and ensure to supply the correct password when prompted.

If you encounter an error when running `chgiphost`, then you should fix the error and run `chgiphost` again.

6.3 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 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.
- A loopback adapter is required for all off-network installations (DHCP or static IP). Refer to Oracle Application Server Installation Guide for more information.

6.3.1 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. No updates to Oracle Application Server are required.

6.3.2 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.

To move onto the network, connect the host to the network using DHCP and configure the hostname to the loopback IP address only.

6.3.3 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.

6.3.4 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.

6.4 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 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.

6.4.1 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. There is no need to update Oracle Application Server.

6.4.2 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. There is no need to update Oracle Application Server.

Enabling SSL

This chapter provides instructions for enabling Secure Sockets Layer (SSL) in Oracle Application Server on Infrastructure and middle-tier installations. It contains the following topics:

- [Overview of SSL](#)
- [Using the SSL Configuration Tool](#)
- [SSL Communication Paths in the Infrastructure](#)
- [Common SSL Configuration Tasks for the Infrastructure](#)
- [SSL Communication Paths in the Middle Tier](#)
- [Common SSL Configuration Tasks for the Middle Tier](#)

7.1 Overview of SSL

In Oracle Application Server, components send requests to and receive responses from other components. These components can be Oracle Application Server components (such as OracleAS Single Sign-On, OracleAS Web Cache, or Oracle HTTP Server) or external clients such as browsers.

To secure these communications, you can configure Oracle Application Server to use SSL, which is an industry standard for securing communications. Oracle Application Server supports SSL versions 2 and 3, as well as TLS version 1.

SSL secures communication by providing message encryption, integrity, and authentication. The SSL standard allows the involved components (such as browsers and HTTP servers) to negotiate which encryption, authentication, and integrity mechanisms to use.

7.2 Using the SSL Configuration Tool

The SSL Configuration Tool is designed to be run after a successful Oracle Application Server installation to automate many of the manual steps currently required for securing HTTP. You use the tool after all Oracle homes you plan to install are successfully installed. If you have a topology where both an OracleAS Infrastructure and middle tier are present, be sure to run the SSL Configuration Tool against the OracleAS Infrastructure first, then the middle tier.

Note: The SSL Configuration Tool is only supported for Oracle Application Server 10g Release 2 (10.1.2.0.2).

If you install Oracle Application Server and choose to make some configuration changes before running the SSL Configuration Tool, you should run the tool and then refer to the SSL Configuration Tool log files to verify that your changes were not overwritten. The SSL Configuration Tool creates log files in the directory from which the tool is run. A new log file is created each time the tool is run. For these reasons, it is suggested that you create a separate directory from which you can run the SSL Configuration Tool.

If you encounter any problems, you should run the SSL Configuration Tool with the `-rollback` option to revert back to your configuration environment prior to running the tool.

The SSL Configuration Tool is available with any Oracle Application Server installation type. OracleAS Infrastructure installations are the only installation type that support SSL configuration during the installation. This option is available on one of the installation screens. See *Oracle Application Server Installation Guide* for more information.

Note: OracleAS Web Cache is the only standalone type supported by the SSL Configuration Tool. All other standalone types (for example, Apache) are not supported.

In some cases, the SSL Configuration Tool cannot completely configure SSL for your specific topology. When this occurs, you should refer to the appropriate component documentation for instructions on how to complete your SSL configuration manually. For some links to documentation containing manual steps, see Chapter 14, "Using the SSL Configuration Tool" in the *Oracle Application Server Administrator's Guide*.

7.2.1 Command Line Interface

This section describes how to use the `SSLConfigTool` command. It contains the following sections:

- [Where Can I Find the SSL Configuration Tool?](#)
- [Syntax](#)

7.2.1.1 Where Can I Find the SSL Configuration Tool?

The `SSLConfigTool` executable is located in the `ORACLE_HOME/bin` directory.

7.2.1.2 Syntax

The `SSLConfigTool` command is used as follows:

```
SSLConfigTool ( -config_w_prompt
                | -config_w_file <input_file_name>
                | -config_w_default
                | -rollback )
                [-dry_run]
                [-wc_for_infra]
                [-secure_admin]
                [-opwd <orcladmin_pwd>]
                [-ptl_dad <dad_name>]
                [-ptl_inv_pwd <ptl_inv_pwd>]
```

[Table 7-1](#) describes the command line options for the `SSLConfigTool` command.

Table 7-1 SSL Configuration Tool Command Line Options

Parameter	Description
<code>-config_w_prompt</code>	Run in interactive mode.
<code>-config_w_file <input_file_name></code>	Run in silent mode using the values specified in the <code><input_file_name></code> file. This input file should be an XML file.
<code>-config_w_default</code>	Run in silent mode using the values specified in the <code>portlist.ini</code> and <code>ias.properties</code> files.
<code>-rollback</code>	Revert to the prior state before the command was last run. SSO registration will be done using virtual host and port.
<code>-dry_run</code>	Print the steps without implementing them.
<code>-wc_for_infra</code>	Forces an OracleAS Web Cache to be used as a load balancer for an infrastructure environment.
<code>-secure_admin</code>	Secure the OracleAS Web Cache and Enterprise Manager administration ports (the ports used to display Application Server Control Console)
<code>-opwd <orcladmin_pwd></code>	Set the Oracle administrator password. This parameter is required.
<code>-ptl_dad <dad-name></code>	Set the Portal dad name. If no name is specified, the default portal will be used.
<code>-ptl_inv_pwd <ptl_inv_pwd></code>	Set the Portal invalidation password used to send invalidation to OracleAS Web Cache. This parameter is required if you installed OracleAS Portal. If you are running <code>SSLConfigTool</code> with the <code>-rollback</code> parameter, this parameter is not required.

Note that the `-config_w_prompt`, `-config_w_file`, `-config_w_default`, and `-rollback` parameters are mutually exclusive; only one can be used with the `SSLConfigTool` command.

If you choose to run the tool interactively with the `-config_w_prompt` parameter, you will be prompted for the appropriate information one question at a time.

If you choose to run the tool silently by specifying a configuration file with the `-config_w_file` parameter, you should read Section 14.4.3, "Configuration File for Silent Mode" in the *Oracle Application Server Administrator's Guide*.

7.3 SSL Communication Paths in the Infrastructure

This section identifies all the SSL communication paths used in the Oracle Application Server Infrastructure, and provides cross-references to the configuration instructions in component guides in the Oracle Application Server documentation library.

Note: When you install Identity Management, you are prompted to select a mode for Oracle Internet Directory. The default mode is the dual mode, which allows some components to access Oracle Internet Directory using non-SSL connections. If you chose SSL mode during installation, then all installed components must use SSL when connecting to the directory.

Before you begin SSL configuration, determine the Oracle Internet Directory mode. Start the `oidadmin` tool and view the SSL mode in Oracle Directory Manager. Navigate to the Directory Server and select **View Properties** and then **SSL Settings**.

The following lists the communication paths through the Oracle Application Server Infrastructure, and the related SSL configuration instructions:

- **Oracle HTTP Server to the OC4J_SECURITY instance**

To configure AJP communication over SSL, you must configure how `mod_oc4j` communicates with the `iaspt` daemon. To do this, follow the instructions in the *Oracle HTTP Server Administrator's Guide*, the section titled "Configuring `mod_oc4j` to Use SSL."

- **Oracle HTTP Server to `iaspt` (Port Tunneling) and then to the OC4J_SECURITY instance**

To configure this connection path for SSL, follow the instructions in the *Oracle HTTP Server Administrator's Guide*, the section titled "Understanding Port Tunneling."

- **OC4J_SECURITY instance to Oracle Internet Directory**

To configure this connection path for SSL, follow the instructions in the *Oracle Application Server Single Sign-On Administrator's Guide*. It explains how to configure SSL communication between the browser and the OracleAS Single Sign-On server (section titled "Enable SSL on the Single Sign-On Middle Tier").

Oracle Delegated Administration Services is SSL-enabled after you configure the Oracle HTTP Server for SSL. The Oracle Delegated Administration Services communication to Oracle Internet Directory is always SSL-enabled; you do not have to perform any configuration tasks to accomplish this. (OracleAS Single Sign-On, Oracle Application Server Certificate Authority, and Oracle Delegated Administration Services communicate with Oracle Internet Directory in SSL mode by default.)

- **Oracle Directory Integration and Provisioning to Oracle Internet Directory and Oracle Internet Directory replication server to Oracle Internet Directory**

As shown in [Figure 7-1](#), you can configure several components and communication paths for SSL. The following lists references to the instructions for each:

- Communication between the Oracle Internet Directory Replication server and the Oracle Internet Directory server: *Oracle Application Server High Availability Guide*, section titled "Secure Sockets Layer (SSL) and Oracle Internet Directory Replication"
- Communication between Oracle Directory Integration and Provisioning and the Oracle Internet Directory server: *Oracle Identity Management Integration Guide*, chapter titled "Oracle Directory Integration and Provisioning Server Administration"

- The OC4J_SECURITY instance to the Metadata Repository database and Oracle Internet Directory to the Metadata Repository database**

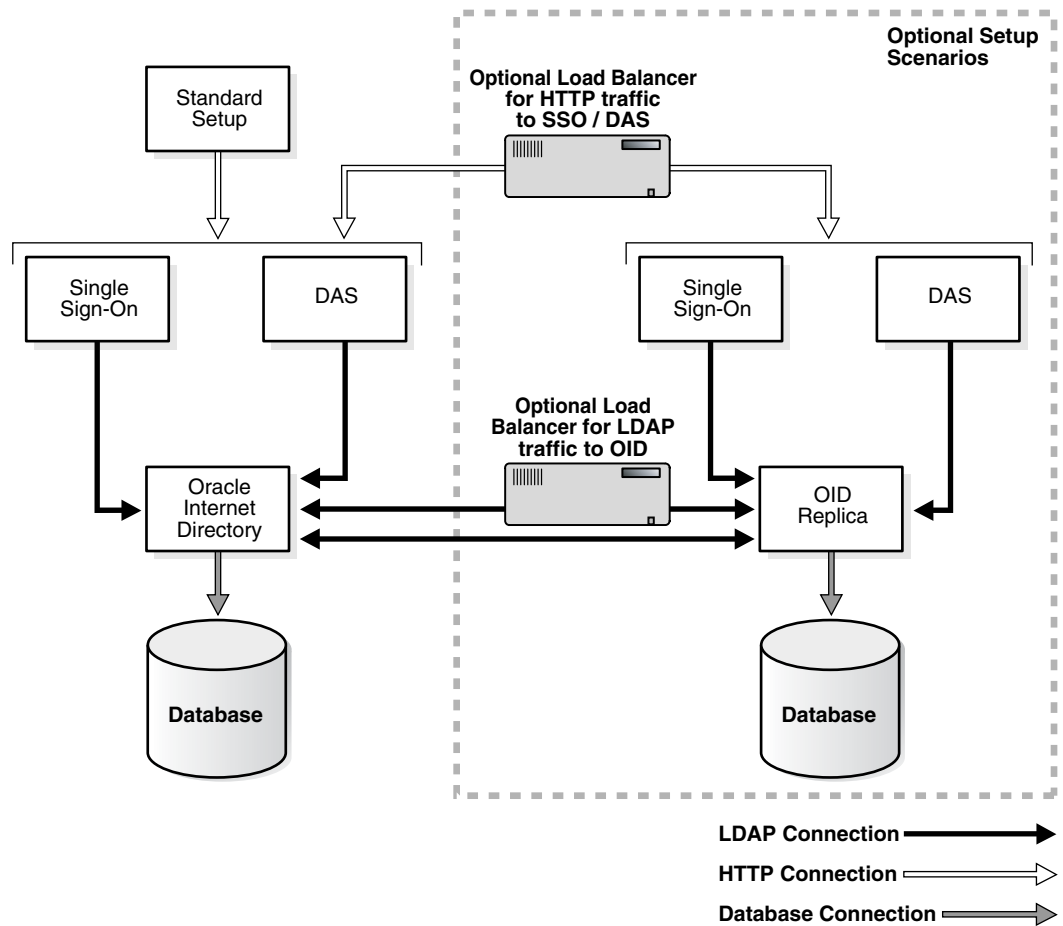
If Oracle Internet Directory is configured to accept SSL connections on the SSL port specified, then you need to specify only the SSL protocol and SSL port in the JDBC URL requesting an application, as follows:

ldaps://host:sslport/...

Note that when you are using a secure connection, you must add an *s* to the name of the protocol. For example, use *ldaps* instead of *ldap*.

If Oracle Internet Directory is not configured to accept SSL connections on the SSL port, then you must modify the configuration. Refer to the section titled "Secure Sockets Layer (SSL) and the Directory" in the *Oracle Internet Directory Administrator's Guide*.

Figure 7-1 Identity Management Components and SSL Connection Paths



7.4 Common SSL Configuration Tasks for the Infrastructure

This section provides references to the component guides in the Oracle Application Server documentation library that provide instructions for configuring SSL in individual components.

7.4.1 Configuring SSL for OracleAS Single Sign-On and Oracle Delegated Administration Services

Follow the instructions in the *Oracle Application Server Single Sign-On Administrator's Guide* to configure SSL communication between:

- The browser and the OracleAS Single Sign-On server (section titled "Enable SSL on the Single Sign-On Middle Tier")
- The OracleAS Single Sign-On server and the Oracle Internet Directory server (section titled "Configuring SSL Between the Single Sign-On Server and Oracle Internet Directory")

Oracle Delegated Administration Services is SSL-enabled after you configure the Oracle HTTP Server for SSL (as described in "Enable SSL on the Single Sign-On Middle Tier"). The Oracle Delegated Administration Services communication to Oracle Internet Directory is always SSL-enabled. You do not have to perform any configuration tasks to accomplish this.

7.4.2 Configuring SSL for Oracle Internet Directory

Instructions for configuring SSL communication in Oracle Internet Directory are provided in the following guides:

- *Oracle Internet Directory Administrator's Guide*, the section titled "Secure Sockets Layer (SSL) and the Directory"
- *Oracle Internet Directory Administrator's Guide*, the section titled "Configuring SSL Parameters"
- *Oracle Internet Directory Administrator's Guide*, the section titled "Limitations of the Use of SSL in 10g (10.1.2)"

7.4.3 Configuring SSL for Oracle Internet Directory Replication Server and Oracle Directory Integration and Provisioning

As shown in [Figure 7-1](#), you can configure several components and communication paths for SSL. The following lists references to the instructions for each:

- Communication between the Oracle Internet Directory Replication server and the Oracle Internet Directory server: *Oracle Application Server High Availability Guide*, section titled "Secure Sockets Layer (SSL) and Oracle Internet Directory Replication"
- Communication between Oracle Directory Integration and Provisioning and the Oracle Internet Directory server: *Oracle Identity Management Integration Guide*, chapter titled "Oracle Directory Integration and Provisioning Server Administration"

7.4.4 Configuring SSL in the Identity Management Database

Follow the instructions in the *Oracle Application Server Single Sign-On Administrator's Guide*, in the section titled "Reconfigure the Identity Management Infrastructure Database" to configure SSL in the Identity Management database.

7.5 SSL Communication Paths in the Middle Tier

This section identifies all SSL communication paths used in the Oracle Application Server middle-tier installation types, and provides cross-references to the

configuration instructions in component guides in the Oracle Application Server documentation library.

The following lists the communication paths through the Oracle Application Server middle tier, and the related SSL configuration instructions:

- **External Clients or Load Balancer to Oracle HTTP Server**

To configure the Oracle HTTP Server for SSL, follow the instructions in the *Oracle HTTP Server Administrator's Guide*, section titled "Enabling SSL."

- **External Clients or Load Balancer to OracleAS Web Cache**

To configure OracleAS Web Cache for SSL, follow the instructions in "Configuring OracleAS Web Cache for HTTPS Requests" in the *Oracle Application Server Web Cache Administrator's Guide*.

- **OracleAS Web Cache to Oracle HTTP Server**

To configure OracleAS Web Cache for SSL, follow the instructions in "Configuring OracleAS Web Cache for HTTPS Requests" in the *Oracle Application Server Web Cache Administrator's Guide*.

- **Oracle HTTP Server to OC4J Applications (AJP)**

To configure the AJP communication over SSL, you must configure mod_oc4j's communication with the `iaspt` daemon. To do this, follow the instructions in the *Oracle HTTP Server Administrator's Guide*, section titled "Configuring mod_oc4j to Use SSL."

- **Oracle HTTP Server to `iaspt` and then to OC4J**

To configure this connection path for SSL, follow the instructions in the *Oracle HTTP Server Administrator's Guide*, section titled "Understanding Port Tunneling."

- **OC4J (the JAAS provider) to Oracle Internet Directory**

To configure the provider, follow the instructions in the *Oracle Application Server Containers for J2EE Security Guide*. To configure the provider for SSL, set the `SSL_ONLY_FLAG` to `true`.

- **OC4J to the database (ASO)**

If Oracle Internet Directory configured to accept SSL connections on the SSL port specified, you need only specify the SSL protocol and SSL port in the JDBC URL requesting an application, as follows:

```
ldaps://host:sslport/...
```

Note that when you are using a secure connection, you must add an `s` to the name of the protocol. For example, use `ldaps` instead of `ldap`.

If Oracle Internet Directory is not configured to accept SSL connections on the SSL port, you must modify the configuration. See *Oracle Internet Directory Administrator's Guide*, section titled "Secure Sockets Layer (SSL) and the Directory."

- **ORMI (Oracle Remote Method Invocation, a custom wire protocol) over HTTP and HTTP over SSL**

ORMI over SSL is not supported. To configure similar functionality, you can configure ORMI over HTTP, and then configure HTTP for SSL.

See the *Oracle Application Server Containers for J2EE Services Guide*, section titled "Configuring ORMI Tunnelling Through HTTP" for instructions on how to configure ORMI/HTTP.

- **SSL into standalone OC4J (HTTPS)**

To configure this connection path for SSL, follow the instructions in the *Oracle Application Server Containers for J2EE Security Guide*, section titled "Configuring SSL in OC4J" explains how to use SSL to secure communication between clients and an OC4J instance.

- **OracleAS Portal Parallel Page Engine (the servlet in the OC4J_PORTAL instance) to OracleAS Web Cache (HTTPS)**

To configure this connection path for SSL, follow the instructions in the *Oracle Application Server Containers for J2EE Security Guide*, section titled "Configuring SSL in OC4J."

7.6 Common SSL Configuration Tasks for the Middle Tier

This section identifies some commonly used SSL configurations in the Oracle Application Server middle-tier installation types, and provides cross-references to the configuration instructions in component guides in the Oracle Application Server documentation library.

7.6.1 Enabling SSL in OracleAS Web Cache

OracleAS Web Cache is part of all Oracle Application Server middle-tier installations. To configure it for SSL, follow the instructions in chapter "Configuring OracleAS Web Cache for HTTPS Requests" in the *Oracle Application Server Web Cache Administrator's Guide*.

A script, `SSLConfigTool`, automates the SSL configuration of the following:

- HTTPS listening ports and wallet location for the cache
- HTTPS operations ports for the cache
- Site for HTTPS requests
- HTTPS port and wallet location for the origin server
- Site-to-server mapping

For instructions on using this script, see Chapter 14, "Using the SSL Configuration Tool" in the *Oracle Application Server Administrator's Guide*.

7.6.2 Enabling SSL in the Oracle HTTP Server

Oracle HTTP Server is part of all Oracle Application Server middle-tier installations. To configure Oracle HTTP Server for SSL, follow the instructions in the *Oracle HTTP Server Administrator's Guide*, the section titled "Enabling SSL."

A script, `SSLConfigTool`, automates the setting of the SSL parameters in the `httpd.conf` file. For more information about this script, see Chapter 14, "Using the SSL Configuration Tool" in the *Oracle Application Server Administrator's Guide*.

7.6.3 Enabling SSL in Oracle Application Server Containers for J2EE (OC4J)

To configure SSL connections to OC4J clients, follow the instructions in the *Oracle Application Server Containers for J2EE Security Guide* section titled "Oracle HTTPS for Client Connections."

7.6.4 Enabling SSL in J2EE and Web Cache Installations

Depending on your security needs and the configuration of the Oracle Application Server J2EE and Web Cache installation, you may implement secure communication in one or more of the installed components. Configuring the first listener (whether it is OracleAS Web Cache or the Oracle HTTP Server) may be sufficient.

To configure the Oracle HTTP Server for SSL, follow the steps in "Enabling SSL for Oracle HTTP Server" in the *Oracle HTTP Server Administrator's Guide*.

To configure OracleAS Web Cache for SSL, follow the instructions in "Configuring OracleAS Web Cache for HTTPS Requests" in the *Oracle Application Server Web Cache Administrator's Guide*.

A script called `SSLConfigTool` is provided to automate some of the configuration tasks. For instructions on using this script, see Chapter 14, "Using the SSL Configuration Tool" in the *Oracle Application Server Administrator's Guide*.

7.6.5 Enabling SSL in Virtual Hosts

You can use virtual hosts to deploy multiple Web sites on a single Oracle HTTP Server (for example, to make an application available over the HTTP protocol and the HTTPS protocol).

The *Oracle Application Server Single Sign-On Administrator's Guide*, section titled "Configuring mod_osso with Virtual Hosts" contains instructions on configuring an SSL virtual host to be protected by mod_osso. You cannot use name-based virtual hosting. You must use IP-based or port-based virtual hosting.

The scenario presented assumes that the following conditions are in effect:

- The host name of the application middle tier is `app.mydomain.com` (replace this name with the host name of your application middle tier).
- The middle tier is already configured as a non-SSL partner application (this is typically done during installation).
- The default SSL port number of the application middle tier is 4443.

7.6.6 Enabling SSL in OracleBI Discoverer

The *Oracle Business Intelligence Discoverer Configuration Guide* explains how to configure OracleBI Discoverer for SSL.

For a discussion of Oracle Application Server Framework Security, including the SSL protocols for Oracle Business Intelligence, refer to the *Oracle Business Intelligence Discoverer Configuration Guide*, the section titled "Using Discoverer with OracleAS Framework Security."

For information about implementing SSL in OracleBI Discoverer, refer to the *Oracle Business Intelligence Discoverer Configuration Guide*, the section titled "What is HTTPS and why should I use it?"

For instructions on enabling OracleBI Discoverer for SSL, refer to the *Oracle Business Intelligence Discoverer Configuration Guide*, the section titled "About running Discoverer over HTTPS."

7.6.7 Enabling SSL in OracleAS Wireless

For instructions on configuring SSL in OracleAS Wireless, refer to the Wireless Security chapter in the *Oracle Application Server Wireless Administrator's Guide*. The section titled

"Site Administration" explains how to use the System Manager HTTP, HTTPS configuration page in Oracle Enterprise Manager 10g to configure the Wireless site's proxy server settings, URLs, and SSL certificates in the Wireless site.

7.6.8 Enabling SSL in OracleAS Portal

OracleAS Portal uses several components for HTTP communication (such as the Parallel Page Engine, Oracle HTTP Server, and OracleAS Web Cache), each of which may function as a client or server. As a result, each component in the Oracle Application Server middle tier may be configured individually to use the HTTPS protocol instead of HTTP.

These components' interact with OracleAS Portal through the following distinct network hops:

- Between the client browser and the entry point of the OracleAS Portal environment. The entry point can be OracleAS Web Cache or a network edge hardware device such as a reverse proxy or SSL accelerator
- Between OracleAS Web Cache and the Oracle HTTP Server of the Oracle Application Server middle tier
- Between the client browser and the Oracle HTTP Server of the OracleAS Single Sign-On or Oracle Internet Directory (or Infrastructure) tier
- A loop back connection between the Parallel Page Engine (PPE) on the middle tier and OracleAS Web Cache or the front-end reverse proxy
- Between the Parallel Page Engine (PPE) and the Remote Web Provider that provides Portlet content
- Between the OracleAS Portal infrastructure and the Oracle Internet Directory server

The following sections in the *Oracle Application Server Portal Configuration Guide* provide an overview of the most common SSL configurations for OracleAS Portal and instructions for implementing them:

- **SSL to OracleAS Single Sign-On:** Follow the instructions in the *Oracle Application Server Portal Configuration Guide* to configure a secure connection to OracleAS Single Sign-On.
- **SSL to OracleAS Web Cache:** Follow the instructions in the *Oracle Application Server Portal Configuration Guide* to configure a secure connection to OracleAS Web Cache.
- **SSL throughout OracleAS Portal:** Follow the instructions in the *Oracle Application Server Portal Configuration Guide* to configure secure connections throughout OracleAS Portal.
- **External SSL with non-SSL within Oracle Application Server:** Follow the instructions in the *Oracle Application Server Portal Configuration Guide* to configure OracleAS Portal such that the site is externally accessible through SSL URLs, with the Oracle Application Server running in the non-SSL mode.

Note: For general information about securing OracleAS Portal, refer to the *Oracle Application Server Portal Configuration Guide* (the chapter about Securing OracleAS Portal).

7.6.9 Configuring SSL for Oracle Enterprise Manager 10g

To configure SSL for Oracle Enterprise Manager 10g, refer to the *Oracle Application Server Administrator's Guide*.

Cloning an Application Server Instance

This chapter provides information about cloning an Oracle Application Server installation. It contains the following topics:

- [Introduction to Cloning](#)
- [Procedure for Cloning](#)

8.1 Introduction to Cloning

Cloning is the process of copying an existing installation to a different location while preserving its configuration. Using cloning, you can create a new installation with all patches applied to it in a single step. This is in contrast to separately installing, configuring and applying any patches to Oracle Application Server. Some situations in which cloning is useful are:

- Creating an installation that is a copy of a production, test, or development installation.
- Rapidly deploying an instance and the applications it hosts.
- Preparing a "gold" image of a patched home and deploying it to many hosts.

The cloned installation behaves the same as the source installation. For example, the cloned instance can be deinstalled or patched using Oracle Universal Installer. It can also be used as the source for another cloning operation.

The cloning process works by copying all files from the source Oracle home to the destination Oracle home. Hence, any files used by the source instance that are located outside the source Oracle home's directory structure are not copied to the destination location.

After the files are copied, a set of scripts is used to update the information in key configuration files. For example, all references to the host name and the Oracle home in `httpd.conf` and `webcache.xml` are updated to their new values.

Any applications deployed in the source instance are also copied to the cloned instance and automatically deployed, provided they are located in the source Oracle home's directory structure.

8.1.1 Installation Types Supported

In this release, you can clone the following types of middle-tier installations:

- J2EE and Web Cache middle tier
- Portal and Wireless middle tier

- Business Intelligence and Forms middle tier

Note the following:

- You cannot clone the OracleAS Infrastructure itself. However, you can clone a middle tier that is connected to OracleAS Infrastructure, including OracleAS Metadata Repository and Oracle Identity Management.
- You cannot clone OracleAS Integration B2B, Oracle BPEL Process Analytics, or Oracle BPEL Process Manager.
- The cloned instance must have a different instance name than the source instance. You specify the instance name when you clone the instance, as described in [Section 8.2.3](#).
- You can clone a middle-tier instance that is a member of an OracleAS Cluster or farm. However, you must remove the instance from an OracleAS Cluster.

See Also: Chapter 10 of the *Oracle Application Server Administrator's Guide* for more information about supported installation types.

8.1.2 General Considerations and Limitations for Cloning

For this release, you cannot clone the following:

- OracleAS Infrastructure components (Oracle Identity Management and OracleAS Metadata Repository)
- Developer Kits, including Oracle Content Management SDK (Oracle CM SDK)
- Installations that include Oracle Application Server Integration B2B, Oracle BPEL Process Analytics, or Oracle BPEL Process Manager.
- Installations that include Oracle Application Server Integration InterConnect
- Adapters, including Oracle Application Server Adapters and Oracle Application Server Integration InterConnect Adapters
- Installations that include Oracle Workflow

Note the following important additional considerations about cloning:

- The user may need to update the security certificates to match the new host name.
- If an instance is part of an OracleAS Cluster, you must remove the instance from the cluster before performing the cloning operation.
- Cloning an Oracle Application Server middle tier that is connected to an OracleAS Infrastructure will result in a new Oracle Application Server middle tier connected to the same OracleAS Infrastructure as the source instance. To join a different OracleAS Infrastructure, you can reassociate the middle tier with a different OracleAS Infrastructure.
- If you have changed the default file permissions for configuration files, then those file permissions are not preserved by cloning.
- User customizations for the following components are not preserved. The status of these components are reset to the default:
 - Log Loader
 - Oracle Application Development Framework
 - Port tunneling
 - UIX

- XDK
- Cloning does not carry over all the dependencies of the source Oracle home, such as loadable modules or application-specific libraries to the cloned home, because cloning proceeds by copying the entire source Oracle home to the destination Oracle home. Any files outside the source Oracle home are not automatically copied. Hence, any applications that refer to files outside the source Oracle home may not work properly in the cloned home.
- If you created symbolic links to files or applications outside the source Oracle home (for example, to Oracle Wallet files that are not stored in the default location), then you must re-create the link manually in the cloned home for your applications to work properly.
- The cloning operation generates default ports for the cloned instance. To specify other ports, you can use the `staticports.ini` file. If you specify ports less than 1024 on UNIX, then the cloned instance will not start during the cloning operation. After the cloning process is completed, you must run the `root.sh` script with root privileges, then start the processes.
- The cloning process does not configure a Load Balancing Router to recognize the cloned instance. If you use a Load Balancing Router in your environment, then you must manually configure the Load Balancing Router, including any invalidation port.
- If a cloning operation fails, but it results in the Oracle home being registered with Oracle Inventory, you cannot use the same Oracle home in subsequent cloning operations. Either use another directory and name for the Oracle home in subsequent cloning operations or deinstall the Oracle home before attempting another cloning operation.

For important considerations for cloning individual components, see Chapter 10, "Cloning Application Server Instances" of the *Oracle Application Server Administrator's Guide*.

8.2 Procedure for Cloning

To clone an Oracle Application Server instance, you first prepare the source Oracle home. Then, you clone the destination.

8.2.1 Prerequisites for Cloning

For cloning, Perl 5.6.1 or higher must be installed on your system. Before running the cloning Perl scripts, you must set the `PERL5LIB` environment variable to the path of the Perl directory in the Oracle home. This path must be the first one listed in the variable definition. For example:

```
setenv PERL5LIB $Oracle_Home/perl/lib/5.6.1:$Oracle_Home/perl/lib/site_perl/5.6.1:$PERL5LIB
```

On Windows:

```
set PERL5LIB=%Oracle_Home%\perl\5.6.1\lib;%OH%\perl\5.6.1\lib\MSWin32-x86;%Oracle_Home%\perl\site\5.6.1\lib;%PERL5LIB%
```

8.2.2 Preparing the Source

To prepare the source Oracle home to be cloned, take the following steps at the source instance:

1. Change to the following directory:

- On UNIX systems:
`Oracle_Home/clone/bin`
 - On Windows systems:
`Oracle_Home\clone\bin`
2. Run the script `prepare_clone.pl`. This script prepares the source to be cloned. The command line for the script has the following format:

```
perl prepare_clone.pl [ORACLE_HOME=OH_dir]
                    [-oid_password OIDPassword]
                    [-oid_admin OIAdmin]
                    [-silent]
                    [-debug]
                    [-help]
```

Table 8–1 describes the parameters and options for the `prepare_clone.pl` script.

Table 8–1 Parameters and Options for the `prepare_clone.pl` Script

Parameter or Option	Description
ORACLE_HOME	The complete directory specification for the source Oracle home. If you do not supply this parameter, the script uses the ORACLE_HOME environment variable, if it exists. If the environment variable does not exist, the script assumes that ORACLE_HOME is the directory from which the script is being run. Use the value that was provided during installation; do not use symbolic links. If ORACLE_HOME is invalid, then the script exits and logs an error to the <code>error_timestamp.log</code> file.
-oid_password	The Oracle Internet Directory password. If the original installation required that the user specify an Oracle Internet Directory password (such as an instance connected to Oracle Identity Management), this option is required. If you do not supply the option, but one is needed, the script prompts the user for the password.
-oid_admin	The Oracle Internet Directory admin value. If you do not specify this option, the script uses a default value of <code>cn=orcladmin</code> .
-silent	Runs the script in silent mode. If the command line does not contain the required password-related options, the script exits.
-debug	Runs the script in debug mode.
-help	Prints the usage for the script.

3. Archive and compress the source Oracle home, using your preferred tool for archiving. For example, you can use WinZip on Windows and tar and gzip on UNIX. Ensure that the tool you are using preserves the permissions and timestamps of the files. The following example shows how to archive and compress the source on UNIX:

```
cd Source_Oracle_Home
tar cf - * | gzip > oracleas.tar.gz
```

Note that you should not use the `jar` utility to archive and compress the Oracle home.

8.2.3 Cloning the Instance

At the destination, to clone the source instance, take the following steps:

1. Copy the compressed Oracle home from the source machine to the destination machine.
2. Extract the compressed Oracle home into a directory, which will become the new Oracle home at the destination location. Use your preferred tool to extract the compressed files. For example, you can use WinZip on Windows and tar and gunzip on UNIX. Ensure that the tool you are using preserves the permissions and timestamps of the files. The following example shows how to extract the files on UNIX:

```
mkdir -p Destination_Oracle_Home
gunzip < Dir_Containing_Tar/oracleas.tar.gz | tar xf -
```

Note: Ensure that the tar and gzip/gunzip versions on the source and destination machines are compatible. You may encounter problems unzipping the archive if these versions differ.

3. Change to the following directory:
 - On UNIX systems:


```
Oracle_Home/clone/bin
```
 - On Windows systems:


```
Oracle_Home\clone\bin
```
4. Run the `clone.pl` script. You must have write permission to the directory containing the Oracle inventory file. (See [Section 8.2.4](#) for information about the location of the Oracle inventory directory.)

The command line for the script has the following format:

```
perl clone.pl ORACLE_HOME=OH_dir
              ORACLE_HOME_NAME=OH_Name
              -instance Instance_Name
              [-ias_admin_old_pwd Old_Ias_Admin_Password]
              [-ias_admin_new_pwd New_Ias_Admin_Password]
              [-oid_password OIDPassword]
              [-dcm_schema_pwd DCMPassword]
              [-lbr {true|false}]
              [-O string]
              [-silent]
              [-debug]
              [-help]
```

[Table 8–2](#) describes the parameters and options for the `clone.pl` script.

Table 8–2 Parameters and Options for the `clone.pl` Script

Parameter or Option	Description
ORACLE_HOME	Required. The complete directory specification for the destination Oracle home. This parameter is required. If you do not supply this parameter, or if the value is invalid, the script exits.
ORACLE_HOME_NAME	Required. The name for the destination Oracle home (the Oracle home of the clone.)

Table 8–2 (Cont.) Parameters and Options for the clone.pl Script

Parameter or Option	Description
-instance	Required. The instance name for the clone. The instance name must be different from the source instance and any other instances that use the same OracleAS Infrastructure or that are part of the same OracleAS Cluster or farm.
-ias_admin_old_pwd	Required. The administrator password for Oracle Application Server for the source instance. If you do not supply this option and the script is not running in silent mode, the script prompts the user for the password.
-ias_admin_new_pwd	Required. A new password for administrator for Oracle Application Server for the cloned instance. If you do not supply this option and the script is not running in silent mode, the script prompts the user for the password.
-oid_password	The Oracle Internet Directory password. If the original installation required that the user specify an Oracle Internet Directory password (such as an instance connected to Oracle Identity Management), then this option is required. If you do not supply this option, but one is needed, the script prompts the user for the password.
-dcm_schema_pwd	The Distributed Configuration Management (DCM) schema password. If the original installation required that the user specify a DCM schema password (such as a J2EE instance connected to a OracleAS Metadata Repository, but not to Oracle Identity Management), then this option is required. If you do not supply this option, but one is needed, the script prompts the user for the password.
-lbr	Whether or not a load balancer is used. The default is <code>true</code> . If you are cloning a Portal and Wireless instance and you specify <code>false</code> , the cloning process overwrites the configuration entries for the source instance, which are stored in the OracleAS Metadata Repository.
-O	Specifies that any text following the option is passed to the Oracle Universal Installer command line. For example, you can use this option to pass the location of the <code>oraparam.ini</code> file to be used by Oracle Universal Installer, by using the following code: <code>'-O-paramFile C:\OraHome_1\oui\oraparam.ini'</code> Note that if the text you want to pass contains spaces or other delimiting characters, you must enclose the option in double quotation marks ("").
-silent	Runs the script in silent mode. If the command line does not contain the required password-related options, the script exits.
-debug	Runs the script in debug mode.
-help	Prints the usage for the script.

For example:

```
perl clone.pl ORACLE_HOME=/opt/oracle/Ora_1012_B
              ORACLE_HOME_NAME=OH_1012_B
              -instance Portal_B
              -ias_admin_old_pwd my_old_ias_pass
              -ias_admin_new_pwd my_new_ias_pass
              -oid_password my_oidpwd
              -dcm_schema_pwd my_DCM_pass]
              -lbr true
              '-O-paramFile /var/opt/oracle/oui/oraparam.ini'
```


-silent

5. On UNIX, run the `root.sh` script in the cloned Oracle home so that the cloned instance works properly. The script is located in the cloned instance's Oracle home directory.

For example:

```
$ORACLE_HOME/root.sh
```

Now, the cloned instance's configuration is identical to that of the source instance. Application Server Control Console and OPMN are able to start and stop all processes in the cloned instance, including any OC4J custom instances. All applications deployed should be visible and able to run as expected.

8.2.4 Locating and Viewing Log Files

The cloning script invokes multiple tools, each of which generates its own log files. However, the following log files, which are generated by Oracle Universal Installer and the cloning scripts, are the key ones of interest for diagnostic purposes:

- `Oracle_inventory/logs/cloneActionstimestamp.log`: Contains a detailed log of the actions that occur during the Oracle Universal Installer part of the cloning.
- `Oracle_inventory/logs/oraInstalltimestamp.err`: Contains information about errors that occur when Oracle Universal Installer is running.
- `Oracle_inventory/logs/oraInstalltimestamp.out`: Contains other miscellaneous messages generated by Oracle Universal Installer.
- `Oracle_Home/clone/logs/clonetimestamp.log`: Contains a detailed log of the actions that occur during the precloning and cloning operations.
- `Oracle_Home/clone/logs/errorstimestamp.log`: Contains information about errors that occur during the precloning and cloning operations. In addition, it contains all messages written to standard error (STDERR) by the multiple tools that are invoked by the cloning script. Depending upon the tool, some of these messages may be informational messages or error messages.

The format of the path is shown in UNIX format. For Windows, invert the slashes.

Note: To find the location of the Oracle Inventory directory:

- On UNIX systems, look in `/var/opt/oracle/oraInst.loc` or `/etc/oraInst.loc`
 - On Windows systems, the location can be obtained from the registry: `HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\INST_LOC`
-

After the `clone.pl` script finishes running, consult these log files to get more information about the cloning process. To view the log files from Application Server Control Console, take the following steps:

1. Select **Logs** from the Home page.
2. In the View Logs page, select **ASClone** from the **Available Components** box. Click **Move** to move the selection to the **Selected Components** box.
3. Click **Search**.

The log files are displayed in the **Results** table.

4. To view the log, click the log name in the **Log File** column.

Backup and Recovery

This chapter describes how to configure and use the Oracle Application Server Backup and Recovery tool and how to backup your Oracle Application Server installation.

The OracleAS Backup and Recovery tool can be used in different ways, depending on your requirements. You can use the tool to perform configuration file and OracleAS Metadata Repository backup and recovery and also use it to set up your own configuration file and OracleAS Metadata Repository backup and recovery scripts.

This chapter contains the following topics:

- [Locating the OracleAS Backup and Recovery Tool](#)
- [Configuring the OracleAS Backup and Recovery Tool](#)
- [Customizing the Tool for Your Configuration Files](#)
- [OracleAS Backup and Recovery Tool Usage Summary](#)
- [Backup Procedures](#)

9.1 Locating the OracleAS Backup and Recovery Tool

The OracleAS Backup and Recovery Tool is installed as part of an Oracle Application Server installation. The tool is located in the *Oracle_Home/backup_restore* directory. [Table 9-1](#) lists the files that may reside in the *backup_restore* directory.

Table 9-1 OracleAS Backup and Recovery Tool Files

File ¹	Description
<code>bkp_restore.pl</code>	If you have installed OracleAS TopLink or REPCA, then run this Perl script.
<code>bkp_restore.sh</code>	A shell script used to run the Perl script on UNIX.
<code>bkp_restore.bat</code>	A batch command file used to run the Perl script on Windows.
<code>config/config.inp</code>	The main configuration file that contains parameters for customizing the tool for your environment
<code>config/config_component_files.inp</code>	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.

Table 9–1 (Cont.) OracleAS Backup and Recovery Tool Files

File ¹	Description
*.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.
*.sql	SQL scripts used by the tool to check the repository database.

¹ Paths are relative to the root of the OracleAS Backup and Recovery Tool directory.

See Also: *Oracle Application Server Installation Guide* for information about installing the Oracle Application Server

9.1.1 Manually Installing the OracleAS Backup and Recovery Tool

If you are running OracleAS TopLink in standalone mode, or ran the OracleAS Metadata Repository Creation Assistant to create a metadata repository in an existing database, then you must install the OracleAS Backup and Recovery Tool manually. Before you install the OracleAS Backup and Recovery Tool, review the following notes:

- 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.
- The tool is a Perl script that requires a Perl 5.6.1 interpreter, or later. You can obtain the interpreter from the Perl site: <http://www.perl.org>, or you can use the Perl interpreter that ships with Oracle Application Server:
 - On UNIX systems:


```
ORACLE_HOME/perl/bin/perl
```
 - On Windows systems:


```
ORACLE_HOME\perl\5.6.1\bin\MSWin32-x86\perl.exe
```
- The tool requires that Java Runtime Environment (JRE) be installed. You can obtain JRE at: <http://java.sun.com/j2se/desktopjava/jre/index.jsp>.

To install the OracleAS Backup and Recovery Tool:

1. Log in as the user who installed Oracle Application Server.
2. Extract the backup_restore.jar file from the backup.jar file which is located in the directory: `CD_ROM/stage/Components/oracle.iappserver.backup_restore/10.1.2.0.0/1/DataFiles/backup.jar` For example:

```
cd ORACLE_HOME
jar xvf CD_ROM/stage/Components/oracle.iappserver.backup_restore/10.1.2.0.0
/1/DataFiles/backup.jar
```

If you ran the OracleAS Metadata Repository Creation Assistant (REPCA) to create a metadata repository in an existing database, then the file `backup_restore.jar` is automatically extracted for you and put in directory `ORACLE_HOME/utilities/backup`

Once you have obtained the `backup_restore.jar`, extract its contents into the Oracle home of the OracleAS TopLink or REPCA installation. For example:

```
cd ORACLE_HOME
jar xvf utilities/backup/backup_restore.jar
```

3. On UNIX, make sure the `bkp_restore.sh` file has execute permission. For example:

```
chmod 755 ORACLE_HOME/backup_restore/bkp_restore.sh
```

4. Familiarize yourself with the OracleAS Backup and Recovery Tool files, which are described in the [Table 9-1](#). Instructions for editing the configuration files are in subsequent steps.

9.2 Configuring 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.

Note for Windows Users: Do not use a rich text editor, such as WordPad, when editing files in the Backup and Recovery Tool directory. It inserts a return character at the end of each line that may cause the tool to fail. Oracle recommends that you use a basic text formatter, such as Notepad, instead.

1. The tool writes out log files and backup files, and you must create the following directories to hold these.;
 - **Log file directory:** (Middle tier and Infrastructure) This directory holds log files created by the tool. This directory should have several megabytes of space.
 - **Configuration file backup directory:** (Middle tier and Infrastructure) This directory holds configuration file backups. This directory should have several hundred megabytes of space.
 - **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 file system 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.
- Ensure 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`:

On Unix:

```
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
```

On Windows:

```
mkdir C:\backups\log_files
mkdir C:\backups\db_files
mkdir C:\backups\config_files
```

2. Edit `config.inp` and modify the parameters as described in [Table 9–2](#). Notice that some of the instructions are different depending on whether this is a middle-tier or Infrastructure installation.

Table 9–2 Parameters in config.inp

Parameter	Value
<code>oracle_home</code>	Specify the full path of the Oracle home.
<code>log_path</code>	Specify the full path of the log file directory.
<code>config_files_list</code>	Do not insert a value for this; leave it as <code>config_files_list=DO_NOT_SET</code> . This parameter will be updated with the appropriate list of configuration files for your installation when you run <code>bkp_restore.pl -m configure</code> .
<code>config_backup_path</code>	Specify the full path of the configuration file backup directory.
<code>install_type</code>	Do not insert a value for this; leave it as <code>install_type=DO_NOT_SET</code> . This parameter is updated with the appropriate value for your installation when you run <code>bkp_restore.pl -m configure</code> .
<code>dbid</code>	Do not insert a value for this; leave it as <code>dbid=DO_NOT_SET</code> . For Infrastructure installations, this value is updated when you run <code>bkp_restore.pl -m configure</code> . By default, the tool obtains the <code>dbid</code> from the Metadata Repository. Or, you can supply a <code>dbid</code> in special cases involving migrating a Metadata Repository from one host to another, such as for Disaster Recovery. For middle-tier installations, this value is untouched.
<code>pfile</code>	Middle-tier Installation: Leave this line commented out. Infrastructure: If desired, specify an alternate <code>pfile</code> to use when starting up the database. Otherwise, leave the line commented out and the default <code>spfile</code> will be used: (UNIX) <code>ORACLE_HOME/dbs/spfileSID.ora</code> (Windows) <code>ORACLE_HOME\database\spfileSID.ora</code> Be sure to leave the <code>pfile</code> entry commented out if you want to use the default because blank values are not allowed in this file. If the <code>spfileorcl.ora</code> file is not present at the default location, the following file will be used as <code>pfile</code> : (UNIX) <code>ORACLE_HOME/dbs/initSID.ora</code> (Windows) <code>ORACLE_HOME\database\initSID.ora</code> If you want to use a different <code>pfile</code> , specify an alternate <code>pfile</code> name for starting up the database.

Table 9–2 (Cont.) Parameters in config.inp

Parameter	Value
database_backup_path	<p>Middle-tier Installation:</p> <p>Do not insert a value for this; leave it as database_backup_path=VALUE_NOT_SET.</p> <p>Infrastructure:</p> <p>Specify the full path of the database backup directory.</p>

1. Set the ORACLE_HOME environment variable to the Oracle Application Server Oracle home.
2. If this is an Infrastructure installation:
 - a. Set the ORACLE_SID environment variable to the Metadata Repository SID. The default is orcl.
 - b. Ensure the Metadata Repository is started.
3. Configure the tool by running it with the `-m configure` option, for example:
 - For UNIX systems:


```
./bkp_restore.sh -m configure
```
 - For Windows systems:


```
bkp_restore.bat -m configure
```
 - For OracleAS TopLink or REPCA installations on UNIX or Windows, after specifying the correct version of perl.exe, run:


```
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.

9.3 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.

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, such as Oracle Application Server component specific log files, to a backup, add entries to the `config_misc_files.inp` file as follows:

- To specify a particular file:
`${ORACLE_HOME}/directorypath/file`
- To specify an entire directory:
`${ORACLE_HOME}/directorypath/`
- To use wildcards:
`${ORACLE_HOME}/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, then 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`.

9.4 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](#)

9.4.1 Prerequisites for Running the Tool

Before running the OracleAS Backup and Recovery Tool:

- Log in as the user who installed Oracle Application Server.
- Ensure the `ORACLE_HOME` environment variable is set.
- If you are performing a database backup, then ensure the `ORACLE_SID` environment variable is set. The default is `orcl`.

9.4.2 Syntax

The syntax for the OracleAS Backup and Recovery Tool is:

On UNIX:

```
bkp_restore.sh [-defsv] -m mode [args]
```

On Windows:

```
bkp_restore.bat [-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.
- -n: Suppress prompts so the tool can be run in batch mode.
- -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 9-3](#) describes the OracleAS Backup and Recovery Tool modes and their arguments. All modes and arguments are case-sensitive.

Table 9-3 Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
<code>backup_cold</code>	<p>Performs a complete cold backup of the Metadata Repository. The command performs the following operations:</p> <ul style="list-style-type: none"> ■ Opens <code>config.inp</code> (or the alternate file specified with the <code>-e</code> option) and retrieves <code>log_path</code>. ■ 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 <code>backup_cold.dat</code>. ■ Stores the backup in the directory specified in <code>backup_cold.dat</code>. (This is usually set to the <code>database_backup_path</code> in <code>config.inp</code>.) ■ Stores a log file in <code>log_path</code>. ■ Opens the database. <p>For a DCM file-based Metadata Repository:</p> <ul style="list-style-type: none"> ■ Executes the <code>dcmtl exportrepository</code> command to perform a backup of the file-based repository. ■ Stores the backup in the directory, specified by <code>config_backup_path</code> parameter in <code>config.inp</code>. <p>If both a metadata repository and a file-based repository coexist in an application server instance, the <code>backup_cold</code> option backs up both of them as a set. This would be the case where a file-based repository exists in an Infrastructure install.</p> <p>To check whether a particular OracleAS instance hosts a file-based repository or a database repository, use the following command:</p> <pre>ORACLE_HOME/dcm/bin/dcmctl whichfarm</pre> <p>Repository Type: Database (host) => Hosts a database repository Repository Type: Distributed File Based (host) => Hosts a file based repository</p>
<code>backup_cold_incr</code> <code>-l incr_backup_level</code>	<p>Performs an incremental backup of the Metadata Repository.</p> <p>Works the same as <code>backup_cold</code>, except:</p> <ul style="list-style-type: none"> ■ The <code>-l</code> option specifies the increment level (0 - 4). ■ Uses the <code>backup_cold_incrlevel.dat</code> file <p>There are two types of incremental backups, cumulative and differential. The tool uses the default type, which is differential. For more information, refer to <i>Oracle Database Backup and Recovery Basics</i> in the Oracle Database 10g Documentation Library.</p>

Table 9–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
backup_config	<p>Performs a full configuration backup. The backup includes the configurations for DCM managed components and non-DCM managed components. The command performs the following operations:</p> <ul style="list-style-type: none"> ■ Opens <code>config.inp</code> (or the alternate file specified with the <code>-e</code> option) and retrieves <code>config_files_list</code>, <code>config_backup_path</code>, and <code>log_path</code>. ■ Creates an archive for configuration of DCM managed components: ■ Attempts to open each file in <code>config_files_list</code>. Exits with an error if it cannot open all of the files. ■ For each file in <code>config_files_list</code>, checks if the first entry (the key file) exists. If the key file does not exist, it is treated as a fatal error. Otherwise, backs up all files in the list. If any other files do not exist, logs an error and continues. ■ Excludes files listed in <code>config_exclude_files.inp</code>. ■ When finished, stores the backup in <code>config_backup_path/config_bkp_timestamp.jar</code> and <code>config_backup_path/dcm_archive_timestamp.jar</code> for DCM-managed components. ■ If any errors are encountered, creates a log file in <code>log_path/config_bkp_timestamp</code>. <p>Process Prerequisites:</p> <p>If the DCM repository type is a database, the following processes should be up:</p> <ul style="list-style-type: none"> ■ The Oracle Internet Directory process must be up. The command <code>opmnctl startproc ias-component=OID</code> can be used to start this process. The Oracle Internet Directory process exists on Infrastructure (Identity Management and Metadata Repository or Identity Management only) installation. Before starting the Oracle Internet Directory process, the OPMN process must be up. The command <code>opmnctl start</code> can be used to bring it up. ■ The database needs to be up. ■ The listener process must be up. <p>To check whether a particular Oracle Application Server instance hosts a file based repository or a database repository, use the following command:</p> <pre>ORACLE_HOME/dcm/bin/dcmctl whichfarm</pre> <p>Repository Type: Database (host) => Hosts a database repository</p> <p>Repository Type: Distributed File Based (host) => Hosts a file based repository</p>
backup_config_incr	<p>Performs an incremental configuration file backup.</p> <p>Works the same as <code>backup_config</code>, except that it backs up all configuration files that have changed since the last full or incremental configuration file backup.</p> <p>For process prerequisites, refer to the <code>backup_config</code> option.</p>
backup_instance_cold	<p>Performs a complete cold backup of the Oracle Application Server instance. The command performs the following operations:</p> <ul style="list-style-type: none"> ■ Stops all OPMN managed processes. ■ Starts the OPMN administrative process. ■ Checks all of the OPMN managed processes to ensure that the processes are stopped. If not, tries to stop them one more time. If the processes still cannot be stopped, issues a fatal error. ■ Performs repository backup (database and file-based). For a database repository, shuts down the database for the duration of the backup. ■ Starts Oracle Internet Directory and DCM-daemon processes for database repositories. ■ Performs configuration backup. ■ Starts all OPMN managed processes. ■ Checks to ensure that all OPMN processes are running. If not, issues a warning message.

Table 9–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
<code>backup_instance_cold_incr -1 <level number></code>	<p>Performs an incremental cold backup of the Oracle Application Server instance. The command performs the following operations:</p> <ul style="list-style-type: none"> Stops all OPMN managed processes. Starts the OPMN administrative process. Checks all of the OPMN managed processes to ensure that the processes are stopped. If not, tries to stop them one more time. If the processes still cannot be stopped, issues a fatal error. Performs repository backup (database or file-based). For a database repository, shuts down the database for the duration of the backup. The level option applies to database repositories only. Backup is performed to the specified level. The default level is 1. Starts Oracle Internet Directory and DCM-daemon processes for database repositories. Performs configuration backup. Starts all OPMN managed processes. Checks to ensure that all OPMN processes are running. If not, issues a warning message.
<code>backup_instance_online</code>	<p>Performs an online backup of the Oracle Application Server instance. The command performs the following operations:</p> <ul style="list-style-type: none"> Performs repository backup (database or file based). For a database repository, the database remains up while being backed up. Performs configuration backup.
<code>backup_instance_online_incr -1 <level number></code>	<p>Performs an incremental online backup of the Oracle Application Server instance. The command performs the following operations:</p> <ul style="list-style-type: none"> Performs an incremental repository backup (database or file-based). For a database repository, the database remains up while being backed up. The level option applies to database repositories only. Backup is performed to the specified level. The default level is 1. Performs incremental configuration backup.
<code>backup_online</code>	<p>Performs an online backup of the Metadata Repository. If you are running this command on an Infrastructure, ensure that the Metadata Repository is up before running this command. The command performs the following operations:</p> <ul style="list-style-type: none"> Opens <code>config.inp</code> (or the alternate file specified with the <code>-e</code> option) and retrieves <code>log_path</code>. Assumes the database is open. Performs a backup of the datafiles and control files using RMAN. The commands are in <code>backup_online.dat</code>. Stores the backup in the directory specified in <code>backup_online.dat</code>. (This is usually set to the <code>database_backup_path</code> in <code>config.inp</code>.) Stores a log file in <code>log_path</code>. Leaves the database open. <p>For a DCM file-based Metadata Repository:</p> <ul style="list-style-type: none"> Executes the <code>dcmctl exportrepository</code> command to perform a backup of the file-based repository. Stores the backup in the directory, specified by <code>config_backup_path</code> parameter in the <code>config.inp</code> file. <p>If both a metadata repository and a file-based repository coexist in an application server instance, the <code>backup_online</code> option backs both of them up as a set. This would be the case where a file-based repository exists in an infrastructure install.</p> <p>To check whether a particular OracleAS instance hosts a file-based repository or a database repository, use the following command:</p> <pre>ORACLE_HOME/dcm/bin/dcmctl whichfarm</pre> <p>Repository Type: Database (host) => Hosts a database repository Repository Type: Distributed File Based (host) => Hosts a file based repository</p>

Table 9–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
backup_online_incr -l incr_backup_level	<p>Performs an incremental online backup of the Metadata Repository.</p> <p>Works the same as backup_online, except:</p> <ul style="list-style-type: none"> ▪ The -l option specifies the increment level (0 - 4). ▪ Uses the backup_online_incrlevel.dat file <p>There are two types of incremental backups, cumulative and differential. The tool uses the default type, which is differential. For more information, refer to <i>Oracle Database Backup and Recovery Basics</i> in the Oracle Database 10g Documentation Library.</p>
configure [-i dbid]	<p>Configures the tool. When using this command on an Infrastructure, make sure the Metadata Repository is started before you run this command. The command performs the following operations:</p> <ul style="list-style-type: none"> ▪ 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	<p>Same as configure but does not perform the Infrastructure configuration.</p> <p>Note: You should use configure for all middle-tier and Infrastructure installations. The configure_nodb argument applies to disaster recovery strategies described in <i>Oracle Application Server High Availability Guide</i>.</p>
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 does not 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.
restore_config[-t config_ bkp_timestamp][-n]	<p>Restores configuration files. The command performs the following operations:</p> <ul style="list-style-type: none"> ▪ 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. ▪ Restores configuration for DCM managed components <p>The -n option suppresses prompts so you can use the tool in batch mode.</p> <p>For the process prerequisites, refer to the backup_config option.</p> <p>Do not run restore_config on multiple nodes in a J2EE cluster in parallel. Doing so will cause restore_config failures. Run restore_config on one node at a time.</p>
restore_db	This command is deprecated. Use restore_repos instead.

Table 9–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
<pre>restore_instance -t <timestamp> -c</pre>	<p>Restores an instance of Oracle Application Server. If the timestamp argument is not specified, then a list of backup timestamps is displayed to the user. The command performs the following operations:</p> <ul style="list-style-type: none"> ■ Stops all OPMN managed processes. ■ Checks to verify that the OPMN processes have stopped. If OPMN processes cannot be stopped (maybe an <code>opmn.xml</code> file is missing), a file system restore runs using the <code>bkp_restore.sh -m restore_instance -F noDCM</code> command. Then, it tries to stop the OPMN processes again. If the OPMN processes still cannot be stopped, issues a fatal error. ■ Starts the OPMN administration process. ■ Performs repository restore. The <code>-c</code> option is applicable for database repositories only. If the <code>-c</code> option is specified, the control file is also restored. ■ Starts Oracle Internet Directory and DCM-Daemon processes (applicable to database repositories only). ■ Performs configuration restore. ■ Starts all OPMN managed processes. ■ Checks to ensure that all OPMN managed processes are started. If not, issues a warning message.
<pre>restore_repos [-u timestamp] [-c] [-n]</pre>	<p>Restores and recovers the Metadata Repository and the DCM file-based repository from the available cold and online backups. To perform <code>restore_repos</code>, the Metadata Repository database must be started and open. The command performs the following operations:</p> <ul style="list-style-type: none"> ■ Opens <code>config.inp</code> (or the alternate file specified with the <code>-e</code> option) and retrieves <code>log_path</code>. ■ Restores the control files and datafiles, and performs recovery using RMAN. The commands are in <code>restore_repos.dat</code>. ■ Stores a log file in <code>log_path</code>. ■ Leaves the database open. <p>By default, this command restores and recovers the database to its most recent state. You can use the <code>-u</code> option to restore and recover the database to its state at a particular point in time. The format for the timestamp is <code>MM/DD/YYYY_HR24:MIN:SEC</code>, for example:</p> <p>On UNIX:</p> <pre>bkp_restore.sh -m restore_repos -u 07/26/2003_13:45:06</pre> <p>On Windows:</p> <pre>bkp_restore.bat -m restore_repos -u 07/26/2003_13:45:06</pre> <p>By default, this command does not restore the control file. You can use the <code>-c</code> option to restore the control file.</p> <p>If you use the <code>-u</code> or <code>-c</code> option, be sure to do a full backup right away because all past backups are invalidated.</p> <p>The <code>-n</code> option suppresses prompts so you can use the tool in batch mode.</p> <p>This command performs the following operations to restore a file-based repository:</p> <ul style="list-style-type: none"> ■ Checks for timestamp input. If not provided, lists the available backup timestamps corresponding to the file-based repository. ■ Executes <code>dcmctl importrepository -file location_in_config_backup_path that stores the repository backup</code>. <p>On UNIX:</p> <pre>bkp_restore.sh -m restore_repos -t 2004-05-10_18-33-12</pre> <p>On Windows:</p> <pre>bkp_restore.bat -m restore_repos -t 2004-05-10_18-33-12</pre> <p>If both the metadata repository and a file-based repository coexist in an application server instance, the <code>restore_repos</code> option restores both of them as a set. This would be the case where DCM uses a file-based repository in an infrastructure install.</p>

Table 9–3 (Cont.) Oracle Application Server Backup and Recovery Tool Modes and Arguments

Mode and Arguments	Description
flashback_repos -u timestamp -b timestamp [-n]	<p>Rewinds the Metadata Repository to a specified time by using the before images of changed data blocks to back out changes made to the database since the specified time. To perform Flashback, the Metadata Repository database must be started and open. The command performs the following operations:</p> <ul style="list-style-type: none"> Opens the <code>config.inp</code> file (or an alternate file specified with the <code>-e</code> option) and retrieves <code>log_path</code>. Recovers the database to or before a specified time by performing Flashback. The commands are located in: <ul style="list-style-type: none"> <code>flashback_repos_to.tmp1</code> <code>flashback_repos_before.tmp1</code> Stores a log file in <code>log_path</code>. Leaves the database open. <p>Flashback requires a database repository. Flashback is not supported on file-based repositories.</p> <p>You do not need to perform a cold backup before running Flashback. Flashback does not require restoring previous backups in order to recover the database. This means the <code>flashback_repos</code> operation is faster than the <code>restore_repos</code> operation. Flashback can undo any logical data corruption or user error, such as deleting an Oracle Application Server schema or undeploying an application by mistake.</p> <p>To perform Flashback, the database must be configured with a Flash Recovery Area, and ARCHIVELOG mode and Flashback must be enabled. Use the following SQL statements to configure and enable Flashback:</p> <pre>ALTER SYSTEM SET DB_RECOVERY_FILE_DEST_SIZE = size SCOPE=BOTH SID='*'; ALTER SYSTEM SET DB_RECOVERY_FILE_DEST = directory_path SCOPE=BOTH SID='*'; ALTER DATABASE ARCHIVELOG; ALTER DATABASE FLASHBACK ON;</pre> <p>Refer to the Oracle Database Backup and Recovery Basics manual, Chapter 3, the section on "Setting up a Flash Recovery Area for RMAN" for more detail. Also, Section 9.5.2, "Enabling ARCHIVELOG Mode" for information on enabling ARCHIVELOG mode.</p> <p>Either the <code>-u</code> or <code>-b</code> option must be specified. The <code>-u</code> option returns the database to its state at the specified time. The <code>-b</code> option returns the database to its state prior to the specified time. The format for the timestamp is <code>MM/DD/YYYY_HR24:MIN:SEC</code>.</p> <ul style="list-style-type: none"> On UNIX systems: <pre>bkp_restore.sh -m flashback_repos -u 07/26/2003_13:45:06</pre> On Windows systems: <pre>bkp_restore.bat -m flashback_repos -u 07/26/2003_13:45:06</pre> <p>The <code>-n</code> option suppresses prompts so that the tool can be run in batch mode.</p> <p>For more information on Flashback technology, refer to the <i>Oracle Database Backup and Recovery Advanced User's Guide</i>.</p> <p>After running <code>flashback_repos</code>, do a full backup immediately because all past backups are invalidated. See the section "Restoring and Recovering the Metadata Repository" in the <i>Oracle Application Server Administrator's Guide</i> for more information.</p>

9.4.3 Usage Examples

This section contains usage examples for the OracleAS Backup and Recovery Tool. The UNIX command is listed first and then the Windows command.

- Configure the tool using the default `config.inp` file:

```
bkp_restore.sh -m configure
bkp_restore.bat -m configure
```

- Configure the tool using a configuration file called `myconfig.inp`:

```
bkp_restore.sh -m configure -e myconfig.inp
bkp_restore.bat -m configure -e myconfig.inp
```

- Perform a full configuration file backup:

```
bkp_restore.sh -v -m backup_config  
bkp_restore.bat -v -m backup_config
```
- Perform a full configuration file backup using an environment file called `myconfig.inp`:

```
bkp_restore.sh -v -m backup_config -e myconfig.inp  
bkp_restore.bat -v -m backup_config -e myconfig.inp
```
- Perform an incremental configuration file backup:

```
bkp_restore.sh -v -m backup_config_incr  
bkp_restore.bat -v -m backup_config_incr
```
- Restore configuration files:

```
bkp_restore.sh -m restore_config -t 2004-09-21_06-12-45  
bkp_restore.bat -m restore_config -t 2004-09-21_06-12-45
```
- Perform a full cold backup of the Metadata Repository:

```
bkp_restore.sh -m backup_cold  
bkp_restore.bat -m backup_cold
```
- Perform a level 2 incremental cold backup of the Metadata Repository:

```
bkp_restore.sh -m backup_cold_incr -l 2  
bkp_restore.bat -m backup_cold_incr -l 2
```
- Perform an full online backup of the Metadata Repository:

```
bkp_restore.sh -m backup_online  
bkp_restore.bat -m backup_online
```
- Perform a level 0 incremental online backup of the Metadata Repository:

```
bkp_restore.sh -m backup_online_incr -l 0  
bkp_restore.bat -m backup_online_incr -l 0
```
- Restore the Metadata Repository to its most recent state:

```
bkp_restore.sh -m restore_repos  
bkp_restore.bat -m restore_repos
```
- Restore the Metadata Repository to its state at a particular time:

```
bkp_restore.sh -m restore_repos -u 07/26/2003_13:45:06  
bkp_restore.bat -m restore_repos -u 07/26/2003_13:45:06
```
- Flashback the Metadata Repository to its state at a particular point in time:

```
bkp_restore.sh -m flashback_repos -u 07/26/2003_13:45:06  
bkp_restore.bat -m flashback_repos -u 07/26/2003_13:45:06
```
- Restores the file based repository to its state at a particular time:

```
bkp_restore.sh -m restore_repos -t 2004-05-10_18-33-12  
bkp_restore.bat -m restore_repos -t 2004-05-10_18-33-12
```

9.5 Backup Procedures

This section describes the backup procedures in detail. There is some data interdependency between the configuration files in your Oracle Application Server middle-tier installations, the Distributed Management Repository, the Identity Management metadata, and the Oracle Application Server Metadata Repository in the Infrastructure. To maintain configuration data consistency, you should back up each of your Oracle Application Server instances (middle-tier and Infrastructure) at the same time. While backing up one Oracle Application Server instance, ensure that no configuration changes are made in any of the other instances.

This section contains the following topics:

- [Enabling Block Change Tracking](#)
- [Enabling ARCHIVELOG Mode](#)
- [Creating a Record of Your Oracle Application Server Configuration](#)
- [Performing a Complete Oracle Application Server Environment Backup](#)
- [Performing a Configuration and Metadata Backup](#)

9.5.1 Enabling Block Change Tracking

To increase performance on incremental database backups, enable block change tracking using the following command:

```
alter database enable block change tracking using file file_name;
```

If the `db_create_file_dest` parameter is set in the `spfile` or `init.ora` file of the database, then the following command can be used:

```
alter database enable block change tracking;
```

Once you enable block change tracking, incremental database backup will use block change tracking.

For more information about block change tracking, refer to *Backup and Recovery Basics* in the *Oracle Database 10g Release 1 (10.1) Documentation Library*.

9.5.2 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 about the parameters in this section, and setting up archive logging in general, in *Oracle Database Administrator's Guide 10g Release 1 (10.1)*.

To enable ARCHIVELOG mode:

1. Run the following sql query to check if the `flashback_recovery_area` is setup:

```
SQL> show parameters db_recovery
```

If the `flashback_recovery_area` is setup, the query returns:

Name	Type	Value
------	------	-------


```
db_recovery_file_dest      string      /private2/AS1012Installs/AS1012Infra/
                           flash_recovery_area
db_recovery_file_dest_size big integer  2G
```

If the `flashback_recovery_area` is set up, then the destination specified by the `db_recovery_file_dest` parameter is used as the archive log destination, and you do not need to specify the destination directory for your archives in the following step.

- Specify the destination directory for your archives by including the initialization parameter `LOG_ARCHIVE_DEST_n` in the initialization file. If `spfile` is used, then the following command can be issued:

```
alter system set log_archive_dest_n="LOCATION=<backup directory>" scope=spfile;
```

In the `log_archive_dest_n` parameter, `n` is a number of 1 through 10.

If `pfile` is used, the following initialization file must be edited:

For UNIX systems:

```
INFRA_ORACLE_HOME/dbs/initSID.ora
```

For Windows systems:

```
INFRA_ORACLE_HOME\database\initSID.ora
```

Change the `LOG_ARCHIVE_DEST_n` parameter to:

```
LOG_ARCHIVE_DEST_n="LOCATION=<backup directory>"
```

(Optional) The default filename format for archive logs is:

- For UNIX systems:

```
%t_%s_%r.dbf
```

- For Windows systems:

```
ARC%S_%R.%T
```

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 = 'log%t_%r_%s.arc'
```

In the preceding example, `t` represents the thread number, `r` represents the reset log ID, and `s` represents the log sequence number.

- Make sure that the `ORACLE_HOME` and `ORACLE_SID` (the default is `orcl`) environment variables are properly set.
- Make sure that no one is using the database.
- Perform a clean, normal shutdown of the database instance.

```
INFRA_ORACLE_HOME/bin/sqlplus /nolog
SQL> connect sys/password as sysdba
SQL> shutdown
```

- Start up the instance and mount, but do not open the database.

```
SQL> startup mount;
```

- Enable database ARCHIVELOG mode.

```
SQL> alter database archivelog;
```

8. Shut down and restart the database instance.

```
SQL> shutdown
```

```
SQL> startup
```

9. 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 997
Next log sequence to archive 999
Current log sequence       999
```

9.5.3 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 e-mail 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

9.5.4 Performing a Complete Oracle Application Server Environment Backup

This section describes how to perform a complete Oracle Application Server environment backup. A complete Oracle Application Server environment backup includes Identity Management metadata and Oracle Application Server Metadata Repository, which can be stored in the same database or different databases. There are two modes for backing up the databases: cold backup and online backup. Before performing a cold backup on an open database, the Backup and Recovery Tool performs a clean shutdown and rolls back any ongoing changes to the database. As a result, a cold backup is a copy of the database at a consistent state. A consistent backup can be restored without recovery. An online backup does not require shutting down the repository database. There is no need to bring down your business applications, providing a higher degree of continuous availability. An online backup is a snapshot or point-in-time image of the database. When you use the Backup and Recovery Tool to restore an online backup, any ongoing changes to the database occurring during the time of the online backup will be recovered by applying the redo logs. Refer to the *Oracle Database Backup and Recovery Advanced User's Guide*, "RMAN Backup Types" for more detail.

This procedure contains the following steps:

- [Task 1: Shut Down Your Oracle Application Server Environment](#)
- [Task 2: Back Up the Middle-Tier Installations](#)
- [Task 3: Back Up the Infrastructure](#)
- [Task 4: Back Up the Oracle System Files](#)
- [Task 5: Start Your Oracle Application Server Environment](#)

Task 1: Shut Down Your Oracle Application Server Environment

If this is the first backup after installing the Oracle Application Server, then you should take the following steps to shut down the Oracle Application Server Environment and perform a cold backup of the databases where the Identity Management metadata and the Oracle Application Server Metadata Repository are stored. If you are performing a complete Oracle Application Server environment backup after a major change, like a rolling- software upgrade, you can perform either a cold backup or an online backup of the databases. If you choose the online backup so that your business applications remain up and running, you can skip this task and proceed with Task 2 and Task 3.

1. Stop the middle-tier instances.
Refer to [Section 3.1.6, "Stopping a Middle-Tier Instance"](#) for instructions.
2. Stop the Infrastructure.
Refer to [Section 3.1.4, "Stopping OracleAS Infrastructure"](#) for instructions.

Task 2: 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
Backup the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
```

2. Back up the middle-tier configuration files.

If the DCM repository type is a database, then the following processes must be up:

- The OPMN process. The command `opmnctl start` can be used to start it.
- The OID process. The command `opmnctl startproc ias-component=OID` can be used to start this process. The OID process exists on Infrastructure (Identity Management and Metadata Repository or Identity Management only) installation.
- The database.
- The listener process.

Back up 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:

- For UNIX systems:

```
bkp_restore.sh -m backup_config
```
- For Windows systems:

```
bkp_restore.bat -m backup_config
```

See Also: Chapter 20, "Oracle Application Server Backup and Recovery Tool" in *Oracle Application Server Administrator's Guide* for more information.

The reason for backing up configuration files 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.

The configuration files are stored in jar files located in the directory specified by the `config_backup_path` parameter in the `config.inp` file. Two jar files are

created, one for DCM-managed components and one for all the other components. The jar files are kept in sync by the timestamp incorporated in each jar file name. For example:

```
config_bkp_2004-05-10_18-33-15.jar
dcm_archive_2004-05-10_18-33-15.jar
```

Task 3: 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:

- For UNIX systems:

```
bkp_restore.sh -m backup_cold
or
bkp_restore.sh -m backup_online
```

- For Windows systems:

```
bkp_restore.bat -m backup_cold
or
bkp_restore.bat -m backup_online
```

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 20, "Oracle Application Server Backup and Recovery Tool" in *Oracle Application Server Administrator's Guide* 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, then perform this step on both Oracle homes. If your Identity Management is split between Oracle Internet Directory in one Oracle home and Single Sign-On, Delegated Administration Service, and so on in another Oracle home, then you also should perform this step on each of those 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
Backup the registry entry HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
```

3. Back up the Infrastructure configuration files.

Note: If your Infrastructure has Identity Management in one Oracle home, and the Metadata Repository in another Oracle home, perform this step on both Oracle homes. If your Identity Management is split between Oracle Internet Directory in one Oracle home and Single Sign-On, Delegated Administration Service, and so on in another Oracle home, then you also should perform this step on each of those Oracle homes.

If the DCM repository type is a database, then the following processes must be started:

- The OPMN process. Use the command `opmnctl start` to start it.
- The OID process. Use the command `opmnctl startproc ias-component=OID` to start this process. The OID process exists on Infrastructure (Identity Management and Metadata Repository or Identity Management only) installation.
- The database.
- The listener process.

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:

- For UNIX systems:

```
bkp_restore.sh -m backup_config
```

- For Windows systems:

```
bkp_restore.bat -m backup_config
```

See Also: Chapter 20, "Oracle Application Server Backup and Recovery Tool" in *Oracle Application Server Administrator's Guide* for more information.

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.

Task 4: 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, then 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, then 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`. On Windows

systems, the location of the oraInventory can be obtained from the registry: HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\INST_LOC.

Task 5: Start Your Oracle Application Server Environment

To start the environment, take the following steps:

1. Start the Infrastructure.
Refer to [Section 3.1.3, "Starting OracleAS Infrastructure"](#) for instructions.
2. Start the middle-tier instances.
Refer to [Section 3.1.5, "Starting a Middle-Tier Instance"](#) for instructions.

9.5.5 Performing a Configuration and Metadata Backup

Once you have performed a complete Oracle Application Server environment backup, you should perform subsequent configuration and metadata backups after every administrative change, or, if this is not possible, on a regular basis.

See Also: Appendix G, "Examples of Administrative Changes" in *Oracle Application Server Administrator's Guide* to learn more about administrative changes

These backups can be performed online (while Oracle Application Server is running), and only contain configuration files, Identity Management metadata, and the Metadata Repository.

This section describes how to perform a configuration and metadata backup of your Oracle Application Server environment. It contains the following steps:

- [Task 1: Back Up the Infrastructure](#)
- [Task 2: Back Up the Middle-tier Installations](#)

Task 1: Back Up the Infrastructure

To backup the Infrastructure:

1. Perform a full or 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:

- On UNIX systems:


```
bkp_restore.sh -m backup_config
or
bkp_restore.sh -m backup_config_incr
```
- On Windows systems:


```
bkp_restore.bat -m backup_config
or
bkp_restore.bat -m backup_config_incr
```

See Also: Chapter 20, "Oracle Application Server Backup and Recovery Tool" in *Oracle Application Server Administrator's Guide* for more information.

2. Perform an online database backup of the Metadata Repository. It can be a full or incremental online 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:

- On UNIX systems:

```
bkp_restore.sh -m backup_online  
or  
bkp_restore.sh -m backup_online_incr -l 2
```

- On Windows systems:

```
bkp_restore.bat -m backup_online  
or  
bkp_restore.bat -m backup_online_incr -l 2
```

See Also: Chapter 20, "Oracle Application Server Backup and Recovery Tool" in *Oracle Application Server Administrator's Guide* for more information.

Task 2: Back Up the Middle-tier Installations

For each middle-tier installation in your environment, perform a full or 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:

- For UNIX systems:

```
bkp_restore.sh -m backup_config  
or  
bkp_restore.sh -m backup_config_incr
```

- For Windows systems:

```
bkp_restore.sh -m backup_config  
or  
bkp_restore.bat -m backup_config_incr
```

See Also: Chapter 20, "Oracle Application Server Backup and Recovery Tool" in *Oracle Application Server Administrator's Guide* for more information.

OPMN Commands

Oracle Process Manager and Notification Server (OPMN) is installed and configured with every Oracle Application Server installation type and is essential for running Oracle Application Server. This appendix lists the key OPMN commands and illustrates their usage.

start

Syntax: `opmnctl start`

Starts the OPMN server for a local Oracle Application Server instance without starting OPMN-managed processes.

startall

Syntax: `opmnctl startall [timeout=seconds]`

Starts OPMN and OPMN-managed processes for a local instance. This is equivalent to the `start` command and the `startproc` command without arguments. Oracle recommends using the `start` or `startproc` command.

This command operates synchronously and waits for the operation to complete before returning. To set a timeout for the request, specify the timeout value in seconds.

stopall

Syntax: `opmnctl stopall`

Shuts down the OPMN server and OPMN-managed processes for the local instance. This request operates synchronously and waits for the operation to complete before returning.

startproc

Syntax: `opmnctl [scope] startproc [attr=value]...`

Starts OPMN-managed processes in the requested scope. The OPMN server for the instance must be started.

The following attributes and values can be used with `startproc`:

- `ias-component`, `process-type`, and `process-set`: The values for these attributes should be the same as the `id` value specified in the `opmn.xml` file. If no attribute is supplied, the command is applied to all OPMN-managed processes.
- `mode`: The value can be either `sync` or `async`. The default value is `sync`. The `sync` value causes the `opmnctl` command to operate synchronously and wait for the command to be executed completely before a return prompt is displayed. The `timeout` element can only be specified when the value of `mode` is `sync`. The

value is specified in number of seconds. After the specified timeout expires, the operation is aborted for `startproc` but not for `restartproc` or `stopproc`. The `opmnctl` command prompt returns, the OPMN server continues to perform the `restartproc` or `stopproc` command request until the operation is finished.

The `async` value causes the return prompt to be displayed immediately, while the OPMN server continues to perform the `opmnctl` command request until the operation is finished.

- `uniqueid`: This value is assigned by OPMN after starting up. You can use this value when you execute the `restartproc` and `stopproc` commands. To obtain this value, enter the following command and look for the unique ID for the component in the `uid` column of the generated output:

```
opmnctl status -l
```

Attribute names other than the those listed may be specified for some types of processes managed by OPMN. Unique attribute names should be specific to each type of process.

When you use the `opmnctl startproc` command with a specified scope and attributes, you can control specific processes in your enterprise. You can execute the `opmnctl startproc` command at the `ias-component`, `process-type`, and `process-set` level.

For example, the following command starts OracleAS Wireless at the `process-set` level:

```
opmnctl startproc ias-component=wireless process-type=alert_server
process-set=alert_instance_1
```

stopproc

Syntax: `opmnctl [scope] stopproc [attr=value]...`

Starts OPMN-managed processes in the requested scope. The OPMN server for the instance must be started.

The attributes and values of the `stopproc` command are identical to those of the `startproc` command.

When you use the `opmnctl startproc` command with a specified scope and attributes, you can control specific processes in your enterprise. You can execute the `opmnctl startproc` command at the `ias-component`, `process-type`, and the `process-set` level.

For example, the following command stops Oracle HTTP Server at the `ias-component` level:

```
opmnctl stopproc ias-component=HTTP_Server
```

status

Syntax: `opmnctl [scope] status [options]...`

Provides information about the processes managed by OPMN.

You can use the `opmnctl status` command with `scope` to obtain additional detailed information. For example, the following command gives you the status of every process of every component of every Oracle Application Server instance in an entire farm:

```
opmnctl @farm status
```

DCM Commands

Distributed Configuration Management is a management framework that enables you to manage the configurations of multiple instances. Distributed Configuration Management (DCM) features enable you to:

- Keep multiple configurations synchronized
- Archive and restore versions of configurations
- Export and import configurations between instances

[Table B-1](#) describes the key DCM commands and illustrates their usage.

Table B-1 DCM Commands and Usage

DCM Commands	Type	Syntax	Description and Example
<code>createCluster</code>	Configuration Management	<code>createCluster -cl cluster_name</code>	Creates a managed cluster. <code>dcmctl createCluster -cl cluster1</code>
<code>createComponent</code>	Configuration Management	<code>createComponent -ct oc4j -co component_name</code>	Creates a new OC4J instance belonging to the local application server instance. You cannot specify another instance with the <code>-i</code> option. The command operates locally. Example: <code>dcmctl createComponent -ct oc4j -co OC4J_myapps</code>
<code>exportRepository</code>	Configuration Management	<code>exportRepository -f myFile [-force]</code>	Copies the file-based repository information to the location specified. Use the <code>-force</code> option to overwrite an existing file. If you do not use the <code>-force</code> option and the named file exists, an exception is thrown. Example: <code>exportrepository -f /export/repository_save_file</code>
<code>getRepositoryId</code>	Configuration Management	<code>getRepositoryId</code>	Returns the file-based repository identifier of the farm to which the instance belongs. If the instance is a standalone instance, this command returns the repository identifier for the instance. If the standalone instance is to be used to establish a new distributed file-based repository, use the returned repository identifier to initialize the repository host with <code>joinFarm</code> and the <code>-r</code> option. Example: <code>dcmctl getrepositoryId</code>

Table B-1 (Cont.) DCM Commands and Usage

DCM Commands	Type	Syntax	Description and Example
importRepository	Configuration Management	importRepository -f file_name [-force]	Moves a file-based repository from one instance to another, based on a saved file from the exportRepository command. The repository may be restored to any instance in the farm. If the current instance is not hosting a repository, dcmctl prompts for confirmation of the action, unless the -force option is used. Example: importrepository -f /export/repository_save_file
joinCluster	Configuration Management	joinCluster -cl cluster_name [-i instance_name]	Adds an application server instance to the managed OracleAS Cluster specified with the -cl option. By default, this command uses the local instance. Specify a different instance with the -i option. Example: dcmctl joinCluster -cl cluster1
joinFarm	Configuration Management	joinFarm [-r repository_ID]	With the -r option and a repository ID, associates an instance with the named file-based repository. The repository_ID is a hostname and port. Example: dcmctl joinFarm -r repository_ID
leaveCluster	Configuration Management	leaveCluster [-i instance_name]	Removes an application server instance from its managed OracleAS Cluster. By default, this command uses the local instance. Specify a different instance with the -i option. Example: dcmctl leaveCluster
leaveFarm	Configuration Management	leaveFarm	Removes an application server instance from a farm. This command affects only the relationship between DCM and a repository, and has no impact on other components. Example: dcmctl leaveFarm
listInstances	Configuration Management	listInstances [-cl cluster_name]	With no options, this command lists the application server instances that belong to the same farm as the local instance, but are not part of a cluster. With the -cl option, it lists only the instances that are part of the specified cluster. Example: dcmctl listInstances
resyncInstance	Configuration Management	resyncInstance [-force] [-i instance_name]	Resynchronizes the instance configuration files with the contents of the DCM repository. This command takes all data from the repository that is not yet propagated and writes it out to the configuration files for the specified instance. It updates the Oracle HTTP Server, OC4J, and OPMN configuration files, as well as targets.xml. Example: dcmctl resyncinstance -i instance1
shell	Configuration Management	dcmctl shell [-f file_name]	Starts the dcmctl shell, and, optionally, executes the commands in a named file. Example: dcmctl shell

Table B-1 (Cont.) DCM Commands and Usage

DCM Commands	Type	Syntax	Description and Example
updateConfig	Configuration Management	updateConfig [-ct component_type [, component_type...]] [-force]	Updates the DCM repository with the information in local configuration files. With no arguments, this command updates all DCM managed components, configuration files, as well as targets.xml. Example: dcmctl updateConfig
whichCluster	Configuration Management	whichCluster [-i instance_name]	Returns the name of the cluster that contains the named instance. If no instance is specified, it returns the name of the cluster that contains the local instance. Example: dcmctl whichCluster
whichFarm	Configuration Management	whichFarm [-i instance_name]	Returns the farm name, farm type (database or distributed file-based repository), the hosting instance, and the host name. Example: dcmctl whichFarm
applyArchiveTo	Archive	applyArchiveTo -src archiveName [-cl clusterName -i instanceName]	When configuration information is stored in the DCM repository, it is recognized as one of the following two types of information: <ul style="list-style-type: none"> Information that is generic to any instance (cluster-wide information). Information that is specific to a particular instance (instance-specific information). Example: dcmctl applyarchiveto -src archive1 -i instance1
createArchive	Archive	createArchive -arch archiveName [-cl myCluster -i myInstance] [-comment "myComments"]	Creates an archive of the named instance or cluster. If you do not specify a cluster or instance, the current instance is archived. dcmctl applyarchiveto -src archive1 -i instance
exportArchive	Archive	exportArchive -arch archiveName -f myFile [-comment "myComments"]	Exports an archive from the repository to a file. Then, you can import the file to the same repository or to a different repository. Example: dcmctl exportArchive -arch archive1 -f /exports/testConfig -comment "this is an export of archive1"
importArchive	Archive	importArchive [-arch archiveName] -f myFile [-comment "myComments"]	Imports the named archive file to the current repository. Use -arch to change the name and -comment to change the comment during the import. Example: dcmctl importArchive -arch Archive1 -f /exports/testConfig -comment "this is an import"
deployApplication	Application	deployApplication -f file -a app_name [-co comp_name] [-enableIIOP] [-rc rootcontext] [-pa parent_name]	Deploys the J2EE application to the local application server instance. Example: dcmctl deployApplication -f app1.ear -a app1
redeployApplication	Application	redeployApplication -f file -a app_name [-co comp_name] [-enableIIOP] [-rc rootcontext]	Redeploys a J2EE application (WAR or EAR file) to the local application server instance. Example: dcmctl redeployApplication -f app1.ear -a app1

Table B-1 (Cont.) DCM Commands and Usage

DCM Commands	Type	Syntax	Description and Example
undeployApplication	Application	undeployApplication -a application_name -co instance_name	Undeploys the named application in the named OC4J instance. Example: undeployApplication -a testAp -co home
getReturnStatus	dcmtl Properties	getReturnStatus	Displays the status of the last dcmtl command that performed an asynchronous operation (as opposed to a command that returned information). Use this command to get the status of a previous command that timed out. Example: dcmtl getReturnStatus
getState	Configuration Management	getState [-i instance_name] [-cl cluster_name] [-co component_name]	Returns the state of all components. Example: dcmtl getState

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:

- [Metadata Repository Schema Descriptions](#)
- [Metadata Repository Schemas, Tablespaces, and Default Datafiles](#)

C.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 Schemas](#)
These schemas are used for Oracle Application Server management.

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.

C.1.1 Identity Management Schemas

[Table C-1](#) lists the schemas used by Identity Management components, sorted alphabetically by component.

Table C-1 *Identity Management Schemas*

Component	Schema	Description
Oracle Internet Directory	ODS	For internal use
OracleAS Certificate Authority	OCA	For internal use
OracleAS Certificate Authority	ORAOCA_PUBLIC	For internal use
OracleAS Single Sign-On	ORASSO	For internal use

Table C–1 (Cont.) Identity Management Schemas

Component	Schema	Description
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

C.1.2 Product Metadata Schemas

Table C–2 lists the schemas used by middle-tier application components, sorted alphabetically by component.

Table C–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.
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 Integration B2B	B2B	Contains the 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 Integration B2B	IP	N/A ¹
Oracle BPEL Process Analytics	BAM	Contains instance and metadata database objects for Oracle BPEL Process Analytics.
Oracle BPEL Process Manager	ORABPEL	Contains instance and metadata database objects for Oracle BPEL Process Manager.
OracleAS Portal	PORTAL	Contains Portal database objects and code. This schema also represents the proxy user account that <code>mod_plsql</code> uses to connect to the database through the credentials provided in the corresponding DAD.
OracleAS Portal	PORTAL_APP	Contains information for authentication of external JSP applications.
OracleAS Portal	PORTAL_DEMO	Contains demonstration code.

Table C–2 (Cont.) Product Metadata Schemas

Component	Schema	Description
OracleAS Portal	PORTAL_PUBLIC	OracleAS Portal schema for all lightweight users, who 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 UDDI Registry	UDDISYS	Contains UDDI entities such as business entities, business services, binding templates, tModels, and publisher assertions; taxonomy structures such as North American Industry Classification System (NAICS), Universal Standard Products and Services Codes (UNSPSC), and ISO 3166 Geographic Taxonomy (ISO 3166); UDDI replication-related internal tables; and other administration-related views and tables.
OracleAS Web Clipping	WCRSYS	Web Clipping Repository for support with OracleAS 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.
OracleBI 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.
N/A	DSGATEWAY ²	N/A

¹ Beginning with Oracle Application Server 10g Release 2 (10.1.2), the IP schema contains no data. It has been replaced by the B2B schema and is provided only for backward compatibility.

² Beginning with Oracle Application Server 10g Release 2 (10.1.2), the DSGATEWAY schema is not used. It is provided for backward compatibility.

C.1.3 Management Schemas

Table C–3 lists the management schemas.

Table C–3 Management Schema

Component	Schema	Description
Distributed Configuration Management (DCM)	DCM	Contains configuration information for OC4J and Oracle HTTP Server instances, application server instances, OracleAS Clusters, and farms.
Oracle Enterprise Manager	OEM_REPOSITORY	Repository for Database Control

C.2 Metadata Repository Schemas, Tablespaces, and Default Datafiles

Table C–4 lists the tablespace and default datafile for each Metadata Repository schema. It is sorted alphabetically by component.

Table C-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 Enterprise Manager	OEM_REPOSITORY	SYS_AUX	sysaux01.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	SYSAUX	sysaux01.dbf
Oracle Ultra Search	WKPROXY	SYSAUX	sysaux01.dbf
Oracle Ultra Search	WKSYS	SYSAUX	sysaux01.dbf
Oracle Workflow	OWF_MGR	IAS_META	ias_meta01.dbf
OracleAS Certificate Authority	OCA	OCATS	oca.dbf
OracleAS Certificate Authority	ORAOCA_PUBLIC	OCATS	oca.dbf
OracleAS Integration B2B	B2B	B2B_DT	b2b_dt.dbf
OracleAS Integration B2B	B2B	B2B_RT	b2b_rt.dbf
OracleAS Integration B2B	B2B	B2B_LOB	b2b_lob.dbf
OracleAS Integration B2B	B2B	B2B_IDX	b2b_idx.dbf
OracleAS Integration B2B	IP ¹	N/A	N/A
Oracle BPEL Process Analytics	BAM	BAM	bam.dbf
Oracle BPEL Process Manager	ORABPEL	ORABPEL	orabpel.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
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 UDDI Registry	UDDISYS	UDDISYS_TS	uddisys01.dbf
OracleAS Web Clipping	WCRSYS	WCRSYS_TS	wcrsys01.dbf

Table C-4 (Cont.) Metadata Repository Tablespaces and Default Datafiles

Component	Schema	Tablespace	Default Datafile
OracleAS Wireless	WIRELESS	IAS_META	ias_meta01.dbf
OracleBI Discoverer	DISCOVERER5	DISCO_PTM5_META	discopl1m1.dbf
OracleBI Discoverer	DISCOVERER5	DISCO_PTM5_CACHE	discopl1m1
N/A	DSGATEWAY ²	DSGATEWAY_TAB	oss_sys01.dbf

¹ Beginning with Oracle Application Server 10g Release 2 (10.1.2), the IP schema does not contain any data. It has been replaced by the B2B schema and is provided only for backward compatibility.

² Beginning with Oracle Application Server 10g Release 2 (10.1.2), the DSGATEWAY schema is not used. It is provided for backward compatibility.

Index

A

adapters
 cloning and, 8-2
administration tools, 2-1 to 2-11
Application Server Control Console, 2-2
 updating port numbers, 4-6
 URL for, 2-5
 using, 2-4
Application Server home page, 2-2, 2-6
archive logging, 9-14
ARCHIVELOG mode, 9-14

B

B2B
 See OracleAS Integration B2B
B2B schema
 description, C-2
B2B_DT tablespace, C-4
B2B_IDX tablespace, C-4
B2B_LOB tablespace, C-4
B2B_RT tablespace, C-4
backup and recovery, 9-1 to 9-22
 adding files, 9-6
 backup procedures, 9-14
 block change tracking, 9-14
 complete environment, 9-17
 creating record of environment, 9-16
BAM schema
 description, C-2
bkp_restore.pl file, 9-1

C

Certificate Authority
 See OracleAS Certificate Authority
changing IP address, 6-14
changing ports, 4-1 to 4-10
chgiphost command, 6-5
 errors, 6-12
 setting log level, 6-11
cloning, 8-1
 clusters, 8-2
 limitations, 8-2
 log files, 8-7

Oracle Application Server Adapters and, 8-2
Oracle Content Management SDK, 8-2
Oracle Identity Management and, 8-2
Oracle Workflow, 8-2
OracleAS Clusters, 8-2
OracleAS Infrastructure and, 8-2
OracleAS Integration B2B, 8-2
OracleAS Integration InterConnect, 8-2
OracleAS Metadata Repository and, 8-2
 port numbers and, 8-3
 using command line, 8-3
CM SDK
 See Oracle Content Management Software
 Development Kit
component topology, 2-9
components
 disabling, 3-5
 enabling, 3-5
 starting and stopping, 3-4
 using Application Server Control Console, 3-5
 using opmnctl, 3-5
configuring network, 6-1

D

Database Control
 password, 2-11
 using, 2-11
DCM
 See Distributed Configuration Management (DCM)
DCM schema
 description, C-3
DCM tablespace, C-4
dcmctl command, 2-4
DHCP address
 changing, 6-14
 moving off-network, 6-14
 moving to, 6-13
diagnostic messages, 5-8
diagnostics, 5-1
disabling components, 3-5
DISCO_PTM5_CACHE tablespace, C-5
DISCO_PTM5_META tablespace, C-5
Discoverer
 See OracleBI Discoverer
DISCOVERER5 schema

- description, C-3
- DISPLAY environment variable, 1-1
- Distributed Configuration Management (DCM), 1-5, 2-3
 - commands, B-1
 - datafile, C-4
 - log files, 5-2
 - schema, C-3
 - starting, 3-1, 3-3
 - stopping, 3-2, 3-4
 - tablespace, C-4
- domain name
 - changing, 6-1
 - middle tier, 6-2
- DSGATEWAY schema
 - description, C-3
- DSGATEWAY_TAB tablespace, C-5
- Dynamic Monitoring Service (DMS), 2-3

E

- enabling components, 3-5
- environment variables, 1-1

F

- farm
 - home page, 2-6
- file-based repositories
 - changing domain name and, 6-3
 - changing hostname and, 6-3

H

- home pages, 2-2
 - Application Server, 2-6
 - OracleAS Farm, 2-6
- hostname
 - changing, 6-1
 - after Windows 2000 upgrade, 6-12
 - middle tier, 6-2
 - references to, 6-8

I

- ias_admin password
 - changing, 1-7
- IAS_META tablespace, C-4, C-5
- Infrastructure
 - See OracleAS Infrastructure*
- INTERNET_APPSERVER_REGISTRY schema, C-1
- IP address
 - changing, 6-1, 6-14
 - moving off-network, 6-13
 - moving to static address, 6-13
- IP schema
 - description, C-2

J

- J2EE

- changing domain name and, 6-3
- changing hostname and, 6-3
- J2EE applications
 - monitoring, 2-10

L

- LD_LIBRARY_PATH environment variable, 1-1
- LD_LIBRARY_PATH_64 environment variable, 1-1
- LIBPATH environment variable, 1-2
- Load Balancing Router
 - cloning and, 8-3
- log files, 5-1 to 5-9
 - cloning and, 8-7
 - configuring, 5-3
 - listing, 5-4
 - searching, 5-5
 - viewing, 5-5
- log loader, 5-6
 - cloning and, 8-2
 - diagnostic messages, 5-8
 - enabling, 5-7
 - log files, 5-2
 - setting properties, 5-7
 - starting and stopping, 5-6
 - updating configuration, 5-7
- log message formats, 5-1
- log repository, 5-3
- logging, 5-1 to 5-9

M

- management schemas, C-1, C-3
- Metadata Repository
 - See OracleAS Metadata Repository*
- middle-tier instances
 - changing domain name, 6-2
 - changing hostname, 6-2
 - changing IP address, 6-2
 - changing port numbers, 4-10
 - SSL communication paths, 7-6
 - SSL configuration tasks, 7-8
 - starting, 3-1, 3-3
 - stopping, 3-2, 3-4
- mod_osso
 - re-register, 4-7
- mod_osso.conf file
 - ports and, 4-8
- monitoring, 5-1
 - application server components, 2-10
 - J2EE applications, 2-10
 - with Application Server Control, 2-8
- multiple installations on one host, 1-2

N

- Net Listener
 - starting, 3-1, 3-3
 - stopping, 3-2, 3-3
- network configurations, 6-1

O

OCA

See OracleAS Certificate Authority

OCA schema

description, C-1

OCATS tablespace, C-4

ODL

See Oracle Diagnostic Logging (ODL)

ODS schema

description, C-1

OEM_REPOSITORY schema

description, C-3

off-network, 6-13

moving on-network

DHCP address, 6-13

static IP address, 6-13

OID

See Oracle Internet Directory

OLTS_ATTRSTORE tablespace, C-4

OLTS_BATTRSTORE tablespace, C-4

OLTS_CT_STORE tablespace, C-4

OLTS_DEFAULT tablespace, C-4

OLTS_SVRMGSTORE tablespace, C-4

on-network, 6-13

moving off-network

DHCP address, 6-14

IP address, 6-13

OPMN *See* Oracle Process Manager and Notification Server (OPMN)

opmnctl command, A-1

opmnctl command, 2-4, 3-5

ORABPEL schema, C-2

Oracle Application Development Framework

cloning and, 8-2

log files, 5-2

Oracle Application Server Adapters

cloning and, 8-2

Oracle Application Server Containers for J2EE (OC4J), 1-6

configuring SSL, 7-8

log files, 5-2

Oracle Application Server environment, 3-6

complete backup, 9-17

starting and stopping, 3-6

Oracle BPEL Process Analytics

log files, 5-2

schema, C-2

Oracle BPEL Process Manager

log files, 5-2

schema, C-2

Oracle Business Intelligence

cloning and, 8-2

SSL protocols and, 7-9

Oracle Content Management Software Development Kit

changing domain name, 6-3

changing hostname, 6-3

cloning and, 8-2

log files, 5-2

Oracle Delegated Administration Services

configuring SSL, 7-6

updating ports, 4-9

Oracle Diagnostic Logging (ODL), 5-1

Oracle Directory Integration and Provisioning
configuring SSL, 7-6

Oracle Enterprise Manager, 2-1

configuring SSL, 7-11

datafiles, C-4

home pages, 2-2

log files, 5-2

schema, C-3

tablespaces, C-4

Oracle Enterprise Manager 10g Grid Control, 2-1, 2-3

Oracle Enterprise Manager Application Server
Control, 2-1

Application Server home page, 2-6

home pages

for components, 2-8

OracleAS Farm home page, 2-6, 2-7

Oracle Enterprise Manager Application Server
Control Console

starting, 3-3

stopping, 3-3

URL for, 2-5

using, 2-4

Oracle HTTP Server, 1-6

configuring SSL, 7-8

log files, 5-2

modify listen and port directives, 4-5

ports

changing, 4-5

starting, 3-1, 3-3

stopping, 3-2, 3-4

Oracle Identity Management

cloning and, 8-2

configuring SSL, 7-6

schemas, C-1

starting, 3-1, 3-3

stopping, 3-3

Oracle Internet Directory

changing domain name, 6-3

changing hostname, 6-3

configuring SSL, 7-6

datafiles, C-4

log files, 5-2

schema, C-1

SSL and, 7-4

tablespaces, C-4

Oracle Internet Directory Manager, 1-6

Oracle Internet Directory Replication Server
configuring SSL, 7-6

Oracle Management Agent, 2-3

Oracle Management Watchdog Process, 2-3

Oracle Process Manager and Notification Server
(OPMN), 1-5, 2-3

commands, A-1

log files, 5-2

Oracle Ultra Search

changing domain name, 6-7

- changing host name, 6-7
- datafile, C-4
- schemas, C-2
- tablespace, C-4
- Oracle Universal Installer
 - log files, 5-2
- Oracle Workflow
 - cloning and, 8-2
 - datafile, C-4
 - schema, C-2
 - tablespace, C-4
- ORACLE_HOME environment variable, 1-2
- ORACLE_SID environment variable, 1-2
- OracleAS Backup and Recovery, 9-1 to 9-22
- OracleAS Backup and Recovery Tool, 9-1 to 9-13
 - configuring, 9-3
 - customizing, 9-5
 - excluding files, 9-6
 - installing, 9-2
 - obtaining, 9-1
 - prerequisites, 9-6
 - syntax, 9-6
 - usage, 9-6
- OracleAS Certificate Authority
 - administration interface, 1-6
 - datafiles, C-4
 - log files, 5-2
 - schemas, C-1
 - tablespaces, C-4
 - updating ports, 4-9
- OracleAS Cluster
 - changing domain name and, 6-3
 - changing hostname and, 6-3
 - cloning and, 8-2
- OracleAS Farm home page, 2-2, 2-6, 2-7
- OracleAS Forms
 - log files, 5-2
- OracleAS Forms Services
 - accessing, 1-6
- OracleAS Infrastructure
 - cloning and, 8-2
 - SSL configuration tasks, 7-5
 - starting, 3-1, 3-3
 - stopping, 3-3
- OracleAS Integration B2B
 - cloning and, 8-2
 - datafiles, C-4
 - log files, 5-2
 - schema, C-2
 - tablespaces, C-4
- OracleAS Integration InterConnect
 - cloning and, 8-2
 - log files, 5-2
- OracleAS Integration InterConnect Adapters
 - cloning and, 8-2
- OracleAS Metadata Repository
 - cloning and, 8-2
 - datafile, C-4
 - enabling archive logging, 9-14
 - managing, 8-1
- managing with Database Control, 2-11
- schemas, C-1 to C-5
- starting, 3-1, 3-3
- stopping, 3-3
- tablespace, C-4
- OracleAS Portal, 1-6
 - changing domain name and, 6-7
 - changing hostname and, 6-7
 - configuring SSL, 7-10
 - datafiles, C-4
 - schemas, C-2
 - tablespaces, C-4
- OracleAS Reports Server
 - log files, 5-2
- OracleAS Reports Services
 - accessing, 1-6
- OracleAS Single Sign-On
 - administration pages, 1-6
 - changing domain name, 6-7
 - changing hostname, 6-7
 - changing port, 4-5
 - configuring SSL, 7-6
 - datafile, C-4
 - log files, 5-2
 - schemas, C-1
 - tablespace, C-4
 - updating port numbers, 4-6
- OracleAS TopLink
 - backup and recovery tool and, 9-1, 9-2
 - log files, 5-2
- OracleAS UDDI Registry
 - datafile, C-4
 - schema, C-3
 - tablespace, C-4
- OracleAS Web Cache, 1-6
 - changing domain name and, 6-3
 - changing hostname and, 6-3
 - configuring SSL, 7-8
 - log files, 5-2
 - starting, 3-1, 3-3
 - stopping, 3-2, 3-4
- OracleAS Web Clipping
 - datafile, C-4
 - schema, C-3
 - tablespace, C-4
- OracleAS Wireless, 1-6
 - changing domain name and, 6-7
 - changing hostname and, 6-7
 - configuring SSL, 7-9
 - datafile, C-5
 - log files, 5-2
 - schema, C-3
 - tablespace, C-5
- OracleBI Discoverer, 1-6
 - configuring SSL, 7-9
 - datafiles, C-5
 - log files, 5-2
 - schema, C-3
 - tablespaces, C-5
- ORAoca_PUBLIC schema

- description, C-1
- ORASSO schema
 - description, C-1
- ORASSO_DS schema
 - description, C-2
- ORASSO_PA schema
 - description, C-2
- ORASSO_PS schema
 - description, C-2
- ORASSO_PUBLIC schema
 - description, C-2
- OWF_MGR schema
 - description, C-2

P

- passwords
 - changing `ias_admin`, 1-7
 - Database Control, 2-11
- PATH environment variable, 1-2
- port numbers
 - cloning and, 8-3
 - less than 1024, 4-6
 - listing, 1-4
- port tunneling
 - cloning and, 8-2
 - log files, 5-2
- Portal
 - See* OracleAS Portal
- PORTAL schema
 - description, C-2
- PORTAL tablespace, C-4
- PORTAL_APP schema
 - description, C-2
- PORTAL_DEMO schema
 - description, C-2
- PORTAL_DOC tablespace, C-4
- PORTAL_IDX tablespace, C-4
- PORTAL_LOG tablespace, C-4
- PORTAL_PUBLIC schema
 - description, C-3
- `portlist.ini`, 1-4
- ports
 - changing, 4-1 to 4-10
 - Oracle HTTP Server, 4-5
- postinstallation tasks, 1-1

R

- re-register `mod_osso`, 4-7
- resource usage, 2-9
- `runstartupconsole` command, 2-3
 - starting Application Server instances, 3-1
 - starting Infrastructure, 3-3
 - starting middle tiers, 3-4
 - stopping Application Server instances, 3-2
 - stopping Infrastructure, 3-3
 - stopping middle tiers, 3-4

S

- schemas
 - for OracleAS Metadata Repository, C-1
 - management, C-1, C-3
 - Oracle Identity Management, C-1
 - product metadata, C-1, C-2
- Secure Sockets Layer (SSL), 7-1
 - communication paths
 - for middle tier, 7-6
 - configuration paths, 7-3
 - configuration tasks
 - for infrastructure, 7-5
 - for middle tier, 7-8
 - configuration tool, 7-1
 - overview, 7-1
- security, 7-1
- `setupinfo.txt` file, 2-5
- SHLIB_PATH environment variable, 1-1
- Single Sign-On
 - See* OracleAS Single Sign-On
- SSL
 - See* Secure Sockets Layer (SSL)
- SSLConfigTool script, 7-2, 7-8
- SSO
 - See* OracleAS Single Sign-On
- start command
 - `opmnctl`, A-1
- startall command
 - `opmnctl`, A-1
- starting
 - Application Server Control Console, 3-3
 - Application Server instance, 3-1
 - DCM, 3-1, 3-3
 - middle-tier instances, 3-1, 3-3
 - Net Listener, 3-1, 3-3
 - Oracle HTTP Server, 3-1, 3-3
 - Oracle Identity Management, 3-1, 3-3
 - OracleAS Infrastructure, 3-1, 3-3
 - OracleAS Metadata Repository, 3-1, 3-3
 - OracleAS Web Cache, 3-1, 3-3
- starting and stopping, 3-1 to 3-7
 - using Application Server Control Console, 3-5
 - using `opmnctl`, 3-5
 - using `runstartupconsole`, 3-1, 3-2
- startproc command
 - `opmnctl`, A-1
- static IP address
 - moving off-network, 6-13
 - moving to, 6-13
- status command
 - `opmnctl`, A-2
- stopall command
 - `opmnctl`, A-1
- stopping
 - Application Server Control Console, 3-3
 - Application Server instance, 3-2
 - DCM, 3-2, 3-4
 - Net Listener, 3-2, 3-3
 - Oracle HTTP Server, 3-2, 3-4
 - Oracle Identity Management, 3-3

- OracleAS Infrastructure, 3-3
- OracleAS Metadata Repository, 3-3
- OracleAS Web Cache, 3-2, 3-4
- stopping and starting, 3-1 to 3-7
- stopproc command
 - opmnctl, A-2
- symbolic links
 - cloning and, 8-3
- SYSAUX tablespace, C-4

- cloning and, 8-3

T

- tablespaces
 - for schemas, C-1
- TEMP environment variable, 1-2
- TMP environment variable, 1-2
- TopLink
 - See* OracleAS TopLink
- topology
 - viewing, 2-9

U

- UDDI Registry
 - See* OracleAS UDDI Registry
- UDDISYS schema
 - description, C-3
- UDDISYS_TS tablespace, C-4
- UIX
 - cloning and, 8-2
- Ultra Search
 - See* Oracle Ultra Search

V

- virtual hosts
 - SSL and, 7-9

W

- WCRSYS schema
 - description, C-3
- WCRSYS_TS tablespace, C-4
- Web Clipping
 - See* OracleAS Web Clipping
- Wireless
 - See* OracleAS Wireless
- wireless schema
 - description, C-3
- WK_TEST schema
 - description, C-2
- WKPROXY schema
 - description, C-2
- WKSYS schema
 - description, C-2
- Workflow
 - See* Oracle Workflow

X

- XDK