Oracle® Application Server

Installation Guide

10*g* (10.1.4.0.1) for Solaris Operating System (SPARC 64-Bit)

B32088-01

September 2006

ORACLE®

Oracle Application Server Installation Guide 10*g* (10.1.4.0.1) for Solaris Operating System (SPARC 64-Bit)

B32088-01

Copyright © 2006, Oracle. All rights reserved.

Primary Authors: Brintha Bennet, Megan Ginter

Contributors: Rupesh Das, Nagesh Jayaram, Suresh Kesavan, Arun Kuzhimattathil, Sonal Pandey, Divya Shankar, Janelle Simmons, Shashidhara Varamballi

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 USA, Inc., 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 Siebel 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 xiii

Intended Audience xiii
Documentation Accessibility xiii
Related Documents xiv
Conventions xiv

1 Product and Installation Overview

1.1 Product Overview 1-1
1.2 Where Do I Find Installation Instructions for My Product? 1-2
1.3 Recommended Topologies 1-3
1.3.1 Installing Oracle Identity Management in a Single Oracle Home 1-5
1.3.2 Installing a Distributed Oracle Identity Management with an Integrated Oracle HTTP Server 1-5
1.3.3 Installing a Distributed Oracle Identity Management with a Standalone Oracle HTTP Server 1-7

2 Requirements

2.1 Using Oracle*MetaLink* to Obtain the Latest Oracle Application Server Hardware and Software Requirements 2-2
2.2 System Requirements 2-2
2.2.1 Tips for Reducing Memory Usage 2-7
2.3 Operating System Patches 2-7
2.4 Operating System Packages 2-9
2.5 Kernel Parameters 2-9
2.6 Ports 2-12
2.6.1 Checking If a Port Is in Use 2-13
2.6.2 Using Default Port Numbers 2-13
2.6.3 Using Custom Port Numbers (the "Static Ports" Feature) 2-14
2.6.3.1 Format of the staticports.ini File 2-14
2.6.3.2 Error Conditions that Will Cause the Installer to Use Default Ports Instead of Specified Ports 2-16
2.6.3.3 Example 2-16
2.6.4 If Port 1521 Is in Use 2-16
2.6.4.1 If Port 1521 Is In Use by an Existing Oracle Database 2-17
2.6.4.2 If Port 1521 Is In Use by Some Other Application 2-19
2.7 Operating System Groups 2-19

2.7.1 Create a Group for the Inventory Directory 2-20
2.7.2 Create Groups for Database Administrators 2-20
2.8 Operating System User 2-21
2.9 Environment Variables 2-22
2.9.1 Environment Variable Tips 2-22
2.9.2 ORACLE_HOME and ORACLE_SID 2-23
2.9.3 PATH, CLASSPATH, and LD_LIBRARY_PATH 2-23
2.9.4 DISPLAY 2-23
2.9.5 TNS_ADMIN 2-23
2.9.6 TMP 2-24
2.10 The /etc/hosts File 2-24
2.10.1 Location of the Default Oracle Identity Management Realm 2-24
2.10.2 Hostname for OracleAS Single Sign-On 2-25
2.11 Network Topics 2-25
2.11.1 Installing on Multihomed (Multi-IP) Computers 2-26
2.11.2 Copying CD-ROMs or DVD-ROM to Hard Drive, and Installing from the Hard Drive.. 2-26
2.11.3 Installing from a Remote CD-ROM or DVD-ROM Drive 2-27
2.11.4 Installing on Remote Computers 2-28
2.11.5 Installing on NFS-Mounted Storage 2-29
2.11.6 Running Multiple Instances from One Installation 2-29
2.11.7 Support for NIS and NIS+ 2-30
2.12 Font Packages for Java 2-30
2.13 Prerequisite Checks Performed by the Installer 2-30

3 Things You Should Know Before Starting the Installation

3.1 Oracle Home Directory 3-1
3.1.1 Installing in an Existing Oracle Home 3-2
3.1.2 Installing in a Non-Empty Oracle Home 3-2
3.2 Can I Use Symbolic Links? 3-2
3.3 First-Time Installation of Any Oracle Product 3-2
3.4 Installing Additional Languages 3-3
3.5 Oracle Application Server Instances and Instance Names 3-3
3.6 The ias_admin User and Restrictions on its Password 3-4
3.7 Comparing Installing Components against Configuring Components 3-5
3.8 Where Does the Installer Write Files? 3-5
3.9 Why Do I Need to be Able to Log In as Root at Certain Times During Installation? 3-6
3.10 Running root.sh During Installation 3-6
3.11 Can I Modify Other Oracle Application Server Instances During Installation? 3-6
3.12 Connecting to Oracle Internet Directory Through SSL Connections 3-7
3.13 Obtaining Software from Oracle E-Delivery 3-7
3.13.1 Finding and Downloading the Oracle Application Server 10*g* (10.1.4.0.1) E-Pack 3-7
3.13.2 Finding Required and Optional Downloads 3-7
3.13.3 Disk Space Requirements 3-7
3.13.4 Software Requirements for Unzipping Files 3-7
3.13.5 Extracting Software from the Zip Files 3-8
3.14 Setting the Mount Point for the CD-ROM or DVD-ROM 3-8

3.15 Starting the Oracle Universal Installer ... 3-9

4 Installing OracleAS Infrastructure

4.1 Infrastructure Installation Types ... 4-1
4.2 Why Would I Select the Different Infrastructure Installation Types? ... 4-2
4.3 Order of Installation for the Infrastructure ... 4-3
4.4 Can I Install Components on Separate Computers? ... 4-4
4.5 Tips for Installing Oracle Identity Management Components Separately ... 4-5
4.6 Do I Need the Oracle Delegated Administration Services or the Oracle Directory Integration Platform Components? ... 4-6
4.7 Can I Configure Components After Installation? ... 4-6
4.8 Can I Use an Existing Database for the OracleAS Metadata Repository? ... 4-6
4.9 Can I Use an Existing Oracle Internet Directory? ... 4-7
4.10 Registration of OracleAS Metadata Repository in Oracle Internet Directory and Password Randomization ... 4-7
4.11 Contents of the OracleAS Metadata Repository ... 4-8
4.12 Can I Use Multiple Metadata Repositories? ... 4-9
4.13 What High Availability Options Does Oracle Application Server Support? ... 4-10
4.14 Restrictions on the Passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP Users 4-10
4.15 Support for NE8ISO8859P10 and CEL8ISO8859P14 Characters Sets ... 4-11
4.16 What Do I Enter in the "Specify Namespace in Internet Directory" Screen? ... 4-11
4.17 How to Determine Port Numbers Used by Components ... 4-11
4.18 Can I Add OCA After Installation? ... 4-12
4.19 How to Deploy Oracle Delegated Administration Services on a Separate Host ... 4-12
4.20 Installing OracleAS Infrastructure ... 4-12
4.21 Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory ... 4-14
4.22 Installing OracleAS Metadata Repository in a New Database ... 4-15
4.23 Installing Oracle Identity Management Components Only (Including Oracle Internet Directory) ... 4-16
4.24 Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory) ... 4-18
4.25 Installing Oracle Internet Directory Only ... 4-20
4.26 Installing OCA and OracleAS Metadata Repository Only ... 4-21
4.27 Install Fragment: The First Few Screens of the Installation ... 4-23
4.28 Install Fragment: The Last Few Screens of the Installation ... 4-25
4.29 Install Fragment: Database Screens ... 4-26
4.30 Install Fragment: OCA Screens ... 4-27

5 Configuring Oracle Internet Directory for Oracle Application Server Installation Privileges

5.1 Default Users in Oracle Internet Directory ... 5-1
5.2 Groups in Oracle Internet Directory ... 5-2
5.2.1 "Global" Groups ... 5-2
5.2.2 Groups for Each Metadata Repository ... 5-3
5.2.3 Groups for Each Component ... 5-3
5.3 Groups Required to Configure or Deinstall Components ... 5-4
5.4 Groups Required to Install Middle Tiers ... 5-7

5.4.1 Groups Required to Install Against the Desired Metadata Repository 5-7
5.4.2 Groups Required to Install Middle-tier Components 5-7
5.4.3 Example 5-7
5.5 Groups Required to Install Additional Metadata Repositories 5-8
5.6 Example of Installation with Different Users 5-8
5.7 How to Create Users in Oracle Internet Directory 5-10
5.8 How to Add Users to Groups in Oracle Internet Directory 5-10
5.8.1 Using Oracle Directory Manager to Add Users to Groups 5-11
5.8.1.1 Navigating to "Global" Groups 5-11
5.8.1.2 Navigating to Metadata Repository Groups 5-12
5.8.1.3 Navigating to Component Groups 5-13
5.8.2 Using Deployment Delegation Console to Add Users to Groups 5-14
5.9 Contents of a New Oracle Internet Directory 5-16
5.10 On the Specify Login for Oracle Internet Directory Screen, What Username and Realm Do I Enter? 5-16

6 Installing Oracle Internet Directory in Replicated Mode

6.1 Oracle Internet Directory Replication Overview 6-1
6.1.1 Fan-Out Replication (LDAP Replication) 6-2
6.1.2 Multimaster Replication (Advanced Replication) 6-2
6.2 Requirements 6-3
6.2.1 Database Requirements 6-3
6.2.2 Clock Synchronization 6-4
6.3 Installation Order 6-4
6.4 Installing a Master Oracle Internet Directory 6-4
6.5 Installing an Oracle Internet Directory Replica 6-5
6.5.1 Overview of Installing a Replica 6-5
6.5.2 Installing an Oracle Internet Directory Replica with a New Database 6-5
6.5.3 Installing an Oracle Internet Directory Replica against an Existing Database 6-8
6.6 Accessing OracleAS Single Sign-On and Oracle Delegated Administration Services .. 6-10

7 Installing in High Availability Environments: Overview

7.1 Overview of High Availability Configurations 7-1
7.1.1 OracleAS Cold Failover Cluster 7-1
7.1.2 OracleAS Clusters 7-3
7.1.3 OracleAS Disaster Recovery 7-4
7.1.4 Summary of Differences 7-4
7.2 Installation Order for High Availability Configurations 7-4
7.3 Requirements for High Availability Configurations 7-5
7.3.1 Check Minimum Number of Nodes 7-5
7.3.2 Check That Groups Are Defined Identically on All Nodes 7-5
7.3.3 Check the Properties of the oracle User 7-5
7.3.4 Check for Previous Oracle Installations on All Nodes 7-6

8 Installing in High Availability Environments: OracleAS Cold Failover Cluster

8.1 OracleAS Cold Failover Cluster: Introduction 8-1

8.2 Pre-Installation Steps for OracleAS Cold Failover Cluster 8-2
8.2.1 Map the Virtual Hostname and Virtual IP Address 8-2
8.2.2 Set Up a File System That Can Be Mounted from Both Nodes 8-4
8.2.3 Review Recommendations for Automatic Storage Management (ASM) 8-5
8.2.4 Check That Clusterware Is Running (Automated Failovers only) 8-5
8.2.5 Modify listener.ora file for Existing Database 8-5
8.3 Installing an OracleAS Cold Failover Cluster (Infrastructure) Configuration 8-6
8.3.1 OracleAS Cold Failover Cluster (Infrastructure): Overview of Installation Steps 8-8
8.3.2 OracleAS Cold Failover Cluster (Infrastructure): Details of Installation Steps 8-8
8.4 Installing a Distributed OracleAS Cold Failover Cluster (Infrastructure) Configuration 8-11
8.4.1 Distributed OracleAS Cold Failover Cluster (Infrastructure): Overview of Installation Steps 8-13
8.4.2 Distributed OracleAS Cold Failover Cluster (Infrastructure): Details of Installation Steps 8-13
8.5 Installing an OracleAS Cold Failover Cluster (Identity Management) Configuration.. 8-14
8.5.1 OracleAS Cold Failover Cluster (Identity Management): Overview of Installation Steps 8-16
8.5.2 OracleAS Cold Failover Cluster (Identity Management): Details of Installation Steps \ 8-17
8.6 Installing a Distributed OracleAS Cold Failover Cluster (Identity Management) Configuration 8-19
8.6.1 Distributed OracleAS Cold Failover Cluster (Identity Management): Overview of Installation Steps 8-21
8.6.2 Distributed OracleAS Cold Failover Cluster (Identity Management): Details of Installation Steps 8-22
8.7 Installing Oracle Delegated Administration Services and OracleAS Single Sign-On in an OracleAS Cold Failover Cluster 8-24
8.7.1 Oracle Delegated Administration Services and OracleAS Single Sign-On in OracleAS Cold Failover Cluster: Overview of Installation Steps 8-26
8.7.2 Oracle Delegated Administration Services and OracleAS Single Sign-On in OracleAS Cold Failover Cluster: Details of Installation Steps 8-26
8.8 Installing Only the OracleAS Metadata Repository in an OracleAS Cold Failover Cluster Environment 8-30
8.9 Post-Installation Steps for OracleAS Cold Failover Cluster 8-31
8.9.1 Edit the ORACLE_HOME/Apache/Apache/htdocs/index.html File 8-31
8.9.2 Copy the /var/opt/oracle Directory to the Other Node 8-31
8.9.3 Running Database Console against a Cold Failover Cluster Database 8-31
8.9.4 Create a Clusterware Agent for Automatic Failover 8-32
8.10 Installing Middle Tiers Against an OracleAS Cold Failover Cluster Infrastructure 8-32
8.10.1 If You Plan to Install Middle Tiers on OracleAS Cold Failover Cluster Nodes 8-32
8.10.1.1 Create a staticports.ini File for the Middle Tier 8-32
8.10.1.2 Rename the /var/opt/oracle Directory Used for the Infrastructure 8-33
8.10.2 Procedure for Installing Middle Tiers Against an OracleAS Cold Failover Cluster Infrastructure 8-33
8.11 Installing Regular Middle-Tiers on OracleAS Cold Failover Cluster Nodes 8-34

9 Installing in High Availability Environments: OracleAS Cluster (Identity Management)

9.1 OracleAS Cluster (Identity Management): Introduction 9-1
9.2 Pre-Installation Steps for OracleAS Cluster (Identity Management) 9-2
9.2.1 Use the Same Path for the Oracle Home Directory (recommended) 9-2
9.2.2 Synchronize Clocks on All Nodes 9-3
9.2.3 Configure Virtual Server Names and Ports for the Load Balancer 9-3
9.2.4 Configure Your LDAP Virtual Server 9-3
9.2.4.1 Load Balancer Supports LDAP Service Monitoring 9-4
9.2.4.2 Load Balancer Does Not Support LDAP Service Monitoring 9-4
9.3 About Oracle Internet Directory Passwords 9-4
9.4 About Configuring SSL and Non-SSL Ports for Oracle HTTP Server 9-5
9.4.1 Case 1: Client ---[HTTP]---> Load Balancer ---[HTTP]---> Oracle HTTP Server 9-5
9.4.2 Case 2: Client ---[HTTPS]---> Load Balancer ---[HTTPS]---> Oracle HTTP Server 9-6
9.4.3 Case 3: Client ---[HTTPS]---> Load Balancer ---[HTTP]---> Oracle HTTP Server 9-6
9.5 Installing an OracleAS Cluster (Identity Management) Configuration 9-7
9.5.1 Installation Order 9-8
9.5.2 Installing OracleAS Metadata Repository 9-9
9.5.3 Installing OracleAS Cluster (Identity Management) on the First Node 9-9
9.5.3.1 Create staticports.ini File 9-9
9.5.3.2 Disable TCP Monitoring on Load Balancer for First Node 9-10
9.5.3.3 Configure the Load Balancer to Return Immediately to the Calling Client 9-10
9.5.3.4 Ensure that the OracleAS Metadata Repository Is Not Registered with any Oracle Internet Directory 9-10
9.5.3.5 Select the Same Components for Each Node 9-10
9.5.3.6 Run the Installer 9-10
9.5.4 Installing OracleAS Cluster (Identity Management) on Subsequent Nodes 9-12
9.6 Installing a Distributed OracleAS Cluster (Identity Management) Configuration 9-15
9.6.1 Installation Order 9-17
9.6.2 Installing OracleAS Metadata Repository 9-17
9.6.3 Installing Oracle Internet Directory on the First Node 9-17
9.6.3.1 Set up staticports.ini File 9-17
9.6.3.2 Select the Same Components for Each Installation 9-18
9.6.3.3 Start the Installer 9-18
9.6.4 Installing Oracle Internet Directory on Subsequent Nodes 9-19
9.6.4.1 Staticports.ini File Not Needed 9-19
9.6.4.2 Select the Same Components for Each Installation 9-19
9.6.4.3 Start the Installer 9-19
9.6.5 Installing OracleAS Single Sign-On and Oracle Delegated Administration Services on Each Node 9-21
9.6.5.1 Set up staticports.ini File 9-21
9.6.5.2 Start the Installer 9-22
9.7 Post-Installation Steps 9-24
9.7.1 Cluster the OC4J_Security Instance for State Replication (First Oracle Delegated Administration Services node only) 9-24
9.7.2 Changing the Ports for Oracle Internet Directory 9-25
9.7.3 Update targets.xml (Case 2 only) 9-25

9.8 Installing Middle Tiers Against OracleAS Cluster (Identity Management) Configurations... 9-26

10 Installing in High Availability Environments: OracleAS Disaster Recovery

10.1 OracleAS Disaster Recovery: Introduction 10-1
10.2 Setting up the OracleAS Disaster Recovery Environment 10-3
10.2.1 Ensure Nodes Are Identical at the Operating System Level 10-3
10.2.2 Set Up staticports.ini File 10-3
10.2.3 Set Up Identical Hostnames on Both Production and Standby Sites 10-4
10.2.4 If You Want to Use OracleAS Cold Failover Cluster on the Production Site 10-8
10.3 Installing Oracle Application Server in an OracleAS Disaster Recovery Environment 10-8
10.3.1 Installing the OracleAS Infrastructure 10-9
10.3.2 Installing Middle Tiers 10-9
10.4 Installing the OracleAS 10g (10.1.2.0.2) Standalone Install of OracleAS Guard into Oracle Homes 10-9
10.5 Patching OracleAS Guard Release 10.1.2.0.0 with Release 10.1.2.0.2 10-10
10.6 What to Read Next 10-11

11 Post-Installation Tasks

11.1 State of Oracle Application Server Instances After Installation 11-1
11.2 Passwords for Oracle Application Server Components 11-1
11.3 NFS Installations 11-2
11.4 Backup and Recovery 11-2
11.5 SSL 11-2
11.6 Operating System Locale and NLS_LANG Environment Variable 11-2
11.6.1 Check the Operating System Locale 11-2
11.6.2 Check the NLS_LANG Setting 11-2
11.7 Component Configuration After Installation 11-3
11.7.1 Configuring mod_osso (Required for Oracle Delegated Administration Services) 11-3
11.8 Components that Require Post-Installation Tasks 11-5
11.9 What to Do Next 11-5

A Installing the Oracle Identity Management Grid Control Plug-in

A.1 Installation Requirements A-1
A.2 Starting the Grid Control Plug-in Installer A-1
A.3 Installing Oracle Identity Management Grid Control Plug-in A-2
A.4 Installing Oracle Identity Management Grid Control Plug-in Agent A-3

B Silent and Non-Interactive Installation

B.1 Silent Installation B-1
B.2 Non-Interactive Installation B-2
B.3 Pre-Installation B-2
B.4 Notes for Silent and Non-Interactive Installations B-3
B.4.1 Installing OracleAS Certificate Authority B-3
B.5 Create the Response File B-3

B.5.1 Creating Response Files from Templates B-3
B.5.2 Creating Response Files by Using the Record Mode in the Installer B-4
B.5.3 Variables to Modify in the Response Files B-4
B.5.4 Example Response Files B-4
B.5.4.1 Example Response File for OracleAS Infrastructure: Oracle Identity Management Only B-5
B.5.4.2 Example Response File for OracleAS Infrastructure: OracleAS Metadata Repository Only B-6
B.5.4.3 Example Response File for OracleAS Infrastructure: Identity Management and OracleAS Metadata Repository B-8
B.5.4.4 Example Response File for Oracle Identity Federation B-10
B.6 Start the Installation B-11
B.7 Post-Installation B-11
B.8 Security Tips for Silent and Non-Interactive Installations B-11
B.9 Deinstallation B-12

C Default Port Numbers

C.1 Method of Assigning Default Port Numbers C-1
C.2 Default Port Numbers C-1
C.3 Ports to Open in Firewalls C-3

D Deinstallation and Reinstallation

D.1 Deconfig Tool D-1
D.1.1 Parameters D-2
D.1.2 Log Files Generated by the Deconfig Tool D-3
D.2 Deinstallation Procedure: Overview D-3
D.3 Deinstalling OracleAS Cold Failover Cluster Installations D-4
D.4 Deinstalling OracleAS Single Sign-On Instances in OracleAS Cluster (Identity Management) D-4
D.5 Deinstalling OracleAS Cluster (Identity Management) D-5
D.6 Deinstalling OracleAS Infrastructure D-5
D.6.1 Deinstallation Order D-5
D.6.2 Deinstallation Steps D-5
D.7 Harmless Errors in the Log File D-7
D.8 Cleaning Up Oracle Application Server Processes D-8
D.9 Reinstallation D-8
D.10 Troubleshooting D-8

E Configuration Assistants

E.1 Troubleshooting Configuration Assistants E-1
E.1.1 General Tips E-1
E.1.2 Configuration Assistant Result Codes E-2
E.2 Description of Oracle Application Server Configuration Assistants E-2

F Troubleshooting

F.1 Log Files F-1

F.2 General Troubleshooting Tips F-1
F.3 Installation Problems and Solutions F-2
F.3.1 Location of Log Files F-2
F.3.2 Linking Failed, ORA Errors F-3
F.3.3 Prerequisite Checks Fail at the Start of Installation F-3
F.3.4 Message About Installing in a Non-Empty Directory F-3
F.3.5 Messages About SHMMAX and SEMMSL F-4
F.3.6 Installer Disappears After Running the Pre-Installation Checks F-4
F.3.7 Unable to Clean Up a Failed Installation F-5
F.3.8 Forgot the Password for the cn=orcladmin Account F-5
F.3.9 cn=orcladmin Account Becomes Locked F-5
F.3.10 User Interface Does Not Display in the Desired Language, or Does Not Display Properly F-5
F.3.11 Installer Does Not Display Correct Database Name for OracleAS Metadata Repository F-6
F.3.12 Configuration Assistant Failures - General F-6
F.3.13 OracleAS Randomize Password Configuration Assistant Failures F-7
F.3.14 Database Configuration Assistant (DBCA) Failures F-7
F.3.15 Harmless Error Message from Database Configuration Assistant (DBCA) F-8
F.3.16 OPMN Configuration Assistant - Start HTTP Server Failures F-8
F.3.17 OPMN Configuration Assistant - Start DAS Instance Failures F-9
F.3.18 OPMN Configuration Assistant - Start OCA Failures F-9
F.3.19 WARNING: DCM service may not be available at this time F-9
F.3.20 OracleAS Cluster (Identity Management)- Cluster Configuration Assistant Fails. F-10
F.3.21 OracleAS Cluster (Identity Management) - Installation Fails on Second Oracle Internet Directory Node F-10
F.3.22 OracleAS Cluster (Identity Management) - Installation Fails on Second Oracle Delegated Administration Services and OracleAS Single Sign-On Node F-10
F.4 Deinstallation Problems and Solutions F-11
F.4.1 Obsolete Partner URLs Still Remain on the OracleAS Single Sign-On Administration Screen F-11
F.4.2 Unable to Reuse Instance Name of a Deleted Instance F-12
F.4.3 Unable to Reuse Database Name F-12
F.4.4 Deconfiguration Failed on Distributed OracleAS Cluster (Identity Management) F-13
F.5 Need More Help? F-14

Index

Preface

The *Oracle Application Server Installation Guide* covers requirements, new features in the Oracle Universal Installer, Oracle Application Server concepts that affect installation, installation procedures, and troubleshooting tips. In addition, this guide also provides some sample topologies for installing and running Oracle Application Server.

Intended Audience

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

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

For additional information, see the following manuals:

- *Oracle Application Server Administrator's Guide*
- *Oracle Application Server Concepts*
- *Oracle Application Server High Availability Guide*

Conventions

The following text conventions are used in this document:

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

1

Product and Installation Overview

This chapter describes what is contained in Oracle Application Server and recommended topologies. It contains the following sections:

- Section 1.1, "Product Overview"
- Section 1.2, "Where Do I Find Installation Instructions for My Product?"
- Section 1.3, "Recommended Topologies"

1.1 Product Overview

Oracle Application Server is made up of a middle tier and OracleAS Infrastructure. You deploy and run your applications on the middle tiers. The infrastructure provides services that are used by middle tiers. These services can be shared by one or more middle tiers.

Oracle Application Server 10*g* (10.1.4.0.1) provides a comprehensive Identity and Access Management solution. The Identity and Access Management Suite includes:

- Oracle Internet Directory: Provides scalable, robust LDAP V3-compliant directory services implemented on the Oracle Database.
- Oracle Identity Federation: Provides standards-based, multi-protocol, and cross-domain single sign-on.
- Oracle Security Developer Tools: Provides a APIs for developing federation and secure web services applications.
- Oracle Access Manager: Provides a state-of-the-art solution for centralized identity administration and access control.
- Oracle Identity Manager: Provides a powerful and flexible enterprise identity management system that automatically manages users' access privileges within enterprise IT resources.
- Oracle Virtual Directory: Provides Internet and industry-standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

In addition to the Identity and Access Management Suite, this release provides a revision of OracleAS Infrastructure, which includes the following Oracle Identity Management components and OracleAS Metadata Repository:

- Oracle Internet Directory: A scalable, robust LDAP V3-compliant directory service implemented on the Oracle Database.

- Oracle Directory Integration Platform: A component of Oracle Internet Directory designed to perform directory synchronization with third party directory products.
- Oracle Application Server Certificate Authority: A component that issues, revokes, renews, and publishes X.509v3 certificates to support PKI-based strong authentication methods.
- Oracle Application Server Single Sign-On (OracleAS Single Sign-On): Provides single sign-on access to Oracle and third-party Web applications.
- Oracle Delegated Administration Services: Provides trusted proxy-based administration of directory information by users and application administrators.
- OracleAS Metadata Repository: Provides a collection of schemas used by other Oracle Application Server components.
- Oracle Enterprise Manager 10*g* Application Server Control Console: Enables you to manage and configure the OracleAS Infrastructure.

This guide focuses on installation instructions for OracleAS Infrastructure. See Section 1.2, "Where Do I Find Installation Instructions for My Product?" for the location of installation instructions for other components.

You can integrate Oracle Application Server 10*g* (10.1.4.0.1) Identity Management with an existing Oracle Application Server environment that includes:

- 10*g* (9.0.4), 10*g* Release 2 (10.1.2), or 10*g* Release 3 (10.1.3) middle tier
- 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) OracleAS Metadata Repository

You can integrate Oracle Application Server 10*g* (10.1.4.0.1) Metadata Repository with an existing Oracle Application Server environment that includes:

- 10*g* Release 2 (10.1.2) middle tier
- 10*g* (9.0.4) or 10*g* Release 2 (10.1.2) Identity Management

> **See Also:** *Oracle Application Server Upgrade and Compatibility Guide* for more information about which specific versions are compatible with 10*g* (10.1.4.0.1).

1.2 Where Do I Find Installation Instructions for My Product?

Table 1–1 summarizes the products available in Oracle Application Server 10*g* (10.1.4.0.1) and the books where the installation instructions are located.

Table 1–1 Product and Installation Documentation Locations

Product	See This Documentation for Installation Details
OracleAS Infrastructure	Chapter 4, "Installing OracleAS Infrastructure"
Oracle Identity Federation	*Oracle Identity Federation Administrator's Guide*
Oracle Identity Management Grid Control Plug-in	Appendix A, "Installing the Oracle Identity Management Grid Control Plug-in"
OracleAS Metadata Repository in an existing database	*Oracle Application Server Metadata Repository Creation Assistant User's Guide*
Oracle Access Manager	*Oracle Access Manager Installation Guide*

1.3 Recommended Topologies

Table 1–2 provides a road map of where to find information about the supported 10*g* (10.1.4.0.1) topologies.

Table 1–2 Recommended Topologies

Topology	See This Documentation for Details
10.1.4.0.1 OracleAS Infrastructure Topologies	
An Oracle Application Server instance containing all Oracle Identity Management components in one Oracle home.	Section 1.3.1, "Installing Oracle Identity Management in a Single Oracle Home"
Two Oracle Homes, one containing Oracle HTTP Server, OracleAS Single Sign-On, and Oracle Delegated Administration Services. and the other containing Oracle Internet Directory and Oracle Directory Integration Platform.	Section 1.3.2, "Installing a Distributed Oracle Identity Management with an Integrated Oracle HTTP Server"
Three Oracle Homes, one containing Oracle HTTP Server, a second containing OracleAS Single Sign-On and Oracle Delegated Administration Services. and a third containing Oracle Internet Directory and Oracle Directory Integration Platform.	Section 1.3.3, "Installing a Distributed Oracle Identity Management with a Standalone Oracle HTTP Server"
An enterprise data center for J2EE applications that uses one of the following methods for user authentication: ▪ OracleAS Single Sign-On ▪ Oracle Access Manager ▪ Oracle Application Server Java Authentication and Authorization Service (JAAS) Provider LDAP Each of these topologies contains a web tier, an application tier, and a data tier. The three tiers are separated by firewalls.	"myJ2EECompany," in the *Oracle Application Server Enterprise Deployment Guide*
Oracle Identity Federation Topologies	
An Oracle Identity Federation instance configured with OracleAS Infrastructure so that it is integrated with OracleAS Single Sign-On.	"Deploying Oracle Identity Federation with OracleAS Single Sign-On," in the *Oracle Identity Federation Administrator's Guide*
An Oracle Identity Federation instance configured with OracleAS Infrastructure and Oracle Access Manager.	"Deploying Oracle Identity Federation with Oracle Access Manager," in the *Oracle Identity Federation Administrator's Guide*
High-Availability Topologies	
An OracleAS Cluster (Identity Management) configuration in which two or more Oracle Identity Management instances serve the same content. A load balancer distributes requests equally among the active instances.	Chapter 9, "Installing in High Availability Environments: OracleAS Cluster (Identity Management)"

Table 1–2 (Cont.) Recommended Topologies

Topology	See This Documentation for Details
An OracleAS Cold Failover Cluster configuration in which two or more OracleAS Infrastructure or Oracle Identity Management instances serve the same content, but only one instance is active at any one time.	Chapter 8, "Installing in High Availability Environments: OracleAS Cold Failover Cluster"
An OracleAS Disaster Recovery configuration in which a standby site mirrors a production site. During normal operation, the production site handles all the requests. If the production site goes down, the standby site takes over and handles all the requests.	Chapter 10, "Installing in High Availability Environments: OracleAS Disaster Recovery"
An active-active topology in which two or more Oracle Access Manager instances serve the same content. A load balancer distributes requests equally among the active instances.	"High Availability for Oracle Access Manager" in the *Oracle Application Server High Availability Guide*
An OracleAS Cold Failover Cluster configuration in which two or more Oracle Identity Federation instances serve the same content, but only one instance is active at any one time.	"High Availability for Oracle Identity Federation" in the *Oracle Application Server High Availability Guide*
OracleAS Cold Failover Cluster or Real Application Clusters configurations for OracleAS Metadata Repository.	"High Availability for OracleAS Metadata Repository" in the *Oracle Application Server High Availability Guide*
10.1.4.0.1 OracleAS Infrastructure with Existing 10.1.2 or 10.1.3 Environments	
10.1.2 or 10.1.3 Middle Tiers: Configure a 10*g* Release 2 (10.1.2) or 10*g* Release 3 (10.1.3) middle-tier instance to use a new 10*g* (10.1.4.0.1) OracleAS Infrastructure. This topology also supports associating a 10*g* Release 2 (10.1.2) or 10*g* Release 3 (10.1.3) middle-tier instance with a new 10*g* (10.1.4.0.1) Oracle Identity Management for the following scenarios: ■ Moving to a new host ■ Creating a failover environment ■ Moving applications from a test environment to a new production environment	"Configuring 10.1.2 and 10.1.3 Middle Tiers to Use OracleAS Infrastructure" in the *Oracle Application Server Administrator's Guide* "Moving Identity Management to a New Host" in *Oracle Application Server Administrator's Guide* "Changing from a Test to a Production Environment" in the *Oracle Application Server Administrator's Guide*

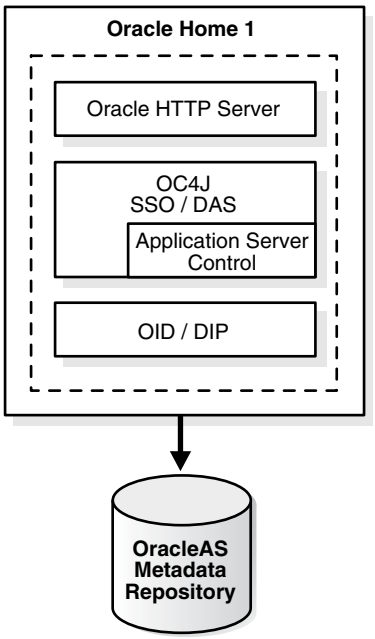
The remainder of this section addresses the recommended topologies for installing OracleAS Infrastructure instances. It contains the following topics:

- Section 1.3.1, "Installing Oracle Identity Management in a Single Oracle Home"
- Section 1.3.2, "Installing a Distributed Oracle Identity Management with an Integrated Oracle HTTP Server"
- Section 1.3.3, "Installing a Distributed Oracle Identity Management with a Standalone Oracle HTTP Server"

1.3.1 Installing Oracle Identity Management in a Single Oracle Home

This topology has all of the Oracle Identity Management components installed in the same Oracle home, as depicted in Figure 1–1. This topology can be associated with a 10*g* Release 2 (10.1.2) or 10*g* Release 3 (10.1.3) middle tier.

Figure 1–1 Oracle Identity Management in a Single Oracle Home



Requirements

The requirements are the same as those listed in Chapter 2, "Requirements".

Installation Sequence

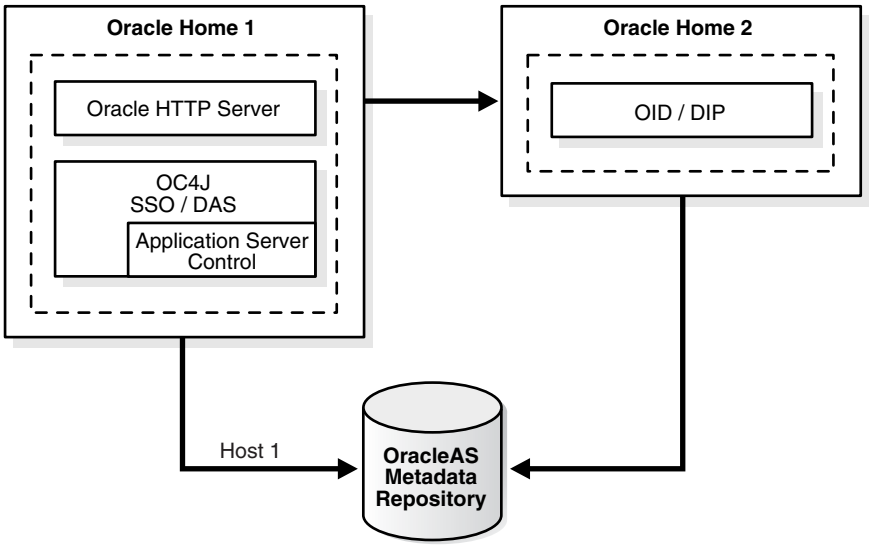
Perform an installation of Oracle Identity Management as described in Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)".

It is recommended that you install OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

1.3.2 Installing a Distributed Oracle Identity Management with an Integrated Oracle HTTP Server

In this topology, there are two Oracle Homes as depicted in Figure 1–2. The first Oracle Home contains Oracle HTTP Server, OracleAS Single Sign-On, and Oracle Delegated Administration Services. The second Oracle Home contains Oracle Internet Directory and Oracle Directory Integration Platform. This topology can be associated with a 10*g* Release 2 (10.1.2) or 10*g* Release 3 (10.1.3) middle tier.

Figure 1–2 Cluster with a Distributed Oracle Identity Management with an Integrated Oracle HTTP Server



Requirements

The requirements are the same as those listed in Chapter 2, "Requirements".

Installation Sequence

To install this topology:

1. Install OracleAS Metadata Repository on a shared disk. It is recommended that you install OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.
2. For Oracle Home 2, follow the installation instructions in Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)". On the Select Configuration Options screen, perform the following steps:
   - Select **Oracle Internet Directory**.
   - Do not select **Oracle Application Server Single Sign-On**.
   - Do not select **Oracle Application Server Delegated Administration Services**.
   - Select **Oracle Directory Integration Platform**.
   - Do not select **Oracle Application Server Certificate Authority (OCA)**.
   - Select **High Availability and Replication**.
3. For Oracle Home 1, follow the installation instructions in Section 4.24, "Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)". On the Select Configuration Options screen, perform the following steps:
   - Do not select **Oracle Internet Directory**.
   - Select **Oracle Application Server Single Sign-On**.
   - Select **Oracle Application Server Delegated Administration Services**.
   - Do not select **Oracle Directory Integration Platform**.
   - Do not select **Oracle Application Server Certificate Authority (OCA)**.

- Select **High Availability and Replication**.

4. On Oracle Home 2, perform the following commands to disable Oracle HTTP Server:

   a. Edit the *ORACLE_HOME*/opmn/bin/opmn.xml file to change the Oracle HTTP Server status to disabled, as shown in bold.

   ```
   <ias-component id="HTTP_Server" status="disabled" >     <process-type
   id="HTTP_Server" module-id="OHS">     <module-data>...</ias-component>
   ```

   b. Perform the following command to stop OPMN:

   ```
   prompt> ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

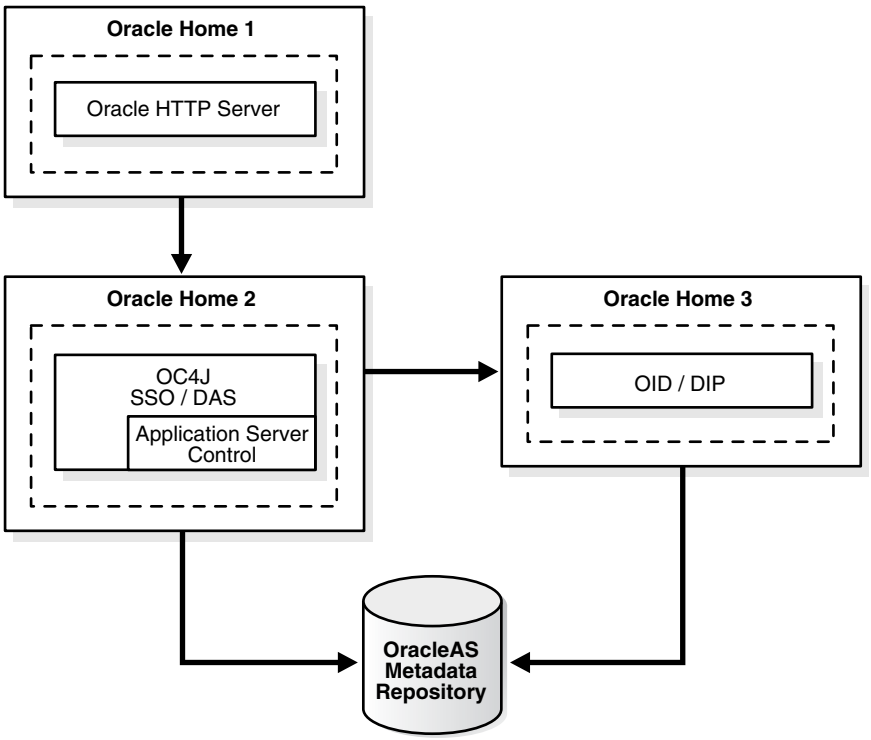
   c. Perform the following command to start OPMN:

   ```
   prompt> ORACLE_HOME/opmn/bin/opmnctl startall
   ```

1.3.3 Installing a Distributed Oracle Identity Management with a Standalone Oracle HTTP Server

In this topology, there are three Oracle Homes as depicted in Figure 1–3. The first Oracle Home contains Oracle HTTP Server. The second Oracle Home contains OracleAS Single Sign-On and Oracle Delegated Administration Services. The second Oracle Home contains Oracle Internet Directory and Oracle Directory Integration Platform. This topology can be associated with a 10*g* Release 2 (10.1.2) or 10*g* Release 3 (10.1.3) middle tier.

Figure 1–3 Cluster with a Distributed Oracle Identity Management with a Standalone Oracle HTTP Server



Requirements

The requirements are the same as those listed in Chapter 2, "Requirements".

Installation Sequence

To install this topology:

1. Install OracleAS Metadata Repository on a shared disk. It is recommended that you install OracleAS Metadata Repository in an existing database. See *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.
2. Install **Oracle HTTP Server with Apache 2.0** from Oracle Application Server Companion CD, included in the 10*g* Release 2 (10.1.2) or 10*g* Release 3 (10.1.3) CD Pack.
3. For Oracle Home 3, follow the installation instructions in Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)". On the Select Configuration Options screen, perform the following steps:
   - Select **Oracle Internet Directory**.
   - Do not select **Oracle Application Server Single Sign-On**.
   - Do not select **Oracle Application Server Delegated Administration Services**.
   - Select **Oracle Directory Integration Platform**.
   - Do not select **Oracle Application Server Certificate Authority (OCA)**.
   - Select **High Availability and Replication**.
4. For Oracle Home 2, follow the installation instructions in Section 4.24, "Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)". On the Select Configuration Options screen, perform the following steps:
   - Do not select **Oracle Internet Directory**.
   - Select **Oracle Application Server Single Sign-On**.
   - Select **Oracle Application Server Delegated Administration Services**.
   - Do not select **Oracle Directory Integration Platform**.
   - Do not select **Oracle Application Server Certificate Authority (OCA)**.
   - Select **High Availability and Replication**.
5. On Oracle Home 2 and 3, perform the following commands to disable Oracle HTTP Server:
   a. Edit the *ORACLE_HOME*/opmn/bin/opmn.xml file to change the Oracle HTTP Server status to disabled, as shown in bold.

      ```
      <ias-component id="HTTP_Server" status="disabled" >     <process-type
      id="HTTP_Server" module-id="OHS">     <module-data>...</ias-component>
      ```

   b. Perform the following command to stop OPMN:

      ```
      prompt> ORACLE_HOME/opmn/bin/opmnctl stopall
      ```

   c. Perform the following command to start OPMN:

      ```
      prompt> ORACLE_HOME/opmn/bin/opmnctl startall
      ```

6. Configure the standalone Oracle HTTP Server in Oracle Home 1. See "Configuring Standalone Oracle HTTP Server with Oracle Application Server" in *Oracle HTTP Server Administering a Standalone Deployment Based on Apache 2.0* in the 10*g* Release 2 (10.1.2) or 10*g* Release 3 (10.1.3) documentation library.

2

Requirements

Before installing Oracle Application Server, ensure that your computer meets the requirements described in this chapter.

Table 2–1 Sections in This Chapter

Section	Highlights
Section 2.1, "Using OracleMetaLink to Obtain the Latest Oracle Application Server Hardware and Software Requirements"	Describes how to find the most current requirements for Oracle Application Server 10*g* (10.1.4.0.1).
Section 2.2, "System Requirements"	Lists requirements such as supported operating systems, processor speed, memory, disk space, and swap space.
Section 2.3, "Operating System Patches"	Lists the required patches.
Section 2.4, "Operating System Packages"	Lists the required packages.
Section 2.5, "Kernel Parameters"	Lists required values for kernel parameters.
Section 2.6, "Ports"	Describes how to configure components to use ports other than the default ports.
Section 2.7, "Operating System Groups"	Describes why the operating system user who installs Oracle Application Server should belong to certain operating system groups.
Section 2.8, "Operating System User"	Describes why you should create an operating system user to install Oracle Application Server.
Section 2.9, "Environment Variables"	Describes how to set or unset environment variables required for installation.
Section 2.10, "The /etc/hosts File"	Describes how the installer uses the information in the `hosts` file. This section also describes how to specify the same information without editing the file.
Section 2.11, "Network Topics"	Describes network issues such as installing Oracle Application Server on a remote computer, using a remote CD-ROM/DVD-ROM drive, or installing from a hard disk.
Section 2.12, "Font Packages for Java"	Describes the font packages required if you want to run using different character sets.
Section 2.13, "Prerequisite Checks Performed by the Installer"	Lists the items checked by the installer, such as length of the Oracle home name and whether or not the Oracle home directory already contains another Oracle product.

2.1 Using Oracle*MetaLink* to Obtain the Latest Oracle Application Server Hardware and Software Requirements

The Oracle Application Server 10*g* (10.1.4.0.1) hardware and software requirements included in this guide were accurate at the time this manual was released to manufacturing. For the most up-to-date information about hardware and software requirements, refer to Oracle*MetaLink*:

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

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

2.2 System Requirements

Table 2–2 lists the system requirements for running Oracle Application Server. The installer checks many of these requirements at the start of the installation process and warns you if any of them is not met. To save time, you can manually check only the ones that are not checked by the installer. Refer to Table 2–2 to see which requirements are not checked by the installer.

You can also run the system checks performed by the installer without doing an installation, by running the `runInstaller` command as shown. The `runInstaller` command is on the Oracle Application Server CD-ROM (Disk 1) or DVD-ROM (in the `application_server` directory).

CD-ROM:

```
prompt> mount_point/1014disk1/runInstaller -executeSysPrereqs
```

DVD-ROM:

```
prompt> mount_point/application_server/runInstaller -executeSysPrereqs
```

The results are displayed on the screen as well as written to a log file. For more information on the types of checks performed, see Section 2.13, "Prerequisite Checks Performed by the Installer".

Table 2–2 System Requirements

Item	Requirement
Operating system	Solaris 8 or Solaris 9 or Solaris 10 See Section 2.3, "Operating System Patches" for a list of required patches. **Checked by Installer:** Yes
Network	You can install Oracle Application Server on a computer that is connected to a network, or on a "standalone" computer (not connected to the network). If you are installing Oracle Application Server on a standalone computer, you can connect the computer to a network after installation. You have to perform some configuration tasks when you connect it to the network; see the*Oracle Application Server Administrator's Guide* for details. **Checked by Installer:** No
IP	The computer's IP address must be static. Oracle Application Server does not support computers using Solaris DHCP. Oracle Application Server supports DHCP computers on Linux and Microsoft Windows. **Checked by Installer:** No

Table 2–2 (Cont.) System Requirements

Item	Requirement
Hostname	Ensure that your hostnames are not longer than 255 characters. **Checked by Installer:** No

Support for 32-bit and 64-bit applications	The operating system must be configured to support 32-bit and 64-bit applications. To check this, run the `isainfo` command with the `-v` option:
	`prompt>` **`/usr/bin/isainfo -v`**
	`64-bit sparcv9 applications`
	`32-bit sparc applications`
	
	If the output does not show both lines, you need to reconfigure your computer. Check with your system administrator.
	Checked by Installer: No

Processor Type	The processor must have a SPARC v9 architecture. This is because Oracle Application Server 10 *g* Release 2(10.1.2) uses the Sun Java 1.4.1 HotSpot Server VM, which no longer supports SPARC v8 and older processors.
	To determine the processor type, run the `psrinfo` command with the `-v` option. The output must show "`sparcv9`":
	`prompt>` **`/usr/sbin/psrinfo -v`**
	`Status of processor 0 as of: 02/10/03 13:21:20`
	`  Processor has been on-line since 02/04/03 15:45:07.`
	`  The sparcv9 processor operates at 450 MHz,`
	`  and has a sparcv9 floating point processor.`
	
	Checked by Installer: No

Processor Speed	450 MHz or greater recommended. Oracle recommends a multiple CPU computer.
	To determine the processor speed, run the `psrinfo` command with the `-v` option:
	`prompt>` **`/usr/sbin/psrinfo -v`**
	`Status of processor 0 as of: 02/10/03 13:21:20`
	`  Processor has been on-line since 02/04/03 15:45:07.`
	`  The sparcv9 processor operates at 450 MHz,`
	`  and has a sparcv9 floating point processor.`
	
	Checked by Installer: Yes

Table 2–2 (Cont.) System Requirements

Item	Requirement
Memory	OracleAS Infrastructure: ■ OracleAS Metadata Repository and Oracle Identity Management: 1 GB ■ Oracle Identity Management only: 1 GB ■ OracleAS Metadata Repository only: 1 GB Oracle Identity Federation: 512 **Notes:** ■ The installer checks the amount of memory on your computer and will warn you if your computer does not meet the minimum memory requirements. ■ These are minimum values that are enough to install and run Oracle Application Server. For most production sites, you should configure at least 1 GB of physical memory. For sites with substantial traffic, increasing the amount of memory further may improve performance. For Java applications, you should either increase the maximum heap allocated to the OC4J processes or configure additional OC4J processes to utilize this memory. See the *Oracle Application Server Performance Guide* for details. ■ To determine the optimal amount of memory for your installation, the best practice is to load test your site. Resource requirements can vary substantially for different applications and different usage patterns. In addition, some operating system utilities for monitoring memory can overstate memory usage, partially due to the representation of shared memory. The preferred method for determining memory requirements is to monitor the improvement in performance resulting from the addition of physical memory in your load test. Refer to your platform vendor documentation for information on how to configure memory and processor resources for testing purposes. To determine the amount of memory, use the `prtconf` command: `prompt>` **`/usr/sbin/prtconf	grep Memory`** **Checked by Installer:** Yes
Disk space	OracleAS Infrastructure: ■ OracleAS Metadata Repository and Oracle Identity Management: 4.83 GB You can install the data files for the OracleAS Metadata Repository database on a disk that is different from the disk where you are installing OracleAS Infrastructure. If you do this, make sure the disk for the Oracle Home has at least 2GB of free space and the disk for the data files has at least 2.8 GB of free space. ■ Oracle Identity Management only: 2.27 GB ■ OracleAS Metadata Repository only: 4.83 GB Oracle Identity Federation: 1 GB To determine the amount of free disk space, use the `df` command: `prompt>` **`df -k`** *`dir`* Replace *dir* with the directory where you plan to install Oracle Application Server or with the parent directory if the directory does not exist yet. For example, if you plan to install Oracle Application Server in `/opt/oracle/infra`, replace *dir* with `/opt/oracle` or `/opt/oracle/infra`. **Checked by Installer:** No

Table 2–2 (Cont.) System Requirements

Item	Requirement
Space in `/tmp` directory	250 MB To determine the amount of free space in the `/tmp` directory, use the `df` command: `prompt>` **`df -k /tmp`** If the `/tmp` directory does not have enough free space, you can specify a different directory by setting the TMP environment variable. See Section 2.9.6, "TMP" for details. **Checked by Installer:** Yes

Table 2–2 (Cont.) System Requirements

Item	Requirement

Swap space	1.5 GB or greater of available swap space
	To determine the amount of available swap space, use the `swap` command:
	`prompt> /usr/sbin/swap -l`
	
	The value in the "free" column indicates the number of free blocks, where a block is 512 bytes. To convert blocks to KB, divide the number by 2. For example, 2,000,000 free blocks is equivalent to 1,000,000 KB.
	If you do not have enough swap space, perform the following tasks:
	1. Log in as the root user, and create an empty swap file:
	`prompt> su`
	`Password: root_user_password`
	`# mkfile size m swap_file_name`
	
	Append an "m" to the size to specify the size in megabytes (example: `900m`). The minimum size of this file must be greater than the difference between the currently available swap space and required swap space. For example, if you have 100 MB of free swap space, then this swap file must be at least 1400 MB.
	2. Add the file to the swap space using the following command:
	`# /usr/sbin/swap -a swap_file_name`
	
	3. Add a line to `/etc/vfstab` file. If you do not add the line, the new swap space will not persist when you restart the computer.
	`/path/to/swap/file - - swap - no -`
	
	Replace */path/to/swap/file* with the location of the swap file.
	4. Verify the new swap space size:
	`prompt> /usr/sbin/swap -l`
	Checked by Installer: Yes

Monitor	256 color display To determine your monitor's display capabilities: **1.** Check that the DISPLAY environment variable is set properly. See Section 2.9.4, "DISPLAY" for details. To test, see if you are able to run `/usr/openwin/bin/xclock`. **2.** Run the `xwininfo` command. `prompt> /usr/openwin/bin/xwininfo` Look for the "Depth" line. You need a depth of at least 8 (bits per pixel). **Checked by Installer:** Yes
Supported browsers	Oracle Enterprise Manager 10*g* is supported on the following browsers: ■ Microsoft Internet Explorer 6.0 SP2 (supported on Microsoft Windows only) ■ Netscape 7.2 ■ Mozilla 1.7. You can download Mozilla from `http://www.mozilla.org`. ■ Firefox 1.0.4. You can download Firefox from `http://www.mozilla.org`. ■ Safari 1.2, 2.0 (on Apple Macintosh computers) For the most current list of supported browsers, check the Oracle*MetaLink* site (`http://metalink.oracle.com`). **Checked by Installer:** No. However, if you access Oracle Enterprise Manager 10*g* using a non-supported browser, you will get a warning message.

2.2.1 Tips for Reducing Memory Usage

If you need to reduce memory consumption:

- Configure only the components that you need.
- After installation, start up only the components that you need. See the *Oracle Application Server Administrator's Guide* for details.
- Run Application Server Control only when you need to administer an instance. In most cases, you do not need Application Server Control running all the time.

  If you are running multiple Oracle Application Server instances on one computer, each Application Server Control can consume a lot of memory. Running Application Server Control only when you need it can free up memory for other components.
- Configure Application Server Control so that it can manage multiple instances. See the *Oracle Application Server Administrator's Guide* for details.

2.3 Operating System Patches

Table 2–3 lists the Solaris operating system patches that you must install before installing. These are patches that make up the "J2SE patch cluster". You can download the patches from:

`http://sunsolve.sun.com`

Refer to the README file included with the patch for instructions on installing it.

Note: Although the patches listed in Table 2–3 are current at the time of publication, Sun Microsystems, Inc. often updates the list of required patches for J2SE. Click the "Readme" link on the following URL for the most current list of patches:

(`http://sunsolve.sun.com/search/advsearch.do?collection=all&max=10&language=en&queryKey1=Patches%20J2SE`)

Table 2–3 Required Patches for Solaris Operating Systems

Operating System	Patches Required
Solaris 8	■ 108652-82 or higher: X11 6.4.1: Xsun patch ■ 108921-21 or higher: CDE 1.4: dtwm patch ■ 108940-62 or higher: Motif 1.2.7 and 2.1.1: Runtime library patch ■ 108773-18 or higher: IIIM and X input and output method patch ■ 111310-01 or higher: /usr/lib/libdhcpagent.so.1 patch ■ 109147-28 or higher: Linker patch ■ 111308-04 or higher: /usr/lib/libmtmalloc.so.1 patch ■ 112438-03 or higher: /kernel/drv/random patch ■ 108434-17 or higher: 32-bit shared library patch for C++ ■ 108435-17 or higher: 64-bit shared library patch for C++ ■ 111111-04 or higher: /usr/bin/nawk patch ■ 112396-02 or higher: /usr/bin/fgrep patch ■ 110386-03 or higher: RBAC feature patch ■ 111023-03 or higher: /kernel/fs/mntfs and /kernel/fs/sparcv9/mntfs patch ■ 111317-05 or higher: /sbin/init and /usr/sbin/init patch ■ 113648-03 or higher: /usr/sbin/mount patch ■ 115827-01 or higher: /sbin/sulogin and /sbin/netstrategy patch ■ 116602-01 or higher: /sbin/uadmin and /sbin/hostconfig patch ■ 108987-13 or higher: Patch for patchadd and patchrm ■ 108528-29 or higher: Kernel update patch ■ 108989-02 or higher: /usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsys patch ■ 108993-36 or higher: LDAP2 client, libc, libthread and libnsl libraries patch ■ 109326-14 or higher: libresolv.so.2 and in.named patch ■ 110615-11 or higher: sendmail patch
Solaris 9	■ 113096-03 or higher: X11 6.6.1: OWconfig patch ■ 112785-35 or higher: X11 6.6.1: Xsun patch

How to Get a List of Operating System Patches Installed on Your Computer

To determine which patches are installed on your computer:

1. Run the `showrev` command with the `-p` option. The following command saves the sorted output to a file called `patchList`.

   ```
   prompt> showrev -p | sort > patchList
   ```

2. Open the file in a text editor, such as vi or emacs, and search for patch numbers.

How the Installer Checks for Operating System Patches

The installer searches for the required patch versions on your computer. If it does not find an exact match, it displays a warning message in the shell where you started the installer.

```
CD-ROM:  prompt> mount_point/10.1.4disk1/runInstaller
DVD-ROM: prompt> mount_point/application_server/runInstaller
...
... installer performs prerequisite checks here ...
...
```

```
Some optional pre-requisite checks have failed. Continue? (y/n) [n] n
```

The installer gives you a choice to exit or continue.

Type **n** to exit the installer if you do not have all the patches. You should download and install the patches.

Type **y** to continue only if you are sure all the required patches are installed.

2.4 Operating System Packages

Check that your computer contains the following operating system packages. If the packages are not present, the installer cannot continue.

- `SUNWarc`
- `SUNWbtool`
- `SUNWhea`
- `SUNWlibm`
- `SUNWlibms`
- `SUNWsprot`
- `SUNWsprox`
- `SUNWtoo`
- `SUNWi1of` (the character after the "i" is the number 1, not the letter "ell")
- `SUNWxwfnt`
- `SUNWi1cs` (the character after the "i" is the number 1, not the letter "ell")
- `SUNWi15cs` (the character after the "i" is the number 1, not the letter "ell")

The last two packages (`SUNWi1cs` and `SUNWi15cs`) are required for the ISO8859-1 and ISO8859-15 codesets.

To check if an operating system package is installed on your computer, run the `pkginfo` command with the name of the package. The syntax for running `pkginfo` is:

```
pkginfo package_name1 package_name2 ...
```

For example, to check if all of the listed packages are installed on your computer, run the following command:

```
prompt> pkginfo SUNWarc SUNWbtool SUNWhea SUNWlibm SUNWlibms SUNWsprot SUNWsprox
SUNWtoo SUNWi1of SUNWxwfnt SUNWi1cs SUNWi15cs
```

If your computer is missing a package, contact your system administrator.

2.5 Kernel Parameters

The computers on which you plan to install OracleAS Metadata Repository require their kernel parameters to be set to the minimum values shown in Table 2–4.

Kernel parameter values are stored in the `/etc/system` file. If your `/etc/system` file does not specify the parameters, you have to add lines to the file to specify them.

Notes:

- The values for kernel parameters are required only for computers that will be running the OracleAS Metadata Repository or OracleAS Web Cache. The installer checks the kernel parameter values only if you are installing these components.
- If any kernel parameter values do not meet the requirements, the installer displays an error message. You will not be able to continue the installation until you update the kernel parameters to the required values.
- If you update kernel parameter values, you need to restart your computer for the new values to take effect.

On Solaris 8 and Solaris 9, verify that the following kernel parameters are set to values greater than or equal to the recommended values shown:

Table 2–4 Kernel Parameters Required by OracleAS Metadata Repository

Parameter	Line in /etc/system Showing the Minimum Value	Description
`semmni`	`set semsys:seminfo_semmni=100`	Defines the maximum number of semaphore sets in the entire system.
`semmns`	`set semsys:seminfo_semmns=1024`	Defines the maximum semaphores on the system. The 256 is only a minimum value for computers that will be running a single database (the OracleAS Metadata Repository that you are installing). If you are already running a database on the computer, see "To determine the minimum value for the semmns parameter" on page 2-11.
`semmsl`	`set semsys:seminfo_semmsl=256`	Defines the minimum recommended value, for initial installation only.
`shmmax`	`set shmsys:shminfo_shmmax=4294967295`	Defines the maximum allowable size of one shared memory segment (4 GB = 4294967295).
`shmmin`	`set shmsys:shminfo_shmmin=1`	Defines the minimum allowable size of a single shared memory segment. **Note**: This parameter is not used in Solaris 9.
`shmmni`	`set shmsys:shminfo_shmmni=100`	Defines the maximum number of shared memory segments in the entire system.
`shmseg`	`set shmsys:shminfo_shmseg=10`	Defines the maximum number of shared memory segments one process can attach. **Note**: This parameter is not used in Solaris 9.

On Solaris 10, verify that the kernel parameters shown in the following table are set to values greater than or equal to the recommended value shown. The table aslo contains the resource controls that replace the /etc/system file for a specific kernel parameter.

Table 2–5 Recommended Kernel Parameter values and Resource Controls that Replace `/etc/system` ***files***

Parameter	Resource Control	Recommended Value
`noexec_user_stack`	`NA`	1
`semsys:seminfo_semmni`	`project.max-sem-ids`	100
`semsys:seminfo_semmsl`	`process.max-sem-nsems`	256
`shmsys:shminfo_shmmax`	`project.max-shm-memory`	4294967295
`shmsys:shminfo_shmni`	`project.max-shm-ids`	100

Notes: On Solaris 10, you are not required to make changes to the `/etc/system` file to implement the System V TPC. Solaris 10 uses the resource control facility for its implementation.

To determine the minimum value for the semmns parameter

If you are installing the OracleAS Metadata Repository on a computer that is not already running an Oracle database (that is, the OracleAS Metadata Repository will be the only Oracle database running on the computer), set the `semmns` parameter to a minimum of 256.

If you are installing the OracleAS Metadata Repository on a computer that is already running an Oracle database, set the `semmns` parameter to the sum of the `processes` initialization parameter for each Oracle database (including the OracleAS Metadata Repository), adding the largest one twice, and then adding an additional 10 for each database.

The default value of the `processes` parameter for the OracleAS Metadata Repository database is 150.

Example: The computer is already running an Oracle database, and its `processes` parameter is set at 200. In this case, you must set the `semmns` parameter to at least 770:

- Sum of the `processes` parameter for all Oracle database: 200 for the existing database + 150 for the OracleAS Metadata Repository that you are installing = 350
- Add the largest one twice: 200 + 200 = 400
- Add 10 for each database: 10 + 10 = 20
- Total: 350 + 400 + 20 = 770

To determine the value of the `processes` parameter for an Oracle database, run the following command in SQL*Plus:

```
prompt> sqlplus "sys/password as sysdba"
SQL> show parameters processes
```

password specifies the password for the SYS user.

To add or update kernel parameter values:

1. Become root user on the computer where you need to change the values.

2. Make a backup copy of the `/etc/system` file. For example, the following command makes a backup copy called `system.back`.

```
# cp /etc/system /etc/system.back
```

3. Using a text editor such as vi or emacs, update the values or add new lines in the `/etc/system` file as necessary. For example, the following lines show sample values for the parameters:

```
set semsys:seminfo_semmni=300
set semsys:seminfo_semmns=1024
set semsys:seminfo_semmsl=256
set shmsys:shminfo_shmmax=4294967295
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=512
set shmsys:shminfo_shmseg=150
```

Tip: The comment character for the `/etc/system` file is the asterisk (`*`), not `#`.

4. Restart the computer for the new values to take effect.

On Solaris 10, use the following procedure to view the current value specified for resource controls, and to change them if necessary:

1. To view the current values of the resource control, enter the following commands:

```
# id -p // to verify the project id
uid=0(root) gid=0(root) projid=1 (user.root)
# prctl -n project.max-shm-memory -i project user.root
# prctl -n project.max-sem-ids -i project user.root
```

2. If you must change any of the current values, then:

   a. To modify the value of max-shm-memory to 6 GB:

```
# prctl -n project.max-shm-memory -v 6gb -r -i project user.root
```

   b. To modify the value of max-sem-ids to 256:

```
# prctl -n project.max-sem-ids -v 256 -r -i project user.root
```

2.6 Ports

Many Oracle Application Server components, such as Oracle HTTP Server, OracleAS Web Cache, and Oracle Enterprise Manager 10*g*, use ports. You can have the installer assign default port numbers, or use port numbers that you specify.

- Section 2.6.1, "Checking If a Port Is in Use"
- Section 2.6.2, "Using Default Port Numbers"
- Section 2.6.3, "Using Custom Port Numbers (the "Static Ports" Feature)"
- Section 2.6.4, "If Port 1521 Is in Use"

Why the Default Port for Oracle HTTP Server Is Port 7777 and Not Port 80

By default, the installer configures Oracle HTTP Server to use port 7777, not port 80. Port 7777 is the default port because on UNIX, components that use port numbers lower than 1024 require additional steps to be done as the root user before the

components can run. Because the installer does not have root access, it has to use a port greater than 1024.

If you want Oracle HTTP Server to use a different port, such as port 80, use the "static ports" feature, which enables you to specify port numbers for components. Although you can change the port number after installation, it is easier to set the port number during installation.

2.6.1 Checking If a Port Is in Use

To check if a port is being used, you can run the `netstat` command as follows:

```
prompt> netstat -an | grep portnum
```

2.6.2 Using Default Port Numbers

If you want to use the default port numbers for components, you do not have to do anything. See Appendix C, "Default Port Numbers" for a list of the default port numbers and ranges. Make sure that at least one port is available in the port range for each component. If the installer is unable to find a free port in the range, the installation will fail.

Tip: The installer will not assign port numbers that are specified in the `/etc/services` file. If you do not want the installer to assign a specific port number, add the port number to the `/etc/services` file. For example, if you want to reserve port 7777 for an application, you can add something like the following line to `/etc/services`:

```
myApplication      7777/tcp
```

The installer will not assign port 7777 to any component if this line exists in the `/etc/services` file.

Note: In the default configuration of the Solaris operating system, the `/etc/services` file includes ports 389 and 636 (for LDAP and LDAP/SSL). These happen to be the default ports for Oracle Internet Directory. This means that if you want to use these port numbers for Oracle Internet Directory, you must either delete or comment out these lines in the `/etc/services` file. To comment out a line, add a # at the beginning of the line, as shown:

```
# ldap   389/tcp   # Lightweight Directory Access Protocol
# ldap   389/udp   # Lightweight Directory Access Protocol
# ldaps  636/tcp   # LDAP protocol over TLS/SSL (was sldap)
# ldaps  636/udp   # LDAP protocol over TLS/SSL (was sldap)
```

If you do not comment out or remove the lines from `/etc/services`, then the installer will not assign ports 389 and 636. It assigns a number from the port number range for Oracle Internet Directory. See Appendix C, "Default Port Numbers" for a list of default port numbers.

2.6.3 Using Custom Port Numbers (the "Static Ports" Feature)

To instruct the installer to assign custom port numbers for components:

1. Create a file containing the component names and port numbers. Section 2.6.3.1, "Format of the staticports.ini File" describes the file format. This file is typically called the `staticports.ini` file, but you can name it anything you want.
2. In the installer, on the Specify Port Configuration Options screen, select **Manual** and enter the *full path* to the `staticports.ini` file.

   If you do not specify the full path to the file, the installer will not be able to find the file. The installer will then assign default ports for all the components, and it will do this without displaying any warning.

> **Difference from Previous Release:** In 10*g* (9.0.4), you used command-line options to specify the staticports.ini file. In this release, you specify the file in the new Specify Port Configuration Options screen.

2.6.3.1 Format of the staticports.ini File

The `staticports.ini` file has the following format. Replace *port_num* with the port number that you want to use for the component.

```
# J2EE and HTTP Server
Oracle HTTP Server port = port_num
Oracle HTTP Server Listen port = port_num
Oracle HTTP Server SSL port = port_num
Oracle HTTP Server Listen (SSL) port = port_num
Oracle HTTP Server Diagnostic port = port_num
Java Object Cache port = port_num
DCM Discovery port = port_num
Oracle Notification Server Request port = port_num
Oracle Notification Server Local port = port_num
Oracle Notification Server Remote port = port_num
Application Server Control port = port_num
Application Server Control RMI port = port_num
Oracle Management Agent port = port_num
Log Loader port = port_num
ASG port = port_num

# Infrastructure
Oracle Internet Directory port = port_num
Oracle Internet Directory (SSL) port = port_num
Oracle Certificate Authority SSL Server Authentication port = port_num
Oracle Certificate Authority SSL Mutual Authentication port = port_num
```

The easiest way to create the file is to use the `staticports.ini` file on the CD-ROM (Disk 1) or DVD-ROM as a template:

1. Copy the `staticports.ini` file from the CD-ROM or DVD-ROM to your hard disk.

Table 2–6 Location of the staticports.ini File on CD-ROM and DVD-ROM

Media	Location of staticports.ini File
CD-ROM	Disk 1: *mount_point*`/1014disk1/stage/Response/staticports.ini`
DVD-ROM	*mount_point*`/application_server/stage/Response/staticports.ini`

2. Edit the local copy (the file on the hard disk) to include the desired port numbers.

   You do not need to specify port numbers for all components in the `staticports.ini` file. If a component is not listed in the file, the installer uses the default port number for that component.

   Note that the `staticports.ini` may contain ports for components that are not included in 10*g* (10.1.4.0.1).

   You cannot change the port used by the OracleAS Metadata Repository (port 1521) during installation, but you can do so after installation. See the *Oracle Application Server Administrator's Guide* for details.

   The following example sets the Application Server Control port and some OracleAS Web Cache ports. For components not specified, the installer will assign the default port numbers.

   ```
   Application Server Control port = 2000
   Oracle Internet Directory port = 2001
   Oracle Internet Directory (SSL) port = 2002
   ```

   When installation is complete, you can check the `ORACLE_HOME/install/portlist.ini` file to see the assigned ports.

   Notes on Choosing Port Numbers:

   - Port numbers cannot be greater than 65535.
   - If you use a port number less than 1024 for a component, you must run the component as the root user.
   - If you use a port number less than 1024 for a component, the installer will not be able to start up the component at the end of installation. You may need to configure the component first before you can start it up. See the appropriate component documentation for details.
   - You still have to comment out ports 389 and 636 in the `/etc/services` file if you want to use these port numbers for Oracle Internet Directory. See the Note on page 2-13 for details.

The installer verifies that the ports specified in the file are available by checking memory. This means that it can only detect ports that are being used by running processes. It does not look in configuration files to determine which ports an application is using.

If the installer detects that a specified port is not available, it displays an alert. The installer will not assign a port that is not available. To fix this:

1. Edit the `staticports.ini` file to specify a different port, or shut down the application that is using the port.
2. Click **Retry**. The installer re-reads the `staticports.ini` file and verifies the entries in the file again.

Using portlist.ini as the staticports.ini File

The `staticports.ini` file uses the same format as the `ORACLE_HOME/install/portlist.ini` file, which is created *after* an Oracle Application Server installation. If you have installed Oracle Application Server and you want to

use the same port numbers in another installation, you can use the `portlist.ini` file from the first installation as the `staticports.ini` file for subsequent installations.

However, note this difference: in `staticports.ini`, the line "`Oracle Management Agent port`" corresponds to "`Enterprise Manager Agent port`" in `portlist.ini`.

2.6.3.2 Error Conditions that Will Cause the Installer to Use Default Ports Instead of Specified Ports

Check your `staticports.ini` file carefully because a mistake can cause the installer to use default ports without displaying any warning. Here are some things that you should check:

- If you specify the same port for more than one component, the installer will use the specified port for the first component, but for the other components, it will use the components' default ports. The installer does not warn you if you have specified the same port for multiple components.
- If you specify different ports for one component on multiple lines, the installer assigns the default port for the component. The installer does not warn you if you have specified different ports for one component.
- If you specify the same port for one component on multiple lines, the installer assigns the default port for the component. The installer does not warn you if you have specified the same port on multiple lines.
- If you have syntax errors in the `staticports.ini` file (for example, if you omitted the = character for a line), the installer ignores the line. For the components specified on such lines, the installer assigns the default ports. The installer does not display a warning for lines with syntax errors.
- If you misspell a component name, the installer assigns the default port for the component. Names of components in the file are case sensitive. The installer does not display a warning for lines with unrecognized names.
- If you specify a non-numeric value for the port number, the installer ignores the line and assigns the default port number for the component. It does this without displaying any warning.
- If you specify a relative path to the staticports.ini file (for example, "`./staticports.ini`" or just "`staticports.ini`"), the installer will not find the file. The installer continues without displaying a warning and it will assign default ports to all components. You must specify a full path to the `staticports.ini` file.

2.6.3.3 Example

This example configures Oracle HTTP Server to use ports 80 and 443. Create a `staticports.ini` file that includes the following lines:

```
Oracle HTTP Server port = 80
Oracle HTTP Server Listen port = 80
Oracle HTTP Server SSL port = 443
Oracle HTTP Server Listen (SSL) port = 443
```

2.6.4 If Port 1521 Is in Use

The installer configures port 1521 for the OracleAS Metadata Repository listener (version 10.1.0.3). This port cannot be changed through the `staticports.ini` file.

> **Note:** If your computer has a listener that uses the IPC protocol with the EXTPROC key, you should change the key to have some other value. This is because the OracleAS Metadata Repository listener requires access to the EXTPROC key.

If port 1521 on your computer is already in use by an existing application, such as Oracle database listener or some other application, you might have to take some action before running the installer. See the following sections for details.

- Section 2.6.4.1, "If Port 1521 Is In Use by an Existing Oracle Database"
- Section 2.6.4.2, "If Port 1521 Is In Use by Some Other Application"

2.6.4.1 If Port 1521 Is In Use by an Existing Oracle Database

If you are installing a new database for the OracleAS Metadata Repository on a computer that is already running an Oracle database, ensure that the listeners for both databases do not conflict.

You might be able to use the same listener for both the existing database and the OracleAS Metadata Repository database. You have to consider the version of the existing listener as well as the port number. Table 2–7 shows scenarios and outcomes.

You can change the OracleAS Metadata Repository listener to use a different port after installation. See the *Oracle Application Server Administrator's Guide* for details.

Table 2–7 Scenarios and Outcomes if You Have an Existing Database on the Computer Where You Want to Install the OracleAS Metadata Repository

Version of the Existing Listener	Existing Listener Uses Port 1521	Existing Listener Uses a Port Other Than 1521
Earlier than 10.1.0.2	You need two listeners: one for the existing database and one for the OracleAS Metadata Repository. See Section 2.6.4.1.1, "Scenario 1: Existing Listener Uses Port 1521 and Listener Version Is Earlier Than 10.1.0.2".	You need two listeners: one for the existing database and one for the OracleAS Metadata Repository. See Section 2.6.4.1.3, "Scenario 3: Existing Listener Uses a Port Other Than 1521".
10.1.0.2 or later	The existing listener supports both the existing database and the OracleAS Metadata Repository. See Section 2.6.4.1.2, "Scenario 2: Existing Listener Uses Port 1521 and Listener Version Is 10.1.0.2 or Later"	You need two listeners: one for the existing database and one for the OracleAS Metadata Repository. See Section 2.6.4.1.3, "Scenario 3: Existing Listener Uses a Port Other Than 1521".

To check the listener version, run the following command:

```
prompt> $ORACLE_HOME/bin/lsnrctl VERSION
```

where ORACLE_HOME is the home directory for your database.

You can also use the same command to check the listener port.

Here is an example of the command's output:

```
prompt> lsnrctl VERSION
LSNRCTL for Solaris: Version 10.1.0.5 - Production on 12-JUL-2005 16:08:16

Copyright (c) 1991, 2004, Oracle.  All rights reserved.
```

```
Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-sun.us.oracle.com)(PORT=1521)))
TNSLSNR for Solaris: Version 10.1.0.5 - Production
        TNS for Solaris: Version 10.1.0.5 - Production
        Unix Domain Socket IPC NT Protocol Adaptor for Solaris: Version 10.1.0.5 -
Production
        Oracle Bequeath NT Protocol Adapter for Solaris: Version 10.1.0.5 -
Production
The command completed successfully
```

2.6.4.1.1 Scenario 1: Existing Listener Uses Port 1521 and Listener Version Is Earlier Than 10.1.0.2 Listeners earlier than version 10.1.0.2 are **not compatible** with the OracleAS Metadata Repository from this Oracle Application Server release. What you need to do is to install the OracleAS Metadata Repository, which installs a version 10.1.0.3 listener. You can then use this new listener to service your existing database and the OracleAS Metadata Repository database.

1. Stop the existing listener before you install the OracleAS Metadata Repository.

   ```
   prompt> $ORACLE_HOME/bin/lsnrctl stop
   ```

   ORACLE_HOME is the home directory for your existing database.

   If you do not stop the existing listener, the installation will fail.

2. Install the OracleAS Metadata Repository.

   See any of the procedures that install an OracleAS Metadata Repository in Chapter 4, "Installing OracleAS Infrastructure" (for example, Section 4.20, "Installing OracleAS Infrastructure" or Section 4.21, "Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory").

3. Update the configuration file of the new listener, as necessary. The name of the listener configuration file is `listener.ora`, located in the `ORACLE_HOME/network/admin` directory.

   a. Check network address entries in the existing listener's configuration file.

      If the existing listener's configuration file contains only the following network addresses:

      * TCP Port 1521
      * IPC key EXTPROC

      you do not have to edit the OracleAS Metadata Repository listener's configuration file for network addresses.

      If the configuration file contains other network addresses, you need to add them to the OracleAS Metadata Repository listener's configuration file.

   b. Check SID_DESC entries in the existing listener's configuration file.

      If the existing listener's configuration file contains SID_DESC entries for the existing database, you need to add these entries to the OracleAS Metadata Repository listener's configuration file.

   c. **Do not start the existing listener** (version earlier than 10.1.0.2). Now that the new listener supports both databases, you do not need to run the existing listener any more.

> **Note:** Step c above is very important. You only need to run one listener (the new listener) to support both databases.

2.6.4.1.2 Scenario 2: Existing Listener Uses Port 1521 and Listener Version Is 10.1.0.2 or Later The existing listener will support both the existing database and the OracleAS Metadata Repository. The installer will perform this configuration automatically.

The listener can be running during installation.

2.6.4.1.3 Scenario 3: Existing Listener Uses a Port Other Than 1521 You will end up running two listeners: one for the existing database and one for the OracleAS Metadata Repository, regardless of the version of the existing listener.

The existing listener can be running during installation, because it is not using port 1521.

2.6.4.2 If Port 1521 Is In Use by Some Other Application

If you have some other application listening on port 1521, you need to reconfigure it to listen on a different port. If that is not possible, shut it down while you install the OracleAS Metadata Repository. After installation, you can reconfigure the OracleAS Metadata Repository to use a port other than 1521. See the *Oracle Application Server Administrator's Guide* for instructions on how to do this.

2.7 Operating System Groups

You need to create operating system groups in these situations:

- If you plan to install Oracle Application Server on a computer that does not have Oracle products, create a group to own the "inventory" directory. See Section 2.7.1, "Create a Group for the Inventory Directory".
- If you plan to install the OracleAS Metadata Repository in a new database (that is, one created by the installer), create groups for database administrators. See Section 2.7.2, "Create Groups for Database Administrators".

To create a local operating system group, use the Solaris Management Console:

1. Set the DISPLAY environment variable to point to the monitor where you want the Solaris Management Console window to appear. See Section 2.9.4, "DISPLAY" if you need help setting the environment variable.
2. Start up the Solaris Management Console.

   ```
   prompt> /usr/sadm/bin/smc
   ```

3. In the left frame, expand **This Computer**, then expand **System Configuration**.
4. Click **Users**. This displays the Log In window.
5. In the Log In window, log in as the root user.
6. In the left frame, expand **Users** and select **Groups**.
7. Select Action > Add Group.
8. In **Group Name**, enter the name of the group.
9. (optional) In **Group ID Number**, enter an ID number for the group.
10. Click **OK**.

For more information about operating system users and groups, see your operating system documentation or contact your system administrator.

2.7.1 Create a Group for the Inventory Directory

If you plan to install Oracle Application Server on a computer that does not have Oracle products, create a group to own the inventory directory. The installer writes its files in the inventory directory to keep track of the Oracle products installed on the computer.

This guide uses the name `oinstall` for this operating system group.

By having a separate group for the inventory directory, you allow different users to install Oracle products on the computer. Users need write permission for the inventory directory. They can achieve this by belonging to the `oinstall` group.

For the first time installation of any Oracle product on a computer, the installer displays a screen where you enter a group name for the inventory directory, and a screen where you enter the location of the inventory directory.

The default name of the inventory directory is `oraInventory`.

If you are unsure if there is already an inventory directory on the computer, look in the `/var/opt/oracle/oraInst.loc` file. This file lists the location of the inventory directory and the group who owns it. If the file does not exist, the computer does not have Oracle products installed on it.

2.7.2 Create Groups for Database Administrators

This section applies only if you plan to install the OracleAS Metadata Repository in a new database created by the installer.

When the database is not mounted and database authentication is unavailable, the database uses operating system groups to determine user privileges. The database recognizes these groups and privileges:

Table 2–8 Privileges for the OSDBA and OSOPER Groups

Group	Description
OSDBA	This is the database administrator group. Users in this group are granted SYSDBA privileges.
OSOPER	Users in this group are granted SYSOPER privileges, which comprise privileges required for basic maintenance. These include database startup and shutdown, and other privileges required for database operation. SYSOPER privileges are a subset of SYSDBA privileges.

You need to create operating system groups for these groups.

If you want an operating system group called `dba` to have SYSDBA privileges:

1. Create the `dba` group.
2. Ensure that the user running the installer is a member of the `dba` group.

If you want a different operating system group to have SYSDBA privileges, or if you want to associate SYSDBA and SYSOPER privileges with different groups, ensure the user running the installer does not belong to the `dba` group.

If the user running the installer does not belong to the `dba` group, the installer displays a screen where you can enter the names of groups to have the database administrator privileges. The screen has two fields: one for the OSDBA group and one

for the OSOPER group (see Table 2–8). You can enter the same operating system group for both fields.

2.8 Operating System User

Create an operating system user to install and upgrade Oracle products. This guide refers to this user as the `oracle` user. The `oracle` user running the installer must have write permission for these directories:

- the Oracle home directory, which contains files for the product you are installing
- the inventory directory, which is used by the installer for all Oracle products

If the computer contains other Oracle products, you might already have a user for this purpose. Look in the `/var/opt/oracle/oraInst.loc` file. This file lists the location of the inventory directory and the group who owns it. If the file does not exist, the computer does not have Oracle products installed on it.

If you do not already have a user for installing Oracle products, create a user with the following properties:

Table 2–9 Properties of the Operating System User Who Runs the Installer

Item	Description
Login name	You can use any name for the user. This guide refers to the user as the `oracle` user.
Group identifier	The primary group of the `oracle` user must have write permission for the `oraInventory` directory. See Section 2.7.1, "Create a Group for the Inventory Directory" for more information about this group. You can use any name for the group. This guide uses the name `oinstall`.
Home directory	The home directory for the `oracle` user can be consistent with the home directories of other users.
Login shell	The default login shell can be the C, Bourne, or Korn shell.

Note: Use the `oracle` user only for installing and running Oracle products. Do not use root as the `oracle` user.

To create a local operating system user, use the Solaris Management Console:

1. Set the DISPLAY environment variable to point to the monitor where you want the Solaris Management Console window to appear. See Section 2.9.4, "DISPLAY" if you need help setting the environment variable.
2. Start up the Solaris Management Console.

   ```
   prompt> /usr/sadm/bin/smc
   ```

3. In the left frame, expand **This Computer**, then expand **System Configuration**.
4. Click **Users**. This displays the Log In window.
5. In the Log In window, in **User Name**, enter `root`. In **Password**, enter the root password.
6. In the left frame, expand **Users** and select **User Accounts**.
7. Select Action > Add User > With Wizard.

8. In **User Name**, enter the name of the user (`oracle`). The **Full Name** and **Description** fields are optional. Click **Next**.
9. In **User ID Number**, accept the default value. Click **Next**.
10. Select **User Must Use This Password At First Login**, and enter a password for the user. Click **Next**.
11. In **Primary Group**, select the primary group for the user. This is the group you created earlier to own the inventory directory. See Section 2.7.1, "Create a Group for the Inventory Directory". Click **Next**.
12. In **Path**, enter a home directory for the user. Click **Next**.
13. Review the mail server information for the user and click **Next**.
14. Review the user information and click **Finish** to create the user.

To check which groups an operating system user belongs to, run the `groups` command with the name of the user. For example:

```
prompt> groups oracle
```

For more information about operating system users and groups, see your operating system documentation or contact your system administrator.

2.9 Environment Variables

The operating system user who will be installing Oracle Application Server needs to set (or unset) the following environment variables.

Table 2–10 summarizes whether you set or unset an environment variable.

Table 2–10 Environment Variable Summary

Environment variable	Set or Unset
ORACLE_HOME and ORACLE_SID	Must not be set.
PATH, CLASSPATH, and LD_LIBRARY_PATH	Must not contain references to directories in any Oracle home directories
DISPLAY	Set it to the monitor where you want to the installer window to appear.
TMP	Optional. If unset, defaults to `/tmp`.
TNS_ADMIN	Must not be set.

2.9.1 Environment Variable Tips

Here are some tips when working with environment variables:

- If you set environment variables in the `.profile` file, they might not be read. To ensure environment variables are set to the correct values, check their values in the shell where you will be running the installer.
- To check the value of environment variables, use the `env` command. This displays all the currently defined environment variables and their values.

  ```
  % env
  ```

- If you use the `su` command to switch users (for example, switching from the root user to the `oracle` user), check the environment variables when you are the new

user because the environment variables might not be passed to the new user. This can happen even if you run `su` with the - parameter (`su - user`).

```
# /* root user */
# su - oracle
% env
```

2.9.2 ORACLE_HOME and ORACLE_SID

These environment variables must not be set.

2.9.3 PATH, CLASSPATH, and LD_LIBRARY_PATH

Edit your PATH, CLASSPATH, and LD_LIBRARY_PATH environment variables so that they do not reference any Oracle home directories.

2.9.4 DISPLAY

Set the DISPLAY environment variable to point to the X server that will display the installer. The format of the DISPLAY environment variable is:

```
hostname:display_number.screen_number
```

Example (C shell):

```
% setenv DISPLAY test.mydomain.com:0.0
```

Example (Bourne or Korn shell):

```
$ DISPLAY=test.mydomain.com:0.0; export DISPLAY
```

You can test the display by running the xclock program:

```
$ /usr/openwin/bin/xclock &
```

Oracle Application Server requires a running X server during installation only. The frame buffer X server installed with your operating system requires that you remain logged in and have the frame buffer running during installation. If you do not wish to do this, then you must use a virtual frame buffer, such as X Virtual Frame Buffer (XVFB) or Virtual Network Computing (VNC).

Visit Oracle Technology Network (`http://www.oracle.com/technology`) for information about obtaining and installing XVFB or other virtual frame buffer solutions. Search OTN for "frame buffer".

2.9.5 TNS_ADMIN

This section describes two requirements:

- The TNS_ADMIN environment variable must not be set. If set, it can cause errors during installation. Section F.3.14, "Database Configuration Assistant (DBCA) Failures" shows such an error.
- The `/etc` and the `/var/opt/oracle` directories must not contain a `tnsnames.ora` file.

These requirements are necessary to prevent conflicts between the Net configuration files for different Oracle products.

If you need to set TNS_ADMIN or if you have the `tnsnames.ora` file in `/etc` or `/var/opt/oracle`, do the following steps before installing Oracle Application Server.

1. If you have the `tnsnames.ora` file in `/etc` or `/var/opt/oracle`, move the file from these directories to a different directory. Alternatively, you can rename the file.
2. Make sure the TNS_ADMIN environment variable is not set.

   Example (C shell):

   ```
   % unsetenv TNS_ADMIN
   ```

   Example (Bourne or Korn shell):

   ```
   $ unset TNS_ADMIN
   ```

After installation, you can merge the contents of the newly created `tnsnames.ora` file with your existing `tnsnames.ora` file.

2.9.6 TMP

During installation, the installer needs to write temporary files to a "temporary" directory. By default, the "temporary" directory is `/tmp`

If you want the installer to use a directory other than `/tmp`, set the TMP environment variable to the full path of an alternate directory. This directory must meet the requirements listed in Table 2–2.

Example (C shell):

```
% setenv TMP /tmp2
```

Example (Bourne or Korn shell):

```
$ TMP=/tmp2; export TMP
```

If you do not set this environment variable, and the default directory does not have enough space, then the installer displays an error message that says the environment variable is not set. You can either set the environment variable to point to a different directory or free up enough space in the default directory. In either case, you have to restart the installation.

2.10 The /etc/hosts File

Although the contents of the `/etc/hosts` file affect these items:

- Section 2.10.1, "Location of the Default Oracle Identity Management Realm"
- Section 2.10.2, "Hostname for OracleAS Single Sign-On"

the installer provides alternative methods for you to enter the values that you want without editing the `hosts` file. See the following subsections for details.

2.10.1 Location of the Default Oracle Identity Management Realm

The installer reads the `hosts` file to construct the location of the default Oracle Identity Management realm. It displays this location in the "Specify Namespace in Internet Directory" screen.

The `hosts` file should use the following format:

```
ip_address   fully_qualified_hostname   short_hostname
```

Example:

```
123.45.67.89   primaryHost.mydomain.com   primaryHost
```

In the preceding example, the location of the default Oracle Identity Management realm would look like "`dc=mydomain,dc=com`".

If the file uses a different format, the installer displays an incorrect value in the screen. For example, if the `hosts` file contains:

```
123.45.67.89   primaryHost   primaryHost.mydomain.com  <--- incorrect format
```

the installer would display "`dc=primaryHost,dc=com`" as the default Oracle Identity Management realm. This is probably not the value that you want for the default Oracle Identity Management realm.

> **Tip:** If you need the `hosts` file to use a different format, you can edit the file to use the required format, perform the installation, then revert the file back to its original format after installation.
>
> If you are unable, or unwilling, to edit the `hosts` file, you can enter the desired value for the default Oracle Identity Management realm in the Custom Namespace field on the "Specify Namespace in Internet Directory" screen.

2.10.2 Hostname for OracleAS Single Sign-On

If you are installing OracleAS Single Sign-On, and your `hosts` file contains only the hostname of your computer, without the domain name, then you will only be able to sign on to the Single Sign-On server using the hostname by itself (without the domain name).

If you want to require a domain name when connecting to the Single Sign-On server, you can edit the `hosts` file to include the domain name. If you do not want to edit the file, you can use the `OUI_HOSTNAME` command-line parameter to the installer to override the value in `hosts`. For example:

```
prompt> mount_point/1014disk1/runInstaller OUI_HOSTNAME=myserver.mydomain.com
```

2.11 Network Topics

Typically, the computer on which you want to install Oracle Application Server is connected to the network, has local storage to contain the Oracle Application Server installation, has a display monitor, and has a CD-ROM or DVD-ROM drive.

This section describes how to install Oracle Application Server on computers that do not meet the typical scenario. It covers the following cases:

- Section 2.11.1, "Installing on Multihomed (Multi-IP) Computers"
- Section 2.11.2, "Copying CD-ROMs or DVD-ROM to Hard Drive, and Installing from the Hard Drive"
- Section 2.11.3, "Installing from a Remote CD-ROM or DVD-ROM Drive"
- Section 2.11.4, "Installing on Remote Computers"
- Section 2.11.5, "Installing on NFS-Mounted Storage"

- Section 2.11.6, "Running Multiple Instances from One Installation"
- Section 2.11.7, "Support for NIS and NIS+"

2.11.1 Installing on Multihomed (Multi-IP) Computers

You can install Oracle Application Server on a multihomed computer. A multihomed computer is associated with multiple IP addresses. This is typically achieved by having multiple network cards on the computer. Each IP address is associated with a hostname; additionally, you can set up aliases for the hostname. By default, Oracle Universal Installer uses the `OUI_HOSTNAME` environment variable setting to find the hostname. If `OUI_HOSTNAME` is not set and you are installing on a computer that has multiple network cards, Oracle Universal Installer determines the hostname by using the first name in the `/etc/hosts` file.

Clients must be able to access the computer using this hostname (or using aliases for this hostname). To check, ping the hostname from the client computers using the short name (hostname only) and the full name (hostname and domain name). Both must work.

2.11.2 Copying CD-ROMs or DVD-ROM to Hard Drive, and Installing from the Hard Drive

Instead of installing from the Oracle Application Server CD-ROMs or DVD-ROM, you can copy the contents of the CD-ROMs or DVD-ROM to a hard drive and install from there. This might be easier if you plan to install many instances of Oracle Application Server on your network, or if the computers where you want to install Oracle Application Server do not have CD-ROM or DVD-ROM drives.

(You can install from remote CD-ROM or DVD-ROM drives; see Section 2.11.3, "Installing from a Remote CD-ROM or DVD-ROM Drive".)

When you install from the hard drive, the installer does not prompt you to swap CD-ROMs. It can find all the files if they are in the proper locations (see Figure 2–1).

Space Requirement

Ensure that the hard drive contains enough space to hold the contents of the CD-ROMs or the `application_server` directory on the DVD-ROM. Each CD-ROM contains approximately 650 MB. This means that if you are copying three CD-ROMs, you need approximately 1.9 GB of disk space.

On the DVD-ROM, the `application_server` directory is approximately 1.6 GB.

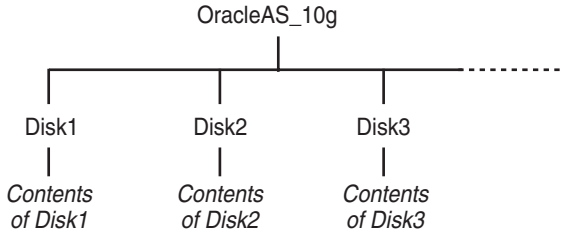
This space is in addition to the space required for installing Oracle Application Server (listed in Table 2–2).

To Copy the CD-ROMs:

1. Create a directory structure on your hard drive as shown in Figure 2–1.

   You need to create a parent directory (called `OracleAS_10g` in the example, but you can name it anything you like), and, under the parent directory, create subdirectories called `Disk1`, `Disk2`, and so on. The names of the subdirectories must be `Disk`*N*, where *N* is the CD-ROM number.

Figure 2–1 Directory Structure for Copying CD-ROMs to Disk



2. Copy the contents of each CD-ROM into the corresponding directory.

```
prompt> cp -pr /cdrom_mount_point/10.1.4disk1/* /path/to/hard/drive/Disk1/
prompt> cp -pr /cdrom_mount_point/10.1.4disk2/* /path/to/hard/drive/Disk2/
... Repeat for each CD-ROM.
```

To run the installer from the copied files, invoke the `runInstaller` executable from the `Disk1` directory. Run it from the computer that will be running Oracle Application Server.

```
prompt> /path/to/hard/drive/Disk1/runInstaller
```

To Copy the application_server Directory from the DVD-ROM

1. (optional) Create a directory to contain the `application_server` directory.
2. Copy the `application_server` directory from the DVD-ROM to your hard disk.

```
prompt> cp -pr /dvd_mount_point/application_server /path/to/hard/drive
```

To run the installer from the copied files, invoke the `runInstaller` executable from the computer that will be running Oracle Application Server:

```
prompt> /path/to/hard/drive/application_server/runInstaller
```

2.11.3 Installing from a Remote CD-ROM or DVD-ROM Drive

If the computer where you want to install Oracle Application Server does not have a CD-ROM or DVD-ROM drive, you can perform the installation from a remote CD-ROM or DVD-ROM drive. Check that you have performed these steps:

- You need to share the remote CD-ROM or DVD-ROM drive through NFS.

  On the remote computer, which has the CD-ROM or DVD-ROM drive:

  1. CD-ROM: Insert Oracle Application Server Disk 1 into the CD-ROM drive.

     DVD-ROM: Insert the Oracle Application Server DVD-ROM into the DVD-ROM drive.

  2. Share the CD-ROM or DVD-ROM drive.

     CD-ROM:

     ```
     prompt> su
     Password: root_password
     # share -F nfs -o ro /cdrom/1012disk1
     ```

     The path `/cdrom/10.1.4disk1` specifies the path to the CD-ROM in the CD-ROM drive. You can use any path you like.

DVD-ROM:

```
prompt> su
Password: root_password
# share -F nfs -o ro /cdrom
```

The path `/cdrom` specifies the path to the DVD-ROM in the DVD-ROM drive. You can use any path you like.

On the local computer, access the CD-ROM or DVD-ROM and run the installer as follows:

CD-ROM:

```
prompt> /net/remote_computer_hostname/cdrom/10.1.4disk1/runInstaller
```

DVD-ROM:

```
prompt> /net/remote_computer_hostname/cdrom/application_server/runInstaller
```

Replace *remote_computer_hostname* with the name of the remote computer.

- This bullet point, switching CD-ROMs, does not apply to DVDs.

  When the installer prompts you to switch CD-ROMs, you need to unshare the CD-ROM drive, eject the CD-ROM, insert the requested CD-ROM, and share the CD-ROM drive again. If you do not unshare, you will not be able to eject the CD-ROM.

  > **Note:** The installer must be running when you are switching CD-ROMs. Do **not** exit the installer when switching CD-ROMs. If you exit the installer, it is unable to continue from where it left off. In addition, the partial installation that it created is not usable, and may need to be removed manually.

  On the remote computer (which has the CD-ROM drive):

```
prompt> su
Password: root_password
# unshare /cdrom/10.1.4disk1
# eject cdrom
... Remove the CD-ROM, and insert the CD-ROM requested by the installer (for
... example, Disk 2).
... Share the CD-ROM.
# share -F nfs -o ro /cdrom/10.1.4disk2
```

2.11.4 Installing on Remote Computers

You can run the installer on a remote computer ("remote_computer"), but have the installer screens display on your local computer ("local_computer"). The installer will install Oracle Application Server on the remote computer.

1. Allow remote_computer to display on local_computer. You need to run this command on the local computer's console.

   ```
   local_computer> xhost +remote_computer
   ```

   If you do not run `xhost`, you might get an Xlib error similar to "Failed to connect to server", "Connection refused by server," or "Can't open display" when starting the installer.

2. On local_computer, perform a remote login (using `telnet` or `rlogin`) to remote_computer. Log in as the `oracle` user, as described in Section 2.8, "Operating System User". Ensure that the user has set the environment variables correctly, as described in Section 2.9, "Environment Variables".

```
local_computer> rlogin -l oracle remote_computer.mydomain.com
- OR -
local_computer> telnet remote_computer.mydomain.com
```

3. Set the DISPLAY environment variable on remote_computer to point to local_computer.

   Example (C shell):

```
remote_computer> setenv DISPLAY local_computer.mydomain.com:0.0
```

   Example (Bourne or Korn shell):

```
remote_computer> DISPLAY=local_computer.mydomain.com:0.0; export DISPLAY
```

4. Run the installer. See Section 3.15, "Starting the Oracle Universal Installer".

> **Note:** You can use a PC X emulator to run the installer if it supports a PseudoColor color model or PseudoColor visual. Set the PC X emulator to use a PseudoColor visual, and then start the installer. Refer to the X emulator documentation for instructions on how to change the color model or visual settings.

2.11.5 Installing on NFS-Mounted Storage

To run Oracle Application Server on NFS systems, you have to use a certified NFS-mounted storage system.

Currently Oracle Application Server is certified to run on these NFS systems:

- Network Appliance (NetApp) filers

The NetApp system should be exported to at least the remote install user and remote root user. You can do this using `exportfs` command:

```
prompt> exportfs -i /vol/vol1
```

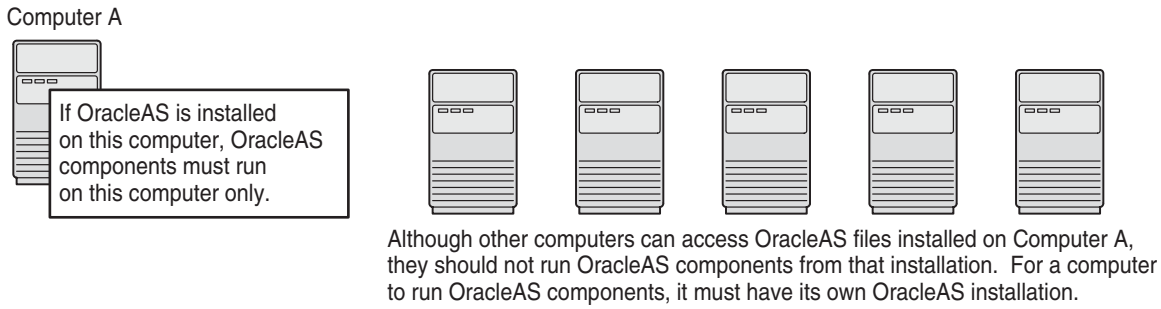
Before installing, verify that the NFS mount setuid permission is set to `suid`. The `nosuid` option will cause the install to fail.

To check the latest certification list for any updates, visit Oracle Technology Network (`http://www.oracle.com/technology`).

2.11.6 Running Multiple Instances from One Installation

Oracle Application Server components are intended to be run only on the computer where they are installed. You cannot run the components on remote computers, even though the computers can access the files through NFS.

Figure 2–2 Run Oracle Application Server Only on the Computer Where It Is Installed



2.11.7 Support for NIS and NIS+

You can install and run Oracle Application Server in NIS and NIS+ environments.

2.12 Font Packages for Java

You may need different character settings for different locales. For Solaris Font Packages for Java, you always need both `SUNWi1of` and `SUNWxwfnt` font packages for all locales. You may need additional font packages depending on your locale. For a list of Solaris Font Packages, see:

`http://java.sun.com/j2se/1.4.1/font-requirements.html`

2.13 Prerequisite Checks Performed by the Installer

Table 2–11 lists the checks performed by the installer:

Table 2–11 Prerequisite Checks Performed by the Installer

Item	Description
Operating system version	See Table 2–2 for supported versions.
Operating system patches	See Section 2.3, "Operating System Patches" for a list of required patches.
Operating system packages	See Section 2.4, "Operating System Packages" for a list of required packages.
Operating system kernel parameters	See Section 2.5, "Kernel Parameters" for a list of required kernel parameters.
Memory	See Table 2–2 for recommended values.
Swap space	See Table 2–2 for recommended values.
TMP space	See Table 2–2 for recommended values.
Instance name	The installer checks that the computer on which you are installing Oracle Application Server does not already have an instance of the same name.
Oracle home directory name	The installer checks that the Oracle home directory name does not contain any spaces.
Path to Oracle home directory	The installer checks that the path to the Oracle home directory is not longer than 127 characters.
Oracle home directory contents	The installer checks that the Oracle home directory does not contain any files that might interfere with the installation.

Table 2–11 (Cont.) Prerequisite Checks Performed by the Installer

Item	Description
Oracle home directory	You should install Oracle Application Server in a new directory. Here are some examples of installations that are **not allowed**: ▪ Any type of Oracle Application Server into an 8.0, 8*i*, 9.0.1, or 9.2 database Oracle home ▪ Any type of Oracle Application Server into an Oracle Management Service Oracle home ▪ Any type of Oracle Application Server into an Oracle Collaboration Suite Oracle home ▪ Any type of Oracle Application Server into an Oracle HTTP Server standalone Oracle home ▪ Any type of Oracle Application Server into an OracleAS Web Cache standalone Oracle home ▪ Any type of Oracle Application Server into an Oracle9*i* Developer Suite 9.0.2 Oracle home ▪ Any type of Oracle Application Server into an Oracle Containers for J2EE standalone Oracle home ▪ Any type of Oracle Application Server into an Oracle9*i*AS 1.0.2.2 Oracle home ▪ Oracle Application Server middle tier into an infrastructure 9.0.2, 9.0.4, or 10*g*Release 2 (10.1.2) Oracle home ▪ OracleAS Infrastructure middle tier into any Oracle9*i*AS 9.0.2, 9.0.3, or 9.0.4 middle tier Oracle home ▪ OracleAS Developer Kits into an infrastructure 9.0.2, 9.0.4, or 10*g* Release 2(10.1.2) Oracle home ▪ OracleAS Developer Kits into an Oracle9*i*AS middle tier 9.0.2, 9.0.3, 9.0.4, or 10.1.2 Oracle home ▪ OracleAS Developer Kits into an Oracle Developer Suite 9.0.2, 9.0.4, or 10g Release 2 (10.1.2) Oracle home ▪ OracleAS Infrastructure into any Oracle9iAS 9.0.2, 9.0.3, or 9.0.4 Oracle home ▪ OracleAS Infrastructure into an Oracle Application Server 10g Release 2(10.1.2) middle tier or OracleAS Developer Kits Oracle home ▪ OracleAS Infrastructure into an Oracle Developer Suite 9.0.2, 9.0.4, or 10g Release 2 (10.1.2) Oracle home ▪ OracleAS Infrastructure or middle tier into an Oracle home installed from the Business Intelligence CD-ROM
Port 1521	The installer displays a warning if port 1521 is in use by any application, including database listeners of any version. You need to stop the application that is using port 1521, then click **OK** in the warning dialog. If it is a database listener that is using port 1521, you might be able to use it for the metadata repository database. See Section 2.6.4, "If Port 1521 Is in Use" for details. If it is another application that is using port 1521, you need to stop it or configure it to use a different port. Alternatively, you can change the database listener to use a port other than 1521, but you can do this only after installation. See the *Oracle Application Server Administrator's Guide* for details.
Static port conflicts	The installer checks the ports listed in the `staticports.ini` file, if specified. See Section 2.6, "Ports".
Monitor	The installer checks that the monitor is configured to display at least 256 colors.
Display permission	The installer checks that the user has permissions to display on the monitor specified by the DISPLAY environment variable.
DISPLAY environment variable	The installer checks that the DISPLAY environment variable is set.

Table 2–11 (Cont.) Prerequisite Checks Performed by the Installer

Item	Description
TNS_ADMIN environment variable	The TNS_ADMIN environment variable must not be set. There must not be a `tnsnames.ora` file in the `/etc` or `/var/opt/oracle` directories.
DBCA_RAW_CONFIG environment variable	If you are installing the OracleAS Infrastructure in a Real Application Clusters environment, you need to set this environment variable to point to a file that describes the locations of your raw partitions.
Cluster file system	The installer checks that you are not installing Oracle Application Server in a cluster file system (CFS).
Oracle Enterprise Manager directories are writable	The installer runs this check only if you are expanding a middle tier or if you are reinstalling Oracle Application Server in the same Oracle home. The installer checks that these directories are writable by the operating system user running the installer: ■ `ORACLE_HOME/sysman/emd` ■ `ORACLE_HOME/sysman/config` ■ `ORACLE_HOME/sysman/webapps/emd/WEB-INF/config`
Oracle Enterprise Manager files exist	The installer runs this check only if you are expanding a middle tier or if you are reinstalling Oracle Application Server in the same Oracle home. The installer checks that these files exist: ■ `ORACLE_HOME/sysman/config/iasadmin.properties` ■ `ORACLE_HOME/sysman/webapps/emd/WEB-INF/config/consoleConfig.xml`

3

Things You Should Know Before Starting the Installation

This chapter contains the following topics:

- Section 3.1, "Oracle Home Directory"
- Section 3.2, "Can I Use Symbolic Links?"
- Section 3.3, "First-Time Installation of Any Oracle Product"
- Section 3.4, "Installing Additional Languages"
- Section 3.5, "Oracle Application Server Instances and Instance Names"
- Section 3.6, "The ias_admin User and Restrictions on its Password"
- Section 3.7, "Comparing Installing Components against Configuring Components"
- Section 3.8, "Where Does the Installer Write Files?"
- Section 3.9, "Why Do I Need to be Able to Log In as Root at Certain Times During Installation?"
- Section 3.10, "Running root.sh During Installation"
- Section 3.11, "Can I Modify Other Oracle Application Server Instances During Installation?"
- Section 3.12, "Connecting to Oracle Internet Directory Through SSL Connections"
- Section 3.13, "Obtaining Software from Oracle E-Delivery"
- Section 3.14, "Setting the Mount Point for the CD-ROM or DVD-ROM"
- Section 3.15, "Starting the Oracle Universal Installer"

3.1 Oracle Home Directory

The directory in which you install Oracle Application Server is called the Oracle home. During installation, you specify the full path to this directory and a name for this Oracle home.

For example, you can install OracleAS Infrastructure in `/opt/oracle/OraHome_Infra`, and you can name it "Infra".

Names of Oracle homes must be 128 characters or fewer, and can contain only alphanumeric characters and underscores.

Notes: Spaces are not allowed anywhere in the Oracle home directory path. For example, you cannot install in "`/opt/oracle/app server/Infra`" because of the space character in "`app server`". The installer does not check for this until several screens after you have entered the path.

If you plan to install a middle tier and an infrastructure on the same computer, you must install them in different Oracle home directories. The installer does not allow you to install a middle tier and an infrastructure in the same Oracle home.

Tip: If you install multiple Oracle Application Server instances (for example, an OracleAS Infrastructure and a middle tier) on the same computer, create scripts for setting the environment for each instance. This is to ensure that you run the binaries from the proper Oracle home. Environment variables that you need to set include ORACLE_HOME and PATH.

3.1.1 Installing in an Existing Oracle Home

Generally, you cannot install Oracle Application Server in an existing Oracle home. See "Oracle home directory" on page 2-31 for a list of combinations that are not allowed.

3.1.2 Installing in a Non-Empty Oracle Home

You cannot install Oracle Application Server in a directory that already contains some files, except for the cases mentioned in Section 3.1.1, "Installing in an Existing Oracle Home". For example, if you cancel an installation, or if an installation failed, you have to clean up the directory before you can reinstall Oracle Application Server in it. Also, the installer cannot "repair" an installation. See Section F.3.4, "Message About Installing in a Non-Empty Directory" for instructions on how to clean up the directory.

3.2 Can I Use Symbolic Links?

You can create symbolic links before installing Oracle Application Server and use them during installation. For example, if you run the following commands:

```
prompt> mkdir /home/basedir
prompt> ln -s /home/basedir /home/linkdir
```

then, when you run the installer, you can specify `/home/linkdir` as the Oracle Home.

After installation, you cannot create symbolic links to the Oracle Home. You also may not move the Oracle Home to a different location and create a symbolic link to the original Oracle Home.

3.3 First-Time Installation of Any Oracle Product

If Oracle Application Server is the first Oracle product to be installed on a computer, the installer displays a screen where you specify an "inventory" directory (also called the "oraInventory" directory). This inventory directory is used by the installer to keep track of all Oracle products installed on the computer.

The inventory directory is separate from the Oracle home directory for Oracle Application Server.

To ensure other users in the `oinstall` group have access to the inventory directory (so that they can install Oracle products), do not use the `oracle` user's home directory as the inventory directory because home directories might not have the proper permissions set up for the `oinstall` group. Instead, you can put the inventory directory in the `/opt/oracle` directory (for example, `/opt/oracle/oraInventory`).

If you have installed an Oracle product previously on the computer, the installer uses the existing inventory directory. Ensure that you have write permissions on that directory. The best way of ensuring this is to run the installer as the same operating system user who installed the existing Oracle products.

Oracle recommends creating an operating system user to perform all tasks related to installation of Oracle products. See Section 2.8, "Operating System User".

3.4 Installing Additional Languages

By default, the installer installs Oracle Application Server with text in English and in the operating system language. If you need additional languages, click the **Product Languages** button in the "Select a Product to Install" screen.

When you select additional languages to install, the installer installs text in the selected languages. It also installs fonts required to display the languages.

For some components, languages are installed only if you select them during installation. In this case, if you access the application in a language that is not available, it will fall back on the server locale language.

For other components, available languages are installed regardless of what you select during installation. In this case, however, fonts are installed only for the languages that are explicitly selected. When you access the application, it uses text in your language because the language was installed. However, if you do not have the appropriate fonts to render the text, the text appears as square boxes. This usually applies to the Chinese, Japanese, and Korean languages.

You can install fonts after installation. See Section F.3.10, "User Interface Does Not Display in the Desired Language, or Does Not Display Properly".

Note that you cannot install additional languages after installation. You must install all languages that you need during installation. If you run Oracle Application Server in an environment that uses a language that you did not install, the user interface can display text in that language and/or in English, or it can display square boxes (caused by missing fonts) instead of text.

3.5 Oracle Application Server Instances and Instance Names

When you install the infrastructure, what you get is an Oracle Application Server instance. The installer prompts you to provide a name for the Oracle Application Server instance you are installing. For example, you can name an instance "infra". This name can be different from the Oracle home name.

You cannot change this name after installation.

Oracle Application Server appends the hostname and domain name to the given instance name to form a complete instance name. For example, if you are installing an instance on a computer named `c1`, and you name the instance `infra1`, then the full name of the instance is `infra1.c1.mydomain.com`, assuming the domain name is `mydomain.com`.

Valid Characters in Instance Names

Instance names can consist only of the alphanumeric characters (`A-Z`, `a-z`, `0-9`) and the _ (underscore) character.

The maximum length for an instance name is 64 characters.

Restrictions on Oracle Application Server Instance Names

Do not use the hostname of the computer when naming Oracle Application Server instances.

If you are planning to place the Oracle Application Server instance in an OracleAS Cluster, the instance name must not contain the following:

- hostname or IP address of any computer in the OracleAS Cluster
- Oracle home of any Oracle Application Server installation in the OracleAS Cluster

How Oracle Application Server Uses Instance Names

Instance names are important because Oracle Application Server uses them to uniquely identify instances. This means that if you install multiple Oracle Application Server instances on the same computer (for example, an OracleAS Infrastructure and a J2EE and Web Cache instance), you must give them different names.

When you administer Oracle Application Server using Oracle Enterprise Manager 10*g* Application Server Control (or Application Server Control for short), the instance name appears on the screens. You can click the instance name to see details about the instance, such as the components that are installed in that instance, if the components are running or stopped, and the log files for the components. The Application Server Control is a browser-based administration tool for Oracle Application Server. See the *Oracle Application Server Administrator's Guide* for details about this administration tool.

In addition, some `dcmctl` commands require an instance name as a parameter. `dcmctl` is a command-line tool for administering Oracle Application Server instances. See the *Distributed Configuration Management Administrator's Guide* for details about `dcmctl`.

3.6 The ias_admin User and Restrictions on its Password

The installer prompts you to specify the password for the `ias_admin` user. The `ias_admin` user is the administrative user for Oracle Application Server instances. To manage Oracle Application Server instances using Application Server Control, you log in as `ias_admin`.

On a computer, you can install multiple Oracle Application Server instances, each with its own unique instance name, but the name of the administrative user is `ias_admin` for all instances. The password for the `ias_admin` user can be different for each instance.

Password for the ias_admin User

The password for the `ias_admin` user must conform to Oracle Internet Directory's password policy:

- If you are using the Oracle Internet Directory that is shipped with this release of Oracle Application Server and you did not change the default password policy, passwords have the following restrictions:
  - The minimum length is five alphanumeric characters.
  - At least one of the characters must be a number.

- If you are using any other version of Oracle Internet Directory (for example, you are using an existing Oracle Internet Directory), your Oracle Internet Directory administrator might have defined a different password policy. The password you enter for the `ias_admin` user must conform to the existing Oracle Internet Directory's password policy.

In addition to the password policy defined in Oracle Internet Directory, the password for the `ias_admin` user has these restrictions:

- Passwords must be shorter than 30 characters.
- Passwords can contain only alphanumeric characters from your database character set, the underscore (_), the dollar sign ($), and the number sign (#).
- Passwords must begin with an alphabetic character. Passwords cannot begin with a number, the underscore (_), the dollar sign ($), or the number sign (#).
- Passwords cannot be Oracle reserved words. The *Oracle Database SQL Reference* lists the reserved words. You can find this guide on Oracle Technology Network (`http://www.oracle.com/technology/documentation`). Or you can just avoid using words that sound like they might be reserved words.

> **Note:** When entering your password, check that the state of the Caps Lock key is what you want it to be. Passwords are case-sensitive.

You must remember the password because you need to enter it to perform the following tasks:

- When you log on to Application Server Control to manage Oracle Application Server, you log on as the `ias_admin` user.
- For middle-tier installations: if you want to install a larger middle tier in an ORACLE_HOME that already contains a middle tier (for example, you want to install the Portal and Wireless type over an existing J2EE and Web Cache type), you must enter the existing password during the installation.

If you forget the password, you can reset it. See the *Oracle Application Server Administrator's Guide* for details.

3.7 Comparing Installing Components against Configuring Components

When you select components on the Select Configuration Options screen, the installer installs and configures the selected components. For the unselected components, the installer still installs them, but does not configure them.

In most cases, you can configure components that you did not select on the Select Configuration Options screen after installation using the Application Server Control. See the *Oracle Application Server Administrator's Guide* for details.

3.8 Where Does the Installer Write Files?

The installer writes files to the following directories:

Table 3–1 Directories Where the Installer Writes Files

Directory	Description
Oracle home directory	This directory contains Oracle Application Server files. You specify this directory when you install Oracle Application Server.

Table 3–1 (Cont.) Directories Where the Installer Writes Files

Directory	Description
Inventory directory	When you install the first Oracle product on a computer, you specify this directory, which the installer uses to keep track of which Oracle products are installed on the computer. In subsequent installations, the installer uses the same inventory directory.
`/var/opt/oracle` directory	This directory contains information on locations of Oracle homes on the computer. If you installed Oracle9*i*AS Release 2 (9.0.2) on your computer, this directory also contains files that provide information for Oracle Enterprise Manager 10*g*.
`/tmp` directory	The installer writes files needed only during installation to a "temporary" directory. By default, the "temporary" directory is `/tmp`. To specify a different directory, set the TMP environment variable. See Section 2.9.6, "TMP" for details.

3.9 Why Do I Need to be Able to Log In as Root at Certain Times During Installation?

At least once during installation, the installer prompts you to log in as the root user and run a script. You need to be root because the script edits files in the `/var/opt/oracle` directory.

3.10 Running root.sh During Installation

The installer prompts you to run the `root.sh` script in a separate window. This script creates files in the local bin directory (`/usr/local/bin`, by default).

If the script finds files of the same name, it prompts you if you want to override the existing files. You should back up these files (you can do this from another window), then overwrite them.

The following lines show the prompts from the `root.sh` script. The default values are enclosed in square brackets.

```
Enter the full pathname of the local bin directory: [/usr/local/bin]:
The file "dbhome" already exists in /usr/local/bin.  Overwrite it? (y/n)[n]:  y
 Copying dbhome to /usr/local/bin ...
The file "oraenv" already exists in /usr/local/bin.  Overwrite it? (y/n)[n]:  y
 Copying oraenv to /usr/local/bin ...
The file "coraenv" already exists in /usr/local/bin.  Overwrite it? (y/n)[n]: y
 Copying coraenv to /usr/local/bin ...
```

After you run `root.sh`, you may see warnings that begin with "chmod: WARNING: Corresponding set-ID also disabled..." You may ignore these warnings.

3.11 Can I Modify Other Oracle Application Server Instances During Installation?

During the installation of an Oracle Application Server instance, you should not change the configuration or passwords of other installations in your environment. For example, if there is an OracleAS Infrastructure installation in your environment, you should not modify it during the installation of a middle tier.

3.12 Connecting to Oracle Internet Directory Through SSL Connections

When you install OracleAS Infrastructure or middle tiers, you can specify that Oracle Application Server components connect to Oracle Internet Directory only through SSL connections. On screens where you specify the hostname and port for Oracle Internet Directory, you can select the **Use Only SSL Connections With This Oracle Internet Directory** option.

Note that Oracle HTTP Server is not set up for SSL connections during installation. If you need Oracle HTTP Server to use SSL, you can set it up after installation. See the *Oracle HTTP Server Administrator's Guide* for details.

3.13 Obtaining Software from Oracle E-Delivery

You can obtain Oracle products from Oracle E-Delivery at `http://edelivery.oracle.com/`. Oracle products are distributed as "E-Packs". An E-Pack is an electronic version of the software that is also available to Oracle Customers on CD-ROM or DVD-ROM.

3.13.1 Finding and Downloading the Oracle Application Server 10*g* (10.1.4.0.1) E-Pack

Refer to the CD/Media Pack description or the list of products that you purchased on your Oracle Ordering Document. Then, view the License List to help you decide which Product Pack you need to select in order to search for the appropriate E-Pack(s) to download. Prior to downloading, verify that the product you are looking for is in the License and Options section of the E-Pack README. Oracle recommends that you print the README for reference.

3.13.2 Finding Required and Optional Downloads

Refer to the README link that is on each E-Pack Download page. In addition to listing the licensable products and options contained in the pack, the README lists downloadable files that are required to run each product and which downloadable files are optional. Oracle recommends that you print the README for reference.

3.13.3 Disk Space Requirements

In addition to having the required disk space necessary to install and run your Oracle software, you'll need to have sufficient disk space to download all the required software files and have enough disk space to extract them.

After extracting the software from the Zip files, you can burn them onto CD-ROM and install from them, or install from your computer's hard drive.

3.13.4 Software Requirements for Unzipping Files

All Oracle E-Delivery files have been archived using Info-ZIP's highly portable Zip utility. After downloading one or more of the archives, you will need the UnZip utility to extract the files.You must unzip the archive on the platform for which it was intended. For example, if you download the file for the Solaris Operating System (SPARC) version of Oracle Application Server, you must unzip the file on a Solaris Operating System (SPARC) computer. If you unzip the file on a Windows computer, and then move the stage area to a Solaris Operating System (SPARC) machine, the stage area files will be corrupted because Windows will not preserve the case sensitivity or the permission bits of UNIX file names.

3.13.5 Extracting Software from the Zip Files

Verify that the file size of your downloaded file matches the file size displayed on E-Delivery. Unzip each Zip file to its own temporary directory. For example, create a directory structure called oraAS10g on your hard drive:

```
c:\oraAS10g
```

Then create a new directory for each Zip file you downloaded:

```
c:\oraAS10g\Disk1
c:\oraAS10g\Disk2
```

etc.

If you plan burn the files on a CD-ROM, create a separate CD-ROM from the contents of each directory. Do not burn a CD-ROM containing the Zip file itself; you need the unzipped contents of the Zip files to do the installation. When you burn the files to CD-ROM, the contents of each disc must be at the root of the CD image.

To install from CD-ROM or from your hard drive, see Section 3.15, "Starting the Oracle Universal Installer".

3.14 Setting the Mount Point for the CD-ROM or DVD-ROM

The Oracle Application Server CD-ROMs are in RockRidge format. The DVD-ROM is in DVD-ROM format.

If you are using the Solaris Volume Management software (installed by default with Solaris Operating Environment), then the CD-ROM or DVD-ROM is mounted automatically at `/cdrom` when you insert the CD-ROM or DVD-ROM. For example, when you insert Oracle Application Server Disk 1 into the CD-ROM drive, you can access its contents at `/cdrom/10.1.4disk1`.

If you are not using the Solaris Volume Management software, then you must mount the CD-ROM or DVD-ROM manually. To manually mount or unmount the CD-ROM or DVD-ROM, you must have root privileges. Be sure to unmount the CD-ROM or DVD-ROM before removing it from the drive.

Follow these steps to mount a CD-ROM or DVD-ROM manually:

1. Log in as the root user.

   ```
   prompt> su
   Password:
   ```

2. Create the CD-ROM or DVD-ROM mount point directory:

   ```
   # mkdir mount_point
   ```

3. Mount the CD-ROM or DVD-ROM drive on the mount point directory:

   ```
   # mount options device_name mount_point
   ```

   The following example mounts the CD-ROM manually on `/cdrom`, without using the Solaris Volume Management software. Execute the following commands as root user:

   ```
   # mkdir /cdrom
   # mount -r -F hsfs device_name /cdrom
   ```

   You can also use the same commands and options to mount the DVD-ROM.

4. Log out from the root user.

```
# exit
```

3.15 Starting the Oracle Universal Installer

1. If you are installing from a CD-ROM or DVD-ROM and your computer does not mount CD-ROMs or DVDs automatically, you need to set the mount point manually. See Section 3.14, "Setting the Mount Point for the CD-ROM or DVD-ROM" for details.
2. Log in as the `oracle` user.
3. If you are installing Oracle Application Server on a multihomed computer, create the `OUI_HOSTNAME` environment variable. Set this variable to point to the hostname of the computer on which you are installing Oracle Application Server.

   See Also:

   - Section 2.11.1, "Installing on Multihomed (Multi-IP) Computers"

4. If you are installing from your hard drive, go to the next step.

   CD-ROM users: Insert Oracle Application Server Disk 1 into the CD-ROM drive.

   DVD-ROM users: Insert the Oracle Application Server DVD-ROM into the DVD-ROM drive.

5. Run the Oracle Universal Installer using the command shown after the notes:

   Notes:

   - Be sure you are not logged in as the root user when you start the Oracle Universal Installer. The installer gives an error message if you try to run it as the root user.
   - Do not start the installation inside the mount_point directory. If you do, then you may not be able to eject the installation disk. The `cd` command below changes your current directory to your home directory.

   CD-ROM:

   ```
   prompt> cd
   prompt> mount_point/10.1.4disk1/runInstaller
   ```

   DVD-ROM:

   ```
   prompt> cd
   prompt> mount_point/application_server/runInstaller
   ```

   Hard Drive:

   ```
   prompt> cd disk1_directory
   prompt> runInstaller
   ```

   where *disk1_directory* is the directory where you unzipped the Disk 1 file.

This launches Oracle Universal Installer, through which you install Oracle Application Server.

4

Installing OracleAS Infrastructure

Table 4–1 lists the contents of this chapter:

Table 4–1 Contents of This Chapter

Topics	Procedures
▪ Section 4.1, "Infrastructure Installation Types" ▪ Section 4.2, "Why Would I Select the Different Infrastructure Installation Types?" ▪ Section 4.3, "Order of Installation for the Infrastructure" ▪ Section 4.4, "Can I Install Components on Separate Computers?" ▪ Section 4.5, "Tips for Installing Oracle Identity Management Components Separately" ▪ Section 4.6, "Do I Need the Oracle Delegated Administration Services or the Oracle Directory Integration Platform Components?" ▪ Section 4.7, "Can I Configure Components After Installation?" ▪ Section 4.8, "Can I Use an Existing Database for the OracleAS Metadata Repository?" ▪ Section 4.9, "Can I Use an Existing Oracle Internet Directory?" ▪ Section 4.10, "Registration of OracleAS Metadata Repository in Oracle Internet Directory and Password Randomization" ▪ Section 4.11, "Contents of the OracleAS Metadata Repository" ▪ Section 4.12, "Can I Use Multiple Metadata Repositories?" ▪ Section 4.13, "What High Availability Options Does Oracle Application Server Support?" ▪ Section 4.14, "Restrictions on the Passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP Users" ▪ Section 4.15, "Support for NE8ISO8859P10 and CEL8ISO8859P14 Characters Sets" ▪ Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?" ▪ Section 4.17, "How to Determine Port Numbers Used by Components" ▪ Section 4.18, "Can I Add OCA After Installation?" ▪ Section 4.19, "How to Deploy Oracle Delegated Administration Services on a Separate Host"	▪ Section 4.20, "Installing OracleAS Infrastructure" ▪ Section 4.21, "Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory" ▪ Section 4.22, "Installing OracleAS Metadata Repository in a New Database" ▪ Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)" ▪ Section 4.24, "Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)" ▪ Section 4.25, "Installing Oracle Internet Directory Only" ▪ Section 4.26, "Installing OCA and OracleAS Metadata Repository Only" ▪ Section 4.27, "Install Fragment: The First Few Screens of the Installation" ▪ Section 4.28, "Install Fragment: The Last Few Screens of the Installation" ▪ Section 4.29, "Install Fragment: Database Screens" ▪ Section 4.30, "Install Fragment: OCA Screens"

4.1 Infrastructure Installation Types

Infrastructure components can be grouped into Oracle Identity Management components and the OracleAS Metadata Repository component. Table 4–2 describes these components:

Table 4–2 OracleAS Infrastructure Components

Infrastructure Components	Description
Oracle Identity Management components	These components provide directory, security, and user management functionality. Some of these components have schemas in the OracleAS Metadata Repository. ■ Oracle Internet Directory ■ OracleAS Single Sign-On ■ Oracle Delegated Administration Services ■ Oracle Directory Integration Platform ■ OracleAS Certificate Authority
OracleAS Metadata Repository	OracleAS Metadata Repository is a collection of schemas used by other Oracle Application Server components. The schemas can be grouped into these categories: ■ Product metadata ■ Oracle Identity Management metadata ■ Management metadata See Section 4.11, "Contents of the OracleAS Metadata Repository" for details.

When you install the infrastructure, the installer asks if you want to install the Oracle Identity Management components, OracleAS Metadata Repository, or both. These are the installation types for the OracleAS Infrastructure:

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

In addition to the components listed in Table 4–2, when you install the OracleAS Infrastructure, you also get the Oracle HTTP Server, Oracle Containers for J2EE, and Oracle Enterprise Manager 10*g* components. These components are always installed and configured, regardless of which installation type you selected.

See the next section, Section 4.2, "Why Would I Select the Different Infrastructure Installation Types?"

4.2 Why Would I Select the Different Infrastructure Installation Types?

By separating the infrastructure into Oracle Identity Management components and OracleAS Metadata Repository, the installer enables you to install the OracleAS Infrastructure components over multiple computers. For example, you can install the OracleAS Metadata Repository on one computer, and the Oracle Identity Management components on another computer. Within the Oracle Identity Management option, you can install Oracle Identity Management components over multiple computers as well.

These options also enable you to create a new database or use an existing database for the OracleAS Metadata Repository. Selecting either the "OracleAS Metadata Repository" or the "OracleAS Metadata Repository and Oracle Identity Management" option causes the installer to create a new database and populate it with the OracleAS Metadata Repository.

To use an existing database, see Section 4.8, "Can I Use an Existing Database for the OracleAS Metadata Repository?"

4.3 Order of Installation for the Infrastructure

If you plan to install both OracleAS Metadata Repository and Oracle Identity Management components on the same computer, select the "Oracle Identity Management and OracleAS Metadata Repository" option. The installer installs the components in the proper order. See Section 4.20, "Installing OracleAS Infrastructure" for the step-by-step procedure.

If you plan to install the infrastructure components on separate computers, install them in this order:

1. Install the OracleAS Metadata Repository.

   You can have the installer create a new database and populate it with the OracleAS Metadata Repository, or you can run the Oracle Application Server Repository Creation Assistant to install the OracleAS Metadata Repository in an existing database.

   Note that you cannot register the OracleAS Metadata Repository with Oracle Internet Directory at this point, because you do not have an Oracle Internet Directory yet. The registration is done in the next step.

   See:

   - Section 4.22, "Installing OracleAS Metadata Repository in a New Database"
   - For information on how to install the OracleAS Metadata Repository in an existing database, see the *Oracle Application Server Metadata Repository Creation Assistant User's Guide*.

2. Install the Oracle Identity Management components.

   The installer prompts you to enter the connect information for the OracleAS Metadata Repository database.

   See Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)" for the step-by-step procedure.

   The installer registers the OracleAS Metadata Repository with the newly created Oracle Internet Directory. See Section 4.10, "Registration of OracleAS Metadata Repository in Oracle Internet Directory and Password Randomization" for details about registration.

Installing Only the OracleAS Metadata Repository Does Not Give You an Oracle Application Server Instance

If you install only the OracleAS Metadata Repository when installing the infrastructure, the installer creates a new database and populates it with the OracleAS Metadata Repository schemas. This instance is different from other Oracle Application Server instances in the following ways:

- The installer does not prompt you to name this Oracle Application Server instance.
- At the end of installation, Oracle Enterprise Manager 10*g* Application Server Control is not started up, because it is not configured for this instance. You do not need it to manage this instance, which consists of only the metadata repository database.

  To manage this instance, you use database management tools. For more information, see the chapter "Introduction to Administration Tools" in the *Oracle Application Server Administrator's Guide*.
- At the end of installation, Oracle HTTP Server is also not started up, because you do not need it to manage this instance.

4.4 Can I Install Components on Separate Computers?

You already know that you can install Oracle Application Server instances on separate computers. In addition, you can also distribute components over multiple computers. This is especially useful for infrastructure components. You might want to do this to improve performance, security, scalability, and availability of infrastructure services.

Examples:

- The OracleAS Infrastructure uses an Oracle database to contain the OracleAS Metadata Repository. You can install this database on its own computer.
- You can install the Oracle Identity Management components in the infrastructure on one or more computers.

Table 4–3 shows some possible OracleAS Infrastructure configurations:

Table 4–3 OracleAS Infrastructure Configurations

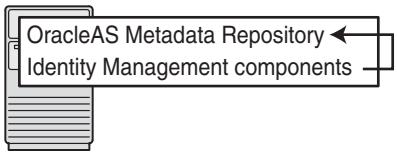
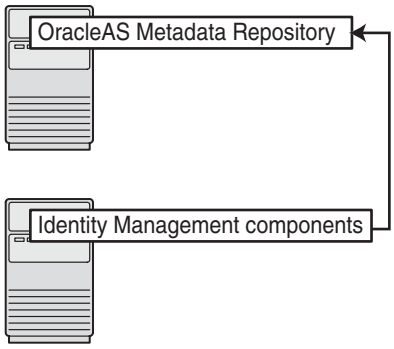
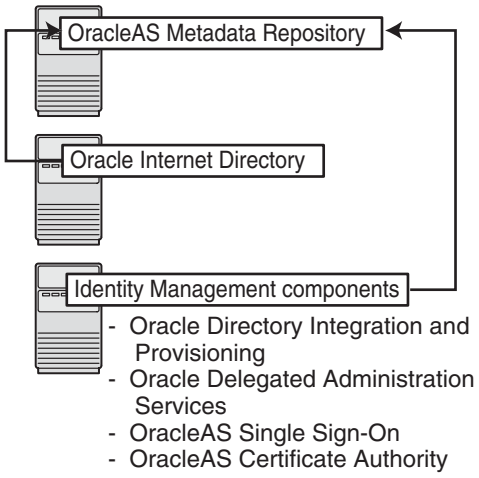
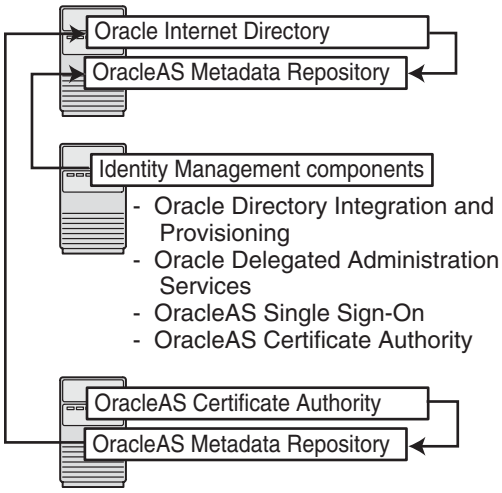
Configuration	Description / How to Install
	In this configuration, the OracleAS Metadata Repository and the Oracle Identity Management components run from the same Oracle home. To install this configuration, install the OracleAS Metadata Repository and the Oracle Identity Management components at the same time. For installation steps, see Section 4.20, "Installing OracleAS Infrastructure".
	In this configuration, the OracleAS Metadata Repository and the Oracle Identity Management components run on separate computers. To install this configuration: **1.** Install the OracleAS Metadata Repository first. See Section 4.22, "Installing OracleAS Metadata Repository in a New Database". Alternatively, you can install the OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details. **2.** Then install the Oracle Identity Management components. See Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)".

Table 4–3 (Cont.) OracleAS Infrastructure Configurations

Configuration	Description / How to Install
	In this configuration, the OracleAS Metadata Repository runs on one computer, Oracle Internet Directory runs on a second computer, and the remaining Oracle Identity Management components run on a third computer. To install this configuration: 1. Install the OracleAS Metadata Repository first. See Section 4.22, "Installing OracleAS Metadata Repository in a New Database". Alternatively, you can install the OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details. 2. Install Oracle Internet Directory. See Section 4.25, "Installing Oracle Internet Directory Only". 3. Install the remaining Oracle Identity Management components. See Section 4.24, "Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)".
	In this configuration, you want OCA to use its own OracleAS Metadata Repository (for security reasons). Other Oracle Identity Management components use another OracleAS Metadata Repository. To install this configuration: 1. Install OracleAS Metadata Repository and Oracle Identity Management components, but not OCA. You can install all these items in the same Oracle home (see the first configuration), or you can distribute them. The figure shows a distributed configuration. 2. Install OCA with its own OracleAS Metadata Repository. See Section 4.21, "Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory".

Note that if you install Oracle Identity Management components on a separate computer from OracleAS Metadata Repository, then the OracleAS Metadata Repository will need network access to the Oracle Identity Management components.

See also Chapter 1, "Product and Installation Overview", which describes configurations involving multiple computers and distributed components.

4.5 Tips for Installing Oracle Identity Management Components Separately

If you are installing Oracle Identity Management components separately, keep the following guidelines in mind when choosing which components to configure in the Select Configuration Options screen:

- You *cannot* install and configure more than one OCA against the same OracleAS Metadata Repository. You *can* install and configure more than one OracleAS Single Sign-On, Oracle Delegated Administration Services, or Oracle Directory

Integration Platform against the same OracleAS Metadata Repository. If you want to configure more than one Oracle Internet Directory against the same OracleAS Metadata Repository, see the *Oracle Internet Directory Administrator's Guide*.

- You must select at least one component to configure. Otherwise the installation will not succeed.
- If you configure OracleAS Single Sign-On and Oracle Delegated Administration Services in separate installations against the same Oracle Internet Directory, make sure you configure OracleAS Single Sign-On before Oracle Delegated Administration Services. This is because Oracle Delegated Administration Services depends on mod_osso, which will not be set up during installation unless the Oracle Internet Directory it points to already has OracleAS Single Sign-On configured.
- If you have an Oracle Identity Management installation that includes Oracle Directory Integration Platform but does not include Oracle Internet Directory, you will still see an Oracle Internet Directory process in the `opmnctl status` output. This is because oidmon must be installed and started in order to start the Oracle Directory Integration Platform process.

4.6 Do I Need the Oracle Delegated Administration Services or the Oracle Directory Integration Platform Components?

These components are optional, but you might want to install them because they provide the following services:

- Oracle Delegated Administration Services provide a browser-based interface to Oracle Internet Directory. Users can use the interface to perform tasks such as changing their passwords, searching for other users in the directory, and creating groups. Users can even create additional users (if they have the proper privilege).
- Oracle Directory Integration Platform enables you to integrate applications and third-party LDAP directories with Oracle Internet Directory. You can use Oracle Directory Integration Platform to synchronize data in all directories, and to send notifications to applications when data in Oracle Internet Directory changes (for example, when you add users or groups to Oracle Internet Directory).

4.7 Can I Configure Components After Installation?

If you did not configure a component during installation (that is, you did not select the component in the Select Configuration Options screen), you can configure some components after installation.

You cannot configure Oracle Internet Directory after installation. You need to install and configure Oracle Internet Directory through the installer.

See Section 11.7, "Component Configuration After Installation" for details.

4.8 Can I Use an Existing Database for the OracleAS Metadata Repository?

You can install the OracleAS Metadata Repository in a new database, or in an existing database.

If you want to install the OracleAS Metadata Repository in an existing database, see *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

4.9 Can I Use an Existing Oracle Internet Directory?

You can use an existing Oracle Internet Directory instead of having the installer create a new one. You might want to do this if your applications need to authenticate users that are already stored in your Oracle Internet Directory. During the infrastructure installation, do not select "Oracle Internet Directory" in the Select Configuration Options screen.

You need to provide the connect information (hostname, port, username, password) for the existing Oracle Internet Directory.

The Oracle Internet Directory must be version 9.0.4 or later. Note that Oracle Internet Directory version 9.2.x is not supported.

To determine the Oracle Internet Directory version, make sure that Oracle Internet Directory is up and running. Then run the following command:

```
prompt> oidldapd -version
```

The `oidldapd` command can be found in the `ORACLE_HOME/bin` directory, where ORACLE_HOME is the root directory where you installed Oracle Internet Directory.

4.10 Registration of OracleAS Metadata Repository in Oracle Internet Directory and Password Randomization

The OracleAS Metadata Repository and the Oracle Internet Directory work closely together. Before you can use an OracleAS Metadata Repository (in most cases), ensure that it is registered with an Oracle Internet Directory.

An exception to this rule is when you want to use a J2EE and Web Cache middle tier with the Database-Based Farm feature but without the Oracle Identity Management Access feature. In this case, you need an OracleAS Metadata Repository, but it need not be registered with an Oracle Internet Directory.

Table 4–4 shows the scenarios where the installer automatically registers the OracleAS Metadata Repository with an Oracle Internet Directory, and the scenarios where you decide whether to register or not.

Table 4–4 Database Registration Scenarios

Scenario	Registration	Schema Passwords
Install and configure the OracleAS Metadata Repository and Oracle Internet Directory in the same installation session For steps, see Section 4.20, "Installing OracleAS Infrastructure".	Automatic	Randomized
Install the OracleAS Metadata Repository against an existing Oracle Internet Directory See Section 4.21, "Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory".	Automatic	Randomized

Table 4–4 (Cont.) Database Registration Scenarios

Scenario	Registration	Schema Passwords
Install an Oracle Internet Directory against an existing OracleAS Metadata Repository See Section 4.25, "Installing Oracle Internet Directory Only".	Automatic	Randomized (the metadata repository schemas are given new randomized passwords)
Install the OracleAS Metadata Repository only (without installing Oracle Identity Management components) and you choose to register it with Oracle Internet Directory This scenario applies to installing it in a new database or in an existing database. To install OracleAS Metadata Repository in a new database, see Section 4.22, "Installing OracleAS Metadata Repository in a New Database". To install OracleAS Metadata Repository in an existing database, see the*Oracle Application Server Metadata Repository Creation Assistant User's Guide*.	Yes	Randomized
Install the OracleAS Metadata Repository only (without installing Oracle Identity Management components) and you choose **not** to register it with Oracle Internet Directory This scenario applies to installing it in a new database or in an existing database.	No	The schemas are locked, and the passwords are expired.

In the last two scenarios, the installer asks you if you want to register the OracleAS Metadata Repository with an Oracle Internet Directory. If you answer yes, you provide connect information for the Oracle Internet Directory. If you answer no, the installer does not register the OracleAS Metadata Repository with an Oracle Internet Directory.

Note: If you did not register the OracleAS Metadata Repository with an Oracle Internet Directory during installation, you can register it later using the Oracle Application Server Repository Creation Assistant. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

4.11 Contents of the OracleAS Metadata Repository

The OracleAS Metadata Repository contains schemas that can be grouped into these categories:

- Product Metadata schemas

  These schemas are used by middle-tier components, such as OracleAS Portal and OracleAS Wireless.

- Oracle Identity Management schemas

  These schemas are used by Oracle Identity Management components, such as Oracle Internet Directory, OracleAS Single Sign-On, and OCA.

- Management schemas

  These schemas are used by components such as DCM.

If you are interested in seeing the names of all the schemas, see the *Oracle Application Server Metadata Repository Creation Assistant User's Guide*.

4.12 Can I Use Multiple Metadata Repositories?

You can install multiple metadata repositories to increase performance. This enables different components in your topology to use different metadata repositories. To use multiple metadata repositories, follow these guidelines:

- To enable a Portal and Wireless or a Business Intelligence and Forms middle tier to use a second metadata repository for product metadata:

  a. Install the second metadata repository and register it with the Oracle Internet Directory.

  You can do this using the installer or the OracleAS RepCA. Use the installer to create a new database containing the OracleAS Metadata Repository, or use the OracleAS RepCA to install the OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

  b. When you install the Portal and Wireless or the Business Intelligence and Forms middle tier, select the second metadata repository from the list of registered repositories. This is the metadata repository that the middle tier will use for its product metadata.

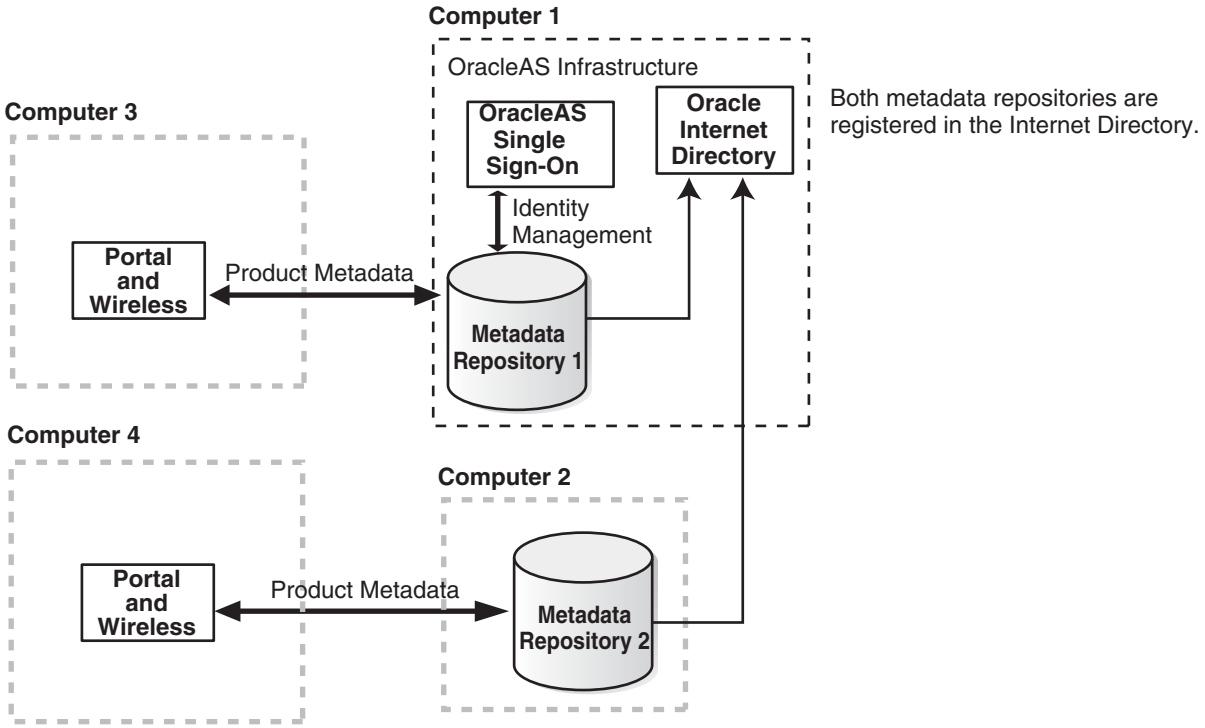
- To use a second metadata repository for a J2EE and Web Cache middle tier, you have different options, depending on which J2EE and Web Cache features you need:

  - If you need both the Oracle Identity Management Access feature and the Database-Based Farm feature, you need to register the second metadata repository with the Oracle Internet Directory.
  - If you need only the Database-Based Farm feature, you do not need to register the second metadata repository. The reason for this is that you might not have an Oracle Internet Directory.

Figure 4–1 shows a topology that involves two metadata repositories. It uses four computers:

- Computer 1 runs a metadata repository and Oracle Identity Management components. The Oracle Identity Management components use this metadata repository.
- Computer 2 has a metadata repository that is registered with the Oracle Internet Directory running on Computer 1.
- Computer 3 has a Portal and Wireless middle tier. This middle tier knows to use the metadata repository on Computer 1 for its product metadata because it was registered with that metadata repository during installation.
- Computer 4 also has a Portal and Wireless middle tier. This middle tier knows to use the metadata repository on Computer 2 for its product metadata because it was registered with that metadata repository during installation.

Figure 4–1 Multiple Metadata Repositories in Use



Notes:

- If you are installing multiple metadata repositories on the same computer, each metadata repository must have a unique global database name and system identifier (SID).
- If you are registering multiple metadata repositories with the same Oracle Internet Directory, each metadata repository must have a unique global database name and SID. If not, the Oracle Internet Directory Configuration Assistant will fail when you install the second metadata repository with the same name.

4.13 What High Availability Options Does Oracle Application Server Support?

Oracle Application Server can run in the following high availability environments:

- OracleAS Cold Failover Cluster
- OracleAS Cluster (Identity Management)
- OracleAS Disaster Recovery

See Chapter 7, "Installing in High Availability Environments: Overview" for details.

4.14 Restrictions on the Passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP Users

When you install the OracleAS Metadata Repository in a new database, the installer prompts you to set the passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP

users, which are privileged users for the database. The passwords for these users have the following restrictions:

- Passwords must be shorter than 30 characters.
- Passwords can contain only alphanumeric characters from your database character set, the underscore (_), the dollar sign ($), and the number sign (#).
- Passwords must begin with an alphabetic character. Passwords cannot begin with a number, the underscore (_), the dollar sign ($), or the number sign (#).
- Passwords cannot be Oracle reserved words. The *Oracle SQL Reference* lists the reserved words. You can find this guide on Oracle Technology Network (`http://www.oracle.com/technology/documentation`). Or you can just avoid using words that sound like they might be reserved words.
- Passwords cannot be the default passwords, which are `change_on_install` and `manager`.

4.15 Support for NE8ISO8859P10 and CEL8ISO8859P14 Characters Sets

If you use characters in the NE8ISO8859P10 or CEL8ISO8859P14 character sets, make sure that your database uses the Unicode character set AL32UTF8. If you are installing a new database, select "AL32UTF8" in the Specify Database Configuration Options screen.

The reason for this is that Java does not support the NE8ISO8859P10 or CEL8ISO8859P14 character sets. If you configure the database to use a character set not supported by Java, you will get an "Unsupported IANA character encoding" error in OracleAS Portal.

4.16 What Do I Enter in the "Specify Namespace in Internet Directory" Screen?

The distinguished name (DN) that you specify on this screen will be designated as the namespace in Oracle Internet Directory where users and groups are administered.

Select the suggested namespace if it meets your deployment requirements. If not, enter a DN that you want in the custom namespace field. The installer determines the suggested namespace from the `/etc/hosts` file. See Section 2.10, "The /etc/hosts File".

If you plan to integrate your Oracle Identity Management components with a third-party directory, you should specify the DN of a namespace that matches the DN of the default namespace in the third-party directory. See the *Oracle Internet Directory Administrator's Guide* for details on integration with third-party directories.

4.17 How to Determine Port Numbers Used by Components

During installation, you might need to know port numbers used by certain Oracle Application Server components. For example, if you install OracleAS Infrastructure against an existing Oracle Internet Directory, the installer prompts for the Oracle Internet Directory hostname and port number.

You can get a list of port numbers in the following ways:

- Use Oracle Enterprise Manager 10*g* Application Server Control.

Click the Ports link on the Enterprise Manager home page. This takes you to a page that lists all ports in use and the suggested port ranges for different components.

- Look in the `ORACLE_HOME/install/portlist.ini` file. `ORACLE_HOME` refers to the directory containing the Oracle Application Server installation.

  Note that if you change a component's port number after installation, the `portlist.ini` file is *not* updated. The `portlist.ini` file is not updated after installation.

4.18 Can I Add OCA After Installation?

If you installed OracleAS Infrastructure but did not select to configure OCA, and later decide that you want to use OCA, you have to install it in a separate Oracle home. You cannot install it in an existing Oracle home.

When you install OCA in a new Oracle home, you can install it on the same or different computer as the OracleAS Infrastructure. You can also install it with its own OracleAS Metadata Repository or install it against an existing OracleAS Metadata Repository:

- Install OCA only.

  OCA will share the OracleAS Metadata Repository that you installed earlier. If you are installing OCA on the same computer as the OracleAS Infrastructure instance, you might want to consider this option for performance reasons. (The second option requires running two databases on the same computer; this could degrade performance.)

  See Section 4.24, "Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)" for details. In the Select Configuration Options screen, select **Oracle Application Server Certificate Authority (OCA)** only.

- Install OCA with its own OracleAS Metadata Repository.

4.19 How to Deploy Oracle Delegated Administration Services on a Separate Host

To configure Oracle Delegated Administration Services in a separate Oracle Home, you perform a standalone installation of it. To do this, select the Identity Management installation type, and, on the Configuration Options screen, select Delegated Administration Services.

4.20 Installing OracleAS Infrastructure

Perform this procedure to install an OracleAS Metadata Repository and Oracle Identity Management components. This procedure provides a complete OracleAS Infrastructure in a single Oracle home.

If you want to use an existing Oracle Internet Directory, see Section 4.21, "Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory".

If you want to use an existing database for the OracleAS Metadata Repository, see the *Oracle Application Server Metadata Repository Creation Assistant User's Guide*.

Table 4–5 Steps for Installing OracleAS Infrastructure

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ▪ In the Select Installation Type screen, select **Identity Management and Metadata Repository**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform**. Select **Oracle Application Server Certificate Authority (OCA)** if you want to configure your own certificate authority which can issue certificates for users and servers. Do not select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file. Click **Next**.
4.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
5.	OCA screens	If you select **Oracle Application Server Certificate Authority (OCA)** in the Select Configuration Options screen, the installer displays screens where you need to enter OCA information. See Section 4.30, "Install Fragment: OCA Screens".
6.	Oracle Database screens	Enter information for the OracleAS Metadata Repository database. See Section 4.29, "Install Fragment: Database Screens".
7.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `infra` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
8.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

4.21 Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory

Perform this procedure to install Oracle Identity Management components (except Oracle Internet Directory) and the OracleAS Metadata Repository.

Prerequisite: Oracle Internet Directory version 9.0.4 or later

You would perform this procedure in cases where you already have an Oracle Internet Directory (and its associated OracleAS Metadata Repository), and you want to:

- Install OCA with its own OracleAS Metadata Repository, or
- Install another OracleAS Metadata Repository for Oracle Internet Directory replication.

You cannot use this procedure to install other Oracle Identity Management components (OracleAS Single Sign-On, Oracle Delegated Administration Services, or Oracle Directory Integration Platform). To install Oracle Identity Management components without OracleAS Metadata Repository, follow the procedure in Section 4.24, "Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)".

Table 4–6 Steps for Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ■ In the Select Installation Type screen, select **Identity Management and Metadata Repository**.
2.	Select Configuration Options	Do not select **Oracle Internet Directory** because you want to use an existing one. Do not select **Oracle Application Server Single Sign-On**. Do not select **Oracle Application Server Delegated Administration Services**. Do not select **Oracle Directory Integration Platform**. Select **Oracle Application Server Certificate Authority (OCA)** if you want to configure your own certificate authority which can issue certificates for users and servers. Do not select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file. Click **Next**.
4.	Register with Oracle Internet Directory	**Hostname**: Enter the name of the computer where Oracle Internet Directory is running. **SSL Port**: Enter the SSL port at which Oracle Internet Directory is listening. See Section 4.17, "How to Determine Port Numbers Used by Components" if you do not know the port number. Click **Next**.

Table 4–6 (Cont.) Steps for Installing OracleAS Infrastructure Against an Existing Oracle Internet Directory

	Screen	Action
5.	Specify Oracle Internet Directory Login	**Username**: Enter the username to log in to Oracle Internet Directory. You must log in as a user who belongs to the necessary groups in Oracle Internet Directory. Which groups are necessary depends on which components you are installing. See Section 5.3, "Groups Required to Configure or Deinstall Components" for details. **Password**: Enter the password for the username. **Realm**: Enter the realm against which to validate the username. This field appears only if your Oracle Internet Directory has multiple realms. Click **Next**.
6.	OCA screens	If you select **Oracle Application Server Certificate Authority (OCA)** in the Select Configuration Options screen, the installer displays screens where you need to enter OCA information. See Section 4.30, "Install Fragment: OCA Screens".
7.	Oracle Database screens	Enter information for the OracleAS Metadata Repository database. See Section 4.29, "Install Fragment: Database Screens".
8.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `infra` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
9.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

4.22 Installing OracleAS Metadata Repository in a New Database

Perform this procedure to create a new database and populate it with the OracleAS Metadata Repository. This procedure does not install any Oracle Identity Management components.

Table 4–7 Steps for Installing OracleAS Metadata Repository in a New Database

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ■ In the Select Installation Type screen, select **Metadata Repository**.
2.	Select Configuration Options	Do not select **High Availability and Replication**. Click **Next**.
3.	Register OracleAS Metadata Repository	If you already have an Oracle Internet Directory and know its connect information, select **Yes** and enter the name of the computer where Oracle Internet Directory is running and the port number. See Section 4.17, "How to Determine Port Numbers Used by Components" if you do not know the port number. **Use Only SSL Connections with this Oracle Internet Directory**: Select this option if you want Oracle Application Server components to use only SSL to connect to Oracle Internet Directory. If you do not have an Oracle Internet Directory, or do not know its connect information, select **No**. Click **Next**.
4.	Specify Oracle Internet Directory Login	This screen appears only if you selected **Yes** in the previous screen. **Username**: Enter the username for logging into Oracle Internet Directory. The user must belong to the iAS Admins group in Oracle Internet Directory. **Password**: Enter the password. **Realm**: This field appears only if your Oracle Internet Directory contains multiple realms. Enter the name of the realm against which to authenticate the user. Click **Next**.
5.	Oracle Database screens	Enter information for the OracleAS Metadata Repository database. See Section 4.29, "Install Fragment: Database Screens".
6.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

7.	--	Unlock the `dcm` schema, and set its password. This step is required only if you want to use the metadata repository for database clustering of middle-tier instances.
		1. Set the ORACLE_HOME environment variable to point to the full path of the directory where you installed the OracleAS Metadata Repository.
		2. Set the ORACLE_SID environment variable to the SID of the OracleAS Metadata Repository.
		3. Unlock the `dcm` schema and set its password using SQL*Plus.
		The following `alter user` command sets the password to "welcome1", but you can set it to any value.
		`prompt> $ORACLE_HOME/bin/sqlplus "sys/password as sysdba"`
		`SQL> alter user dcm identified by welcome1 account unlock;`

4.23 Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)

Perform this procedure to install Oracle Identity Management components without installing an OracleAS Metadata Repository.

Follow this procedure to configure Oracle Internet Directory against a remote OracleAS Metadata Repository. You have installed the OracleAS Metadata Repository in an existing database (see the *Oracle Application Server Metadata Repository Creation Assistant User's Guide*) or in a new database (Section 4.22, "Installing OracleAS Metadata Repository in a New Database").

Prerequisite: OracleAS Metadata Repository that is not already registered with any Oracle Internet Directory

Table 4–8 Steps for Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ▪ In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services** and/or **Oracle Directory Integration Platform** if you need the services provided by these components. See Section 4.6, "Do I Need the Oracle Delegated Administration Services or the Oracle Directory Integration Platform Components?" Select **Oracle Application Server Certificate Authority (OCA)** if you want to configure your own certificate authority which can issue certificates for users and servers. Do not select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file. Click **Next**.
4.	Specify Repository	**Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the name of the computer where the database is running, and the port number at which it is listening. Use the format: *`host:port`*. **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.

Table 4–8 (Cont.) Steps for Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)

	Screen	Action
6.	Enter information to configure OCA	Provide the information as prompted by the OCA screens. See Section 4.30, "Install Fragment: OCA Screens" for details.
7.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `id_mgmt` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
8.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

4.24 Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)

Perform this procedure to install Oracle Identity Management components without installing an OracleAS Metadata Repository or Oracle Internet Directory.

Use this procedure to install additional OracleAS Single Sign-On, Oracle Delegated Administration Services, or Oracle Directory Integration Platform components against an existing Oracle Internet Directory.

Prerequisites: OracleAS Metadata Repository, Oracle Internet Directory version 9.0.4 or later.

Table 4–9 Steps for Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ▪ In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Do not select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services** and/or **Oracle Directory Integration Platform** if you need the services provided by these components. See Section 4.6, "Do I Need the Oracle Delegated Administration Services or the Oracle Directory Integration Platform Components?" Select **Oracle Application Server Certificate Authority (OCA)** if you want to configure your own certificate authority which can issue certificates for users and servers. Do not select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file. Click **Next**.
4.	Register with Oracle Internet Directory	**Hostname**: Enter the name of the computer where Oracle Internet Directory is running. **SSL Port**: Enter the SSL port at which Oracle Internet Directory is listening. See Section 4.17, "How to Determine Port Numbers Used by Components" if you do not know the port number. Click **Next**.
5.	Specify Oracle Internet Directory Login	**Username**: Enter the username to log in to Oracle Internet Directory. You must log in as a user who belongs to the necessary groups in Oracle Internet Directory. Which groups are necessary depends on which components you are installing. See Section 5.3, "Groups Required to Configure or Deinstall Components" for details. **Password**: Enter the password for the username. **Realm**: Enter the realm against which to validate the username. This field appears only if your Oracle Internet Directory has multiple realms. Click **Next**.
6.	Specify ODS Password	Enter the password for the ODS schema in the OracleAS Metadata Repository. The ODS schema is the main schema used by Oracle Internet Directory. By default, the ODS password is the same as the ias_admin password (the password that you entered in the Specify Instance Name and ias_admin Password screen). Click **Next**.

Table 4–9 (Cont.) Steps for Installing Oracle Identity Management Components Only (Excluding Oracle Internet Directory)

	Screen	Action
7.	Enter information to configure OCA	Provide the information as prompted by the OCA screens. See Section 4.30, "Install Fragment: OCA Screens" for details.
8.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `id_mgmt` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
9.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

4.25 Installing Oracle Internet Directory Only

Perform this procedure to install an Oracle Internet Directory.

Prerequisite: OracleAS Metadata Repository

Table 4–10 Steps for Installing Oracle Internet Directory

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ■ In the Select Installation Type screen, select **Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Do not select **Oracle Application Server Single Sign-On**. Do not select **Oracle Application Server Delegated Administration Services**. Do not select **Oracle Directory Integration Platform**. Do not select **Oracle Application Server Certificate Authority (OCA)**. Do not select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file. Click **Next**.

Table 4–10 (Cont.) Steps for Installing Oracle Internet Directory

	Screen	Action
4.	Specify Repository	**Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the name of the computer where the database is running, and the port number at which it is listening. Use the format: *`host:port`*. **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
6.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `infra` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
7.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

4.26 Installing OCA and OracleAS Metadata Repository Only

Perform this procedure to install the OCA and the OracleAS Metadata Repository components only.

Prerequisites: Oracle Internet Directory version 9.0.4 or later

Table 4–11 Steps for Installing OCA and OracleAS Metadata Repository

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ■ In the Select Installation Type screen, select **Identity Management and OracleAS Metadata Repository**.
2.	Select Configuration Options	Do not select **Oracle Internet Directory** because you want to use an existing one. Do not select **Oracle Application Server Single Sign-On**. Do not select **Oracle Application Server Delegated Administration Services**. Do not select **Oracle Directory Integration Platform**. Select **Oracle Application Server Certificate Authority (OCA)**. Do not select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file. Click **Next**.
4.	Register with Oracle Internet Directory	**Hostname**: Enter the name of the computer where Oracle Internet Directory is running. **SSL Port**: Enter the SSL port at which Oracle Internet Directory is listening. See Section 4.17, "How to Determine Port Numbers Used by Components" if you do not know the port number. Click **Next**.
5.	Specify Oracle Internet Directory Login	**Username**: Enter the username to log in to Oracle Internet Directory. You must log in as a user who belongs to the Trusted Application Admins group and to the iAS Admins group in Oracle Internet Directory. **Password**: Enter the password for the username. **Realm**: Enter the realm against which to validate the username. This field appears only if your Oracle Internet Directory has multiple realms. Click **Next**.
6.	OCA screens	Enter information to configure OCA. See Section 4.30, "Install Fragment: OCA Screens".
7.	Oracle Database screens	Enter information for the OracleAS Metadata Repository database. See Section 4.29, "Install Fragment: Database Screens".
8.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `infra_oca` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
9.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

4.27 Install Fragment: The First Few Screens of the Installation

The first few screens of the installer are described here because they are the same for all installations. Most installation procedures in this chapter refer to this section as their starting point.

Table 4–12 First Few Screens of the Installation

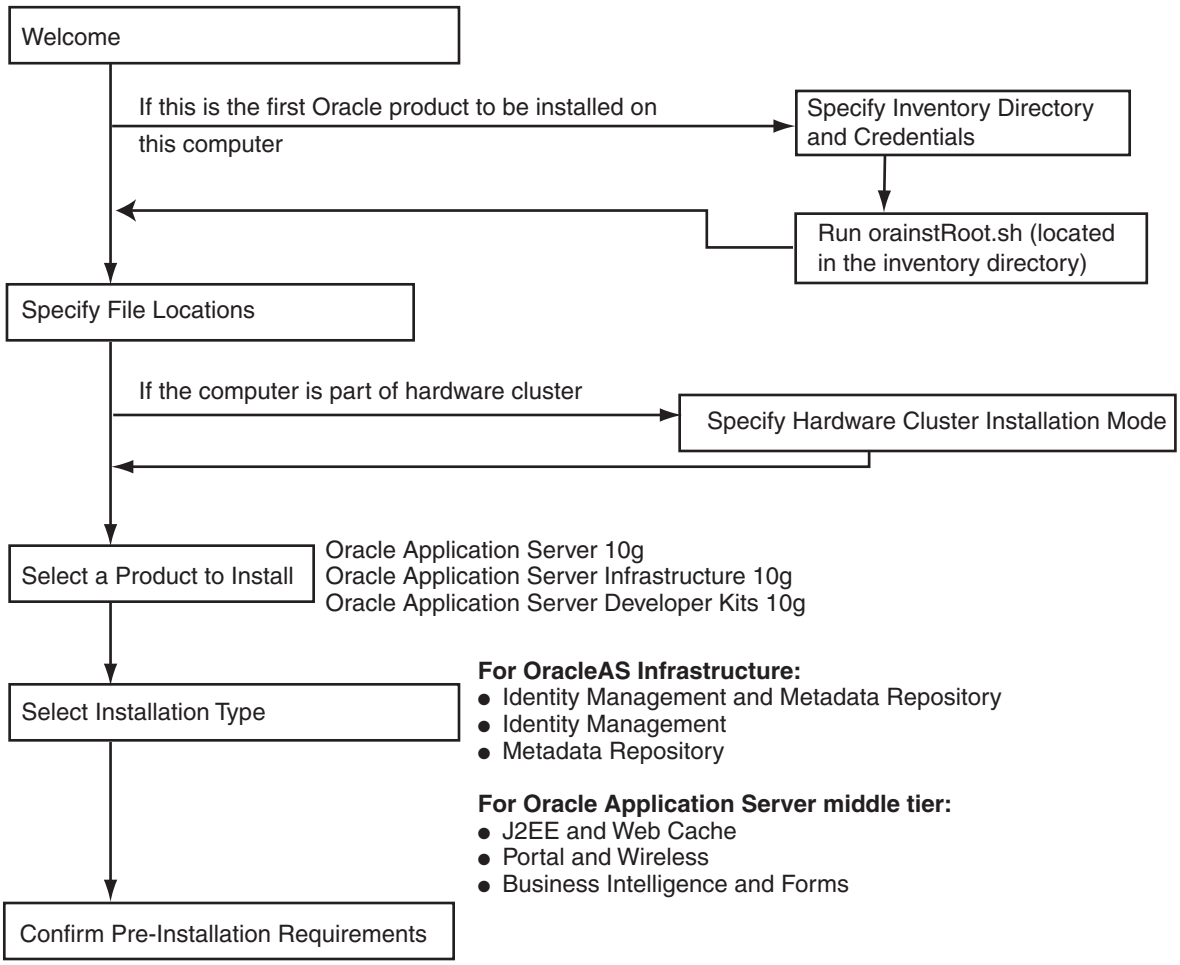
	Screen	Action
1.	--	Start the installer. See Section 3.15, "Starting the Oracle Universal Installer" for details.
2.	Welcome	Click **Next**.
3.	Specify Inventory Directory and Credentials	This screen appears only if this is the first installation of any Oracle product on this computer. **Enter the full path of the inventory directory**: Enter a full path to the inventory directory. Enter a directory that is different from the Oracle home directory for the product files. Example: `/opt/oracle/oraInventory` **Specify Operating System group name**: Select the operating system group that will have write permission for the inventory directory. Example: `oinstall` Click **Next**.
4.	Run `orainstRoot.sh`	This screen appears only if this is the first installation of any Oracle product on this computer. Run the `orainstRoot.sh` script in a different shell as the root user. The script is located in the oraInventory directory. After running the script, click **Continue**.
5.	Specify File Locations	**Name**: Enter a name to identify this Oracle home. The name can consist of alphanumeric and the underscore (_) characters only, and cannot be longer than 128 characters. Example: `OH_INFRA` **Path**: Enter the full path to the destination directory. This is the Oracle home. If the directory does not exist, the installer creates it. If you want to create the directory beforehand, create it as the `oracle` user; do not create it as the root user. Example: `/opt/oracle/infra` Click **Next**.
6.	Specify Hardware Cluster Installation Mode	This screen appears only if the computer is part of a hardware cluster. If you are installing an infrastructure, select the computers in the hardware cluster where you want to install the infrastructure. You can select multiple computers, or you can just select the current computer. Click **Next**.
7.	Select a Product to Install	Select **Oracle Application Server Infrastructure 10*g***. If you need to install additional languages, click **Product Languages**. See Section 3.4, "Installing Additional Languages" for details. Click **Next**.

Table 4–12 (Cont.) First Few Screens of the Installation

	Screen	Action
8.	Select Installation Type	The options displayed on this screen depend on what you selected in the Select a Product to Install screen. The installation types for OracleAS Infrastructure are: ▪ **Identity Management and Metadata Repository** ▪ **Identity Management** ▪ **Metadata Repository** Click **Next**. If you get an error message saying that the TMP environment variable is not set, it means that the default temp directory does not have enough space. You can either set the TMP environment variable to point to a different directory or free up enough space in the default temp directory. For details on the TMP environment variable, see Section 2.9.6, "TMP".
9.	Upgrade Existing Oracle9iAS Infrastructure	This screen appears if the installer detects an Infrastructure Release 2 (9.0.2) instance on the computer and you selected to install OracleAS Infrastructure. This screen presents you with the option to upgrade the existing Release 2 (9.0.2) Infrastructure, or install the current version of the OracleAS Infrastructure. If you want to upgrade, see the *Oracle Application Server Upgrade and Compatibility Guide*.
10.	Confirm Pre-Installation Requirements	Verify that your computer meets all the requirements. Click **Next**.

Figure 4–2 summarizes the screen sequence.

Figure 4–2 Sequence for the First Few Screens in the Installation



4.28 Install Fragment: The Last Few Screens of the Installation

The last few screens of the installer are described in this section because they are the same for all installations. Most installation procedures in this chapter refer to this section as their end point.

Table 4–13 Last Few Screens in the Installation

	Screen	Action
1.	Summary	Verify your selections and click **Install**.
2.	Install Progress	This screen shows the progress of the installation.
3.	Run `root.sh`	**Note:** Do not run the `root.sh` script until this dialog appears. **1.** When you see this dialog, run the `root.sh` script in a different shell as the root user. The script is located in this instance's Oracle home directory. **2.** Click **OK**.
4.	Configuration Assistants	This screen shows the progress of the configuration assistants. Configuration assistants configure components.
5.	End of Installation	Click **Exit** to quit the installer.

4.29 Install Fragment: Database Screens

If you are installing a new database for the OracleAS Metadata Repository, the installer displays the following screens:

Table 4–14 Database Screens

	Screen	Action
1.	Specify Database Configuration Options	**Global Database Name**: Enter a name for the OracleAS Metadata Repository database. Append a domain name to the database name. This domain name for the global database name can be different from your network domain name. The domain name portion of the global database name has the following naming restrictions: ▪ Can contain only alphanumeric, underscore (_), minus (-), and pound (#) characters ▪ Must not be longer than 128 characters The database name portion of the global database name has the following naming restrictions: ▪ Can contain only alphanumeric, underscore (_), and pound (#) characters ▪ Must not be longer than eight characters ▪ Must not contain `PORT` or `HOST` in uppercase characters. If you want the name to contain "host" or "port", use lowercase characters. Example: `orcl.mydomain.com` **Note:** Be sure that you do not enter two or more periods together, for example, `orcl.mydomain.com`. The installer does not check for this, and this will lead to errors later during the installation process. **SID**: Enter the system identifier for the OracleAS Metadata Repository database. Typically this is the same as the global database name, but without the domain name. The SID must be unique across all databases on this system. SIDs have the following naming restrictions: ▪ Must contain alphanumeric characters only ▪ Must not be longer than eight characters ▪ Must not contain `PORT` or `HOST` in uppercase characters. If you want the name to contain "host" or "port", use lowercase characters. Example: `orcl` **Database Character Set**: Select the character set to use. See also Section 4.15, "Support for NE8ISO8859P10 and CEL8ISO8859P14 Characters Sets". **Database File Location**: Enter the full path to the parent directory for the data files directory. This parent directory must already exist, and you must have write permissions in this directory. The installer will create a subdirectory in this parent directory, and the subdirectory will have the same name as the SID. The data files will be placed in this subdirectory. Example: If you enter `/u02/oradata`, and the SID is `orcl`, then the data files will be located in `/u02/oradata/orcl`. Click **Next**.
2.	Specify Database Schema Passwords	Set the passwords for these privileged database schemas: SYS, SYSTEM, SYSMAN, and DBSNMP. You can set different passwords for each schema, or you can set the same password for all the schemas. Click **Next**.

4.30 Install Fragment: OCA Screens

If you select **Oracle Application Server Certificate Authority (OCA)** in the Select Configuration Options screen when you are installing an OracleAS Infrastructure, the installer displays the screens listed in Table 4–15.

Note that you cannot install more than one OCA against the same OracleAS Metadata Repository. When you are installing Oracle Identity Management components only against an existing OracleAS Metadata Repository, be sure that the metadata repository does not already have an instance of OCA configured against it.

Example: You install OracleAS Metadata Repository and Oracle Identity Management components including OCA on a computer. Then if you try to install additional Oracle Identity Management components (including OCA) on the same or different computer against the same OracleAS Metadata Repository, this installation would fail.

Table 4–15 OCA Screens

	Screen	Action
1.	Select OracleAS Metadata Repository	This screen appears only if you are configuring OCA **and** you are using an existing Oracle Internet Directory **and** you are using an existing OracleAS Metadata Repository. The Oracle Internet Directory must contain the registration for the OracleAS Metadata Repository that you want to use. Select the OracleAS Metadata Repository that you want OCA to use. Click **Next**.
2.	Specify OCA Distinguished Name	OCA uses the DN specified on this screen to populate the Issuer field of certificates that it issues. **Typical DN**: Use this section if your DN uses only the attributes listed in this section. You do not have to fill in all the attributes specified in this section. Only the `o` (organization) attribute is required. Note that the ' (single quote) character is not a valid character in any of the attributes. ■ **Common Name (CN)**: Enter the name that you want on the certificate. This name must be different from your hostname. Example: `John Doe`. ■ **Organizational Unit (OU)**: Enter the name of your division or department. Example: `Sales`. ■ **Organization (O)***: Enter the name of your company or organization. Example: `Oracle Corporation`. ■ **Country (C)**: Select your country from the drop-down list. **Custom DN**: If your DN uses attributes not listed in the Typical DN section, specify your DN in this section. Click **Next**.
3.	Select OCA Key Length	**Key Length (bits)**: Select the key length used in RSA algorithm to sign all certificates issued by OCA. Oracle recommends that you use at least a 2048-bit key length. Longer key lengths provide greater security, but require more time to issue each new certificate. Click **Next**.

Table 4–15 (Cont.) OCA Screens

	Screen	Action
4.	Specify OCA Administrator's Password	**Administrator's Password** and **Confirm Password**: Specify and confirm the password for the OCA administrator. The password has the following restrictions: ■ It must contain at least eight characters. ■ It must contain at least one alphabetic character. ■ It must contain at least one non-alphabetic character (for example, a number). ■ Its first character cannot be a number. You need this password to manage OCA. This password is also used by the OCA Configuration Assistant. You can change the password after installation using the `ocactl` command. See the OCA Online Help for details. Click **Next**.

5

Configuring Oracle Internet Directory for Oracle Application Server Installation Privileges

When you install certain infrastructure components, the installer prompts you for a username to log in to Oracle Internet Directory. For the installation to complete successfully, this user must belong to certain groups in Oracle Internet Directory. The groups that are required depend on what you are installing.

By putting users into groups, you allow other users to perform installations. Users do not have to log in as the `cn=orcladmin` superuser to perform the installations.

This chapter contains the following topics:

- Section 5.1, "Default Users in Oracle Internet Directory"
- Section 5.2, "Groups in Oracle Internet Directory"
- Section 5.3, "Groups Required to Configure or Deinstall Components"
- Section 5.4, "Groups Required to Install Middle Tiers"
- Section 5.5, "Groups Required to Install Additional Metadata Repositories"
- Section 5.6, "Example of Installation with Different Users"
- Section 5.7, "How to Create Users in Oracle Internet Directory"
- Section 5.8, "How to Add Users to Groups in Oracle Internet Directory"
- Section 5.9, "Contents of a New Oracle Internet Directory"
- Section 5.10, "On the Specify Login for Oracle Internet Directory Screen, What Username and Realm Do I Enter?"

5.1 Default Users in Oracle Internet Directory

When you install Oracle Internet Directory, it has two users: `cn=orcladmin` and `orcladmin`:

- `cn=orcladmin` is the Oracle Internet Directory superuser. This user has all the privileges to perform all tasks in Oracle Internet Directory.

  The initial password for `cn=orcladmin` is the same as the password for the ias_admin user for the Oracle Application Server instance. You specified this password during installation.

  `cn=orcladmin` is the owner of the objects created in the same installation session. For example, if you installed Oracle Internet Directory, OracleAS Metadata

Repository, and Oracle Delegated Administration Services, the `cn=orcladmin` user is created and becomes a member of the Repository Owners group and the DAS Component Owners group. `cn=orcladmin` also becomes a member of the iAS Admins group.

Note that you cannot log in to Oracle Internet Directory as the superuser (`cn=orcladmin`) using Oracle Delegated Administration Services. To log in as `cn=orcladmin`, you must use the Oracle Directory Manager.

- The `orcladmin` user is also created when you install Oracle Internet Directory. The DN for this user is: `cn=orcladmin,cn=users,<default realm DN>`.

  The initial password for `orcladmin` is the same as the password for the ias_admin user for the Oracle Application Server instance. You specified this password during installation.

  You can log in to Oracle Internet Directory as `orcladmin` using Oracle Delegated Administration Services to manage other Oracle Internet Directory users. You can do this because `orcladmin` is a valid OracleAS Single Sign-On user.

For more information on the `cn=orcladmin` and `orcladmin` users, see the *Oracle Internet Directory Administrator's Guide*.

5.2 Groups in Oracle Internet Directory

Groups in Oracle Internet Directory can be classified into these categories:

- Section 5.2.1, ""Global" Groups"
- Section 5.2.2, "Groups for Each Metadata Repository"
- Section 5.2.3, "Groups for Each Component"

5.2.1 "Global" Groups

Table 5–1 describes the groups that affect all Oracle Application Server instances and components registered with Oracle Internet Directory.

Table 5–1 "Global" Groups

Group	Description
IAS Admins DN: cn=IASAdmins, cn=groups, cn=OracleContext	IAS Admins have the following privileges: ▪ Install and register new metadata repositories. IAS Admins have no privileges to manage existing repositories already registered with Oracle Internet Directory. ▪ Install middle tiers.
Trusted Application Admins DN: cn=Trusted Application Admins, cn=groups, cn=OracleContext	To install Oracle Identity Management, OracleAS Portal, or OracleAS Wireless components, you must belong to several groups, one of which is the Trusted Application Admins group. Table 5–4 lists the required groups for each component.
IAS & User Management Application Admins DN: cn=IAS & User Mgmt Application Admins, cn=groups, cn=OracleContext	To install OracleAS Portal or OracleAS Wireless, you must belong to several groups, one of which is the IAS & User Management Application Admins group. Table 5–4 lists the required groups for each component.

5.2.2 Groups for Each Metadata Repository

Each metadata repository registered with Oracle Internet Directory has its own groups, as described in Table 5–2. This enables you to assign different owners and users for each repository.

Table 5–2 Groups Associated with Each Metadata Repository Registered with Oracle Internet Directory

Group	Description
Repository Owners DN: cn=Repository Owners, orclReferenceName=*dbName*, cn=IAS Infrastructure Databases, cn=IAS, cn=Products, cn=OracleContext	The user who installs the metadata repository becomes a member of this group. Repository Owners have the following privileges: ▪ Add/remove users to/from this group. ▪ De-register this repository. ▪ Add/remove users to/from the Mid-Tier Admins group for this repository. ▪ Add/remove middle-tier instances to/from this repository. ▪ All privileges of the Mid-Tier Administrators group.
Mid-Tier Administrators DN: cn=Repository Mid-tiers, orclReferenceName=*dbName*, cn=IAS Infrastructure Databases, cn=IAS, cn=Products, cn=OracleContext	Mid-Tier Administrators have the following privileges: ▪ Add/remove middle-tier instances from the Associated Middle Tiers group for this repository. This is required to install a middle tier or to configure a middle-tier component to use a different repository. ▪ Access metadata for the repository database object.
Associated Middle Tiers DN: cn=Associated Mid-tiers, orclReferenceName=*dbName*, cn=IAS Infrastructure Databases, cn=IAS, cn=Products, cn=OracleContext	Members of this group are middle-tier instances associated with this metadata repository. The middle-tier instances are added to this group during installation. You do not have to add the instances manually to this group. Members of this group have the following privilege: ▪ Access metadata for the repository database object and its schemas.

5.2.3 Groups for Each Component

Oracle Application Server components also have groups in Oracle Internet Directory. Each component has a Component Owners group and an Associated Middle Tiers group, as described in Table 5–3.

Table 5–3 Groups Associated with Each Component

Group	Description
Component Owners DN: cn=Component Owners, orclApplicationCommonName=*componentCommonName*, cn=*componentName*, cn=Products, cn=OracleContext	Component Owners have the following privileges: ▪ Add/remove owners for this component. ▪ De-register this component. ▪ Associate additional middle tiers with this component.
Associated Middle Tiers DN: cn=Associated Mid-tiers, orclApplicationCommonName=*componentCommonName*, cn=*componentName*, cn=Products, cn=OracleContext	Members of this group are middle-tier instances.

Figure 5–6 shows these groups for the Oracle Delegated Administration Services component.

5.3 Groups Required to Configure or Deinstall Components

Table 5–4 shows the groups that a user needs to belong to in order to configure or deinstall Oracle Application Server components.

The user who installs and configures the components becomes the owner of the components.

Table 5–4 Oracle Internet Directory Groups Required to Configure Components

To Configure This Component	User Must Be a Member of ALL Listed Groups:
Infrastructure Components	
OracleAS Metadata Repository	To register OracleAS Metadata Repository against Oracle Internet Directory, you must log in to Oracle Internet Directory as a user who belongs to the iAS Admins group.
Oracle Internet Directory	In OracleAS Cluster (Identity Management) environments, to install subsequent Oracle Internet Directory instances after the first one, you must be the Oracle Internet Directory superuser (`cn=orcladmin`).
Oracle Delegated Administration Services	▪ Trusted Application Admins ▪ iAS Admins ▪ Mid-Tier Admins group for the metadata repository used by OracleAS Single Sign-On If you are unsure which metadata repository is used by OracleAS Single Sign-On, see "To Determine the Metadata Repository Used by OracleAS Single Sign-On" on page 5-6. ▪ Component Owners for the Oracle Delegated Administration Services component **Note:** This is required only if you are installing multiple instances of Oracle Delegated Administration Services. When you are installing the second and subsequent instances, then you need to belong to the Component Owners group. You do not need to be a member when you install the first Oracle Delegated Administration Services instance. See Section 5.8.1, "Using Oracle Directory Manager to Add Users to Groups" for steps on how to add users to groups.
OracleAS Single Sign-On	You must install OracleAS Single Sign-On as the superuser (`cn=orcladmin`).
Oracle Directory Integration Platform	▪ iAS Admins ▪ Trusted Application Admins ▪ Admin for Oracle Directory Integration Platform, which is identified by "`cn=dipadmingrp,cn=odi,cn=oracle internet directory`" ▪ Mid-Tier Admins group for the metadata repository used by OracleAS Single Sign-On. If you are unsure which metadata repository is used by OracleAS Single Sign-On, see "To Determine the Metadata Repository Used by OracleAS Single Sign-On" on page 5-6.
OCA, configured against an existing OracleAS Metadata Repository	▪ Trusted Application Admins ▪ iAS Admins ▪ Repository Owners group for the existing metadata repository

Table 5–4 (Cont.) Oracle Internet Directory Groups Required to Configure Components

To Configure This Component	User Must Be a Member of ALL Listed Groups:
OCA, configured against a new OracleAS Metadata Repository (that is, you are installing and configuring OCA and OracleAS Metadata Repository in the same installation session)	▪ Trusted Application Admins ▪ iAS Admins
J2EE and Web Cache Middle-tier Features	
Oracle Identity Management Access only	▪ iAS Admins
Oracle Identity Management Access and Farm Repository (Database-Based or File-Based)	▪ iAS Admins ▪ Mid-Tier Admins or Repository Owners group for the metadata repository
Portal and Wireless, and Business Intelligence and Forms Middle-tier Components	
OracleAS Portal	▪ Trusted Application Admins ▪ IAS & User Management Application Admins ▪ iAS Admins ▪ Mid-Tier Admins or Repository Owners group for the metadata repository ▪ Component Owners group for the OracleAS Portal component **Note:** This group is applicable only when you are installing additional OracleAS Portal instances. It does not apply for the first OracleAS Portal installation. For subsequent OracleAS Portal installations, you can perform the installation as the same Oracle Internet Directory user who performed the first installation. If you want to allow a different Oracle Internet Directory user to install OracleAS Portal, you have to add this user to the Component Owners group for the Portal application entity.

Table 5–4 (Cont.) Oracle Internet Directory Groups Required to Configure Components

To Configure This Component	User Must Be a Member of ALL Listed Groups:
OracleAS Wireless	■ IAS & User Management Application Admins ■ iAS Admins ■ Mid-Tier Admins or Repository Owners group for the metadata repository ■ Component Owners group for the OracleAS Wireless component **Note:** This group is applicable only when you are installing additional OracleAS Wireless instances. It does not apply for the first OracleAS Wireless installation. For subsequent OracleAS Wireless installations, you can perform the installation as the same Oracle Internet Directory user who performed the first installation. If you want to allow a different Oracle Internet Directory user to install OracleAS Wireless, you have to add this user to the Component Owners group for the Wireless application entity. ■ In addition, the user must be one of the owners of the OracleAS Wireless application entity. To determine the name of the OracleAS Wireless application entity, run the following command from the first OracleAS Wireless installation: `prompt> $ORACLE_HOME/wireless/bin/getAppEntityName.sh` Then add the user as a component owner for this application entity. You can do this using the Deployment Delegation Console or the Oracle Directory Manager.
OracleAS Reports Services OracleAS Forms Services OracleAS Personalization OracleBI Discoverer	■ iAS Admins ■ Mid-Tier Admins or Repository Owners group for the metadata repository

To Determine the Metadata Repository Used by OracleAS Single Sign-On

1. Run the following command (all on one line):

```
prompt> ldapsearch -h oidhostname -p oidport -D cn=orcladmin -w password
 -b "orclapplicationcommonname=orasso_ssoserver,cn=sso,cn=products,
      cn=oraclecontext"
 -s base "objectclass=*" seealso
```

   Values you need to provide:

   oidhostname - name of the computer running Oracle Internet Directory. Example: `dbmachine.mydomain.com`.

   oidport - port number on which Oracle Internet Directory is listening. Example: `389`.

   password - password for the `cn=orcladmin` user.

2. If the command in the preceding step does not return the name of the metadata repository, then run the following commands:

   a. Run this command first to get the "orclreplicaid" value, which you need for the next command.

```
prompt> ldapsearch -h oidhostname -p oidport -D cn=orcladmin -w password
 -b "" -s base "objectclass=*" orclreplicaid
```

b. Then run this command.

```
prompt> ldapsearch -h oidhostname -p oidport -D cn=orcladmin -w password
 -b "orclreplicaid=value_from_previous_command,cn=replication
configuration"
 -s base "objectclass=*" seealso
```

This returns a "seealso" value in the format: `cn=Metadata repository DB Name,cn=oraclecontext`.

5.4 Groups Required to Install Middle Tiers

When you install middle tiers, the installer prompts you to log in to Oracle Internet Directory. Log in as a user who is a member of these groups:

- Section 5.4.1, "Groups Required to Install Against the Desired Metadata Repository"
- Section 5.4.2, "Groups Required to Install Middle-tier Components"

5.4.1 Groups Required to Install Against the Desired Metadata Repository

To install middle tiers against a metadata repository, the user must belong to these groups:

- IAS Admins group
- Mid-Tier Admins group for the metadata repository to be used with the middle tier. When the installer prompts for the OracleAS Metadata Repository to use with this middle tier, the installer displays only the metadata repositories for which the user is a mid-tier admin. For example, in Figure 5–2, userA can see only the repository for orcl.oracle.com, and userB can see only the repository for orcl1.oracle.com.

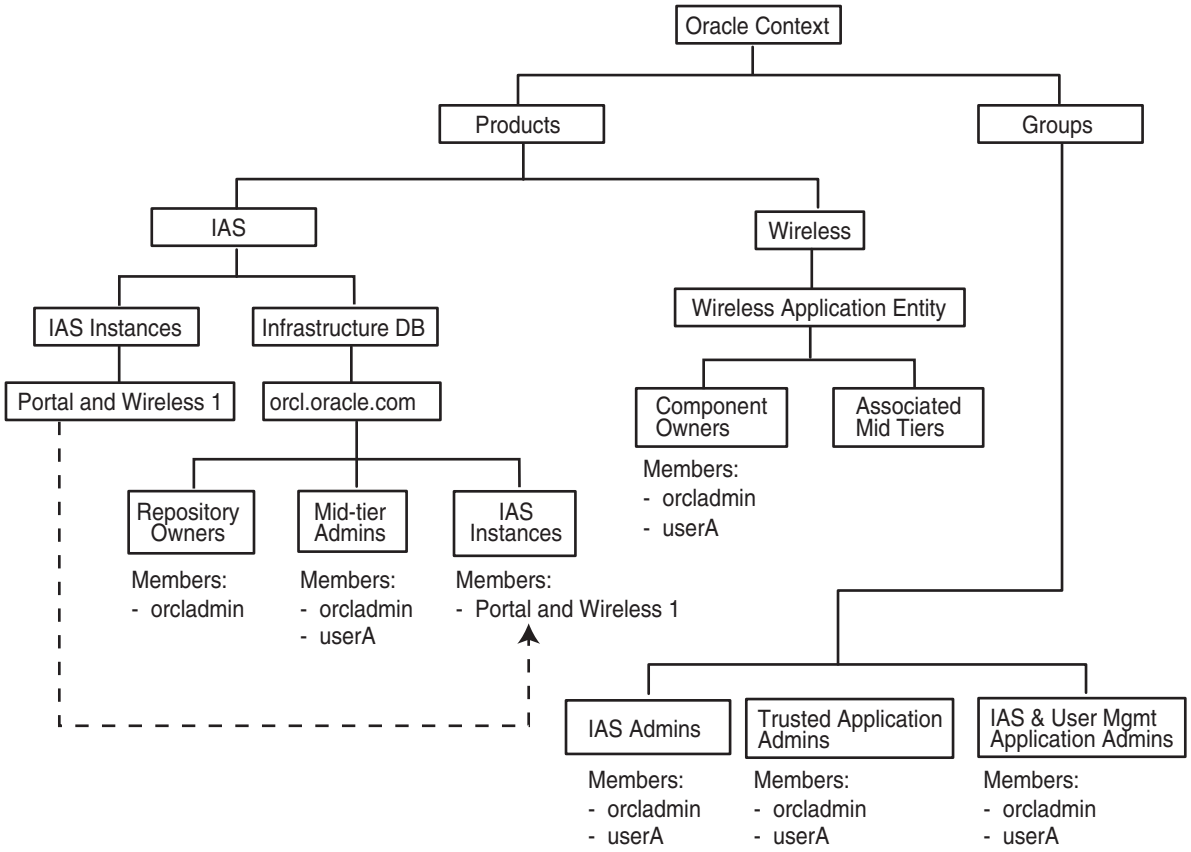
5.4.2 Groups Required to Install Middle-tier Components

To install middle-tier components, such as OracleAS Portal and OracleAS Wireless, the user must belong to additional groups. See Table 5–4 for a list of components and required groups.

5.4.3 Example

Figure 5–1 shows an Oracle Internet Directory with one metadata repository and one middle-tier instance. userA can install middle tiers against the orcl metadata repository because userA belongs to the Mid-Tier Admins and the IAS Admins groups. userA can also install middle-tier components because userA belongs to the Trusted Application Admins group, the IAS & User Management Application Admins group, and the Component Owners group for Wireless.

Figure 5–1 Contents of Oracle Internet Directory with One Infrastructure and One Middle Tier



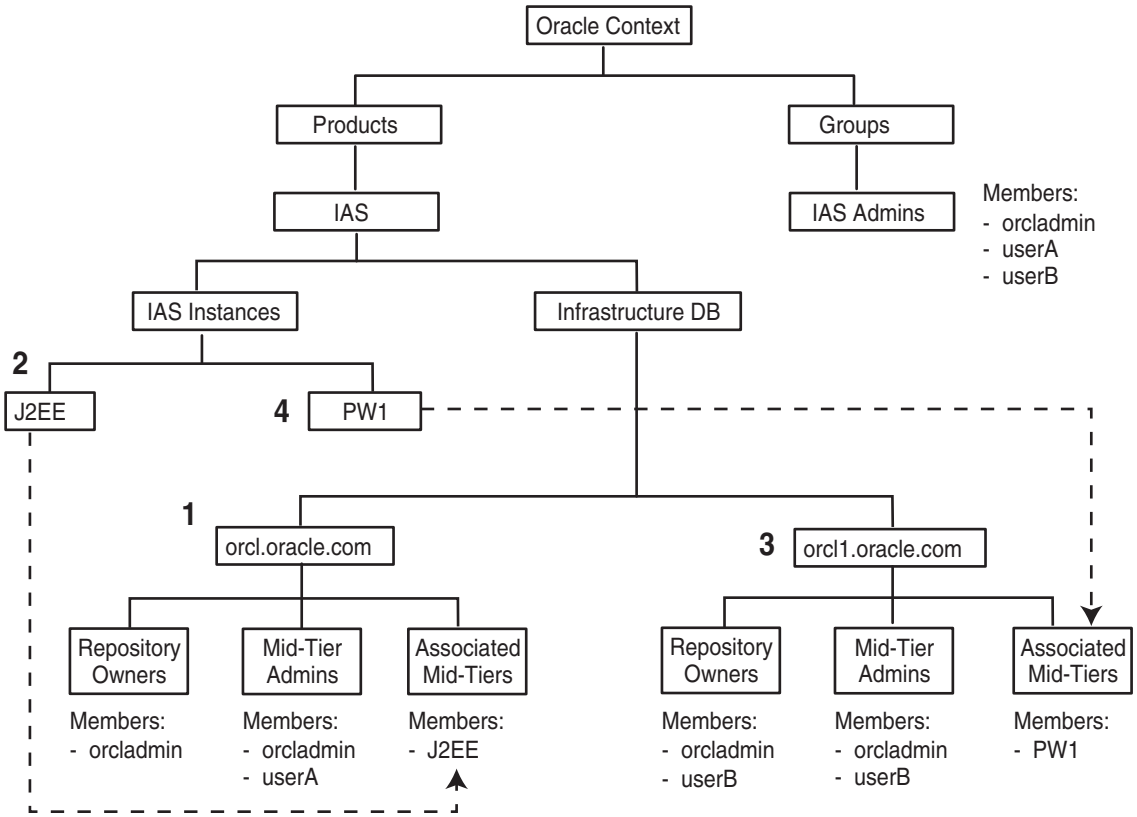
5.5 Groups Required to Install Additional Metadata Repositories

To install additional metadata repositories, a user must be a member of the IAS Admins group. After installation, the user then becomes a member of the Repository Owners group for that metadata repository.

5.6 Example of Installation with Different Users

Figure 5–2 shows an Oracle Internet Directory with two metadata repositories and two middle tiers installed by different users.

Figure 5–2 Oracle Internet Directory with Two Metadata Repositories and Two Middle Tiers



The numbers in the figure correspond to these steps:

1. Install OracleAS Infrastructure (including Oracle Internet Directory and OracleAS Metadata Repository)

This first installation creates an Oracle Internet Directory and a metadata repository.

The installer registers the metadata repository with Oracle Internet Directory by creating the "orcl.oracle.com" entry.

The orcladmin user becomes a member of the Repository Owners group and the Mid-Tier Admins group for this repository.

2. Install J2EE and Web Cache Middle Tier

userA was added to the following groups:

- Mid-Tier Admins group of "orcl.oracle.com"

  This enables userA to use the "orcl.oracle.com" repository for this middle tier. Note that this group is required only if you install the J2EE and Web Cache middle tier with the OracleAS Database-Based Cluster option. If you install the middle tier without this option, userA does not need to belong to this Mid-Tier Admins group.

- iAS Admins group

The installer registers this middle tier with Oracle Internet Directory by creating the "J2EE" entry. (The "J2EE" is the name of the middle-tier instance, specified by userA.)

The middle tier becomes a member of the Associated Mid-Tiers group for "orcl.oracle.com".

3. Install OracleAS Infrastructure (OracleAS Metadata Repository only)

userB was added to the iAS Admins group so that userB can perform this installation. See Section 5.5, "Groups Required to Install Additional Metadata Repositories".

The installer registers this new repository with Oracle Internet Directory by creating the "orcl1.oracle.com" entry.

userB becomes a member of the Repository Owners group and the Mid-Tier Admins group for the new repository.

4. Install Portal and Wireless Middle Tier

userB was added to these groups:

- Mid-Tier Admins group of "orcl1.oracle.com", so that userB can use the repository for this middle tier
- Trusted Application Admins, required for installing OracleAS Portal
- IAS & User Management Application Admins, required for installing OracleAS Portal and OracleAS Wireless
- iAS Admins, required for installing OracleAS Portal and OracleAS Wireless

The installer registers this middle tier with Oracle Internet Directory by creating the "PW1" entry.

The middle tier becomes a member of the Associated Mid-Tiers group for "orcl1.oracle.com".

5.7 How to Create Users in Oracle Internet Directory

You can create users in Oracle Internet Directory using the Self-Service Console, which is part of the Oracle Delegated Administration Services. See the *Oracle Internet Directory Administrator's Guide* for details.

> **Note:** You **cannot** connect to Oracle Internet Directory as the `cn=orcladmin` superuser using the Oracle Delegated Administration Services consoles. To connect to Oracle Internet Directory as the superuser, use Oracle Directory Manager.

5.8 How to Add Users to Groups in Oracle Internet Directory

To add users to groups in Oracle Internet Directory, you can use these tools:

- Oracle Directory Manager is a Java-based tool for managing Oracle Internet Directory.
- Oracle Delegated Administration Services is a Web-based tool intended for end-users to perform tasks such as changing their passwords and editing their personal information. If users have the proper privileges, they can also use this tool to create groups and users.

> **Note:** You cannot log in to Oracle Internet Directory as the `cn=orcladmin` superuser using Oracle Delegated Administration Services. In cases where you have to log in as the superuser to add users to groups (or to perform other Oracle Internet Directory-related tasks), you have to use Oracle Directory Manager.

5.8.1 Using Oracle Directory Manager to Add Users to Groups

When you have to log in as the `cn=orcladmin` superuser to add users to groups, you have to use Oracle Directory Manager, instead of Oracle Delegated Administration Services.

To add users using Oracle Directory Manager:

1. Start up Oracle Directory Manager. ORACLE_HOME refers to the home directory where Oracle Internet Directory is installed.

   ```
   prompt> cd $ORACLE_HOME/bin
   prompt> ./oidadmin
   ```

2. In the Oracle Directory Manager Connect screen, enter the connect information for Oracle Internet Directory:
   - **User**: Enter `cn=orcladmin`.
   - **Password**: Enter the password for `cn=orcladmin`.
   - **Server** and **Port**: Click the icon at the right of the field to enter the name of the computer running Oracle Internet Directory and the port number on which Oracle Internet Directory is listening.
   - Click **Login**.
3. On the left side, navigate to the group to which you want to add users. Select the group on the left side to display its attributes on the right side.

   To navigate to "global" groups, see Section 5.8.1.1, "Navigating to "Global" Groups".

   To navigate to metadata repository groups, see Section 5.8.1.2, "Navigating to Metadata Repository Groups".

   To navigate to component groups, see Section 5.8.1.3, "Navigating to Component Groups".
4. Add new users to the group by adding the DNs of the users to the `uniquemember` attribute.

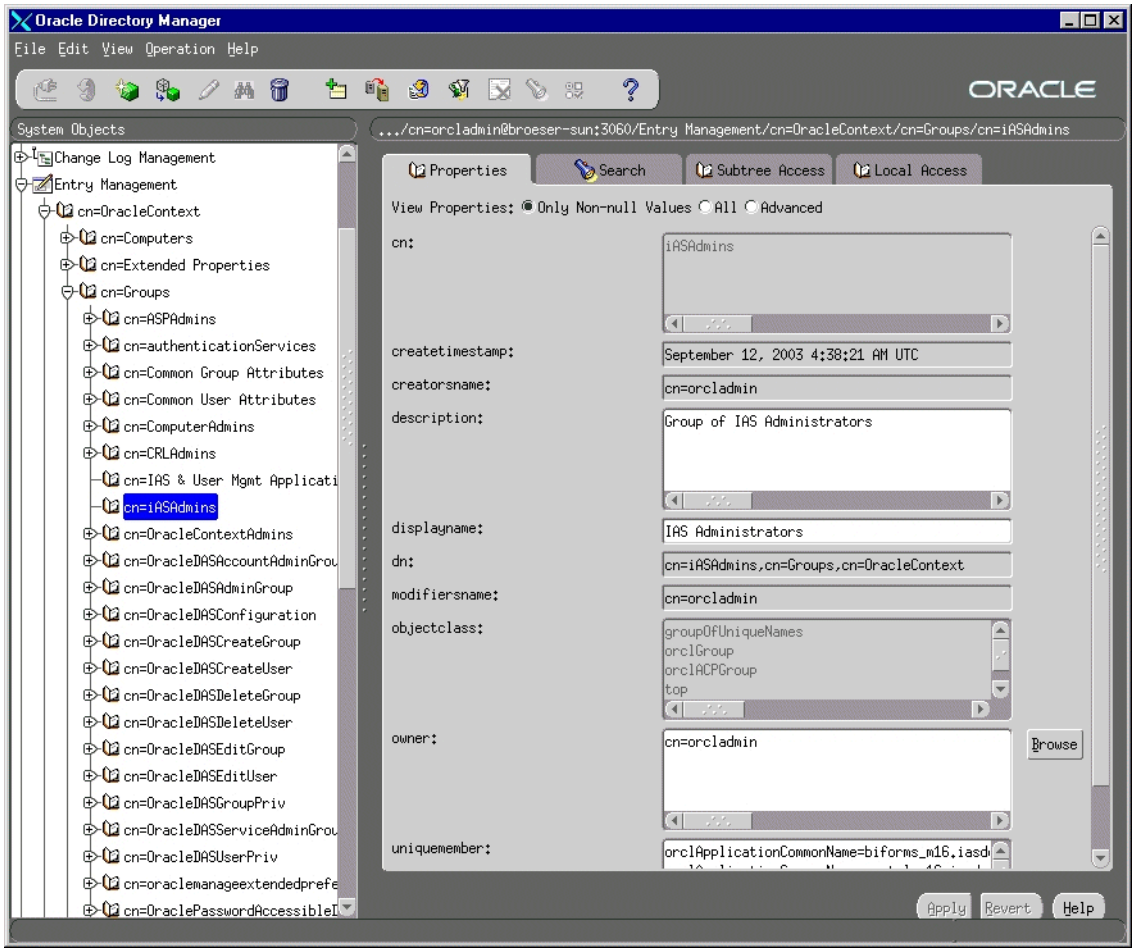
5.8.1.1 Navigating to "Global" Groups

The "global" groups are listed in Table 5–1.

The general navigation path is as follows. See Figure 5–3 for a screenshot.

1. Expand the top-level entry, "Oracle Internet Directory Servers".
2. Expand the specific Oracle Internet Directory.
3. Expand the following entries: **Entry Management** > **cn=OracleContext** > **cn=Groups**.
4. Click the group to which you want to add users. Figure 5–3 shows Oracle Directory Manager with the iASAdmins group selected.

Figure 5–3 Using Oracle Directory Manager to Add Users to "Global" Groups



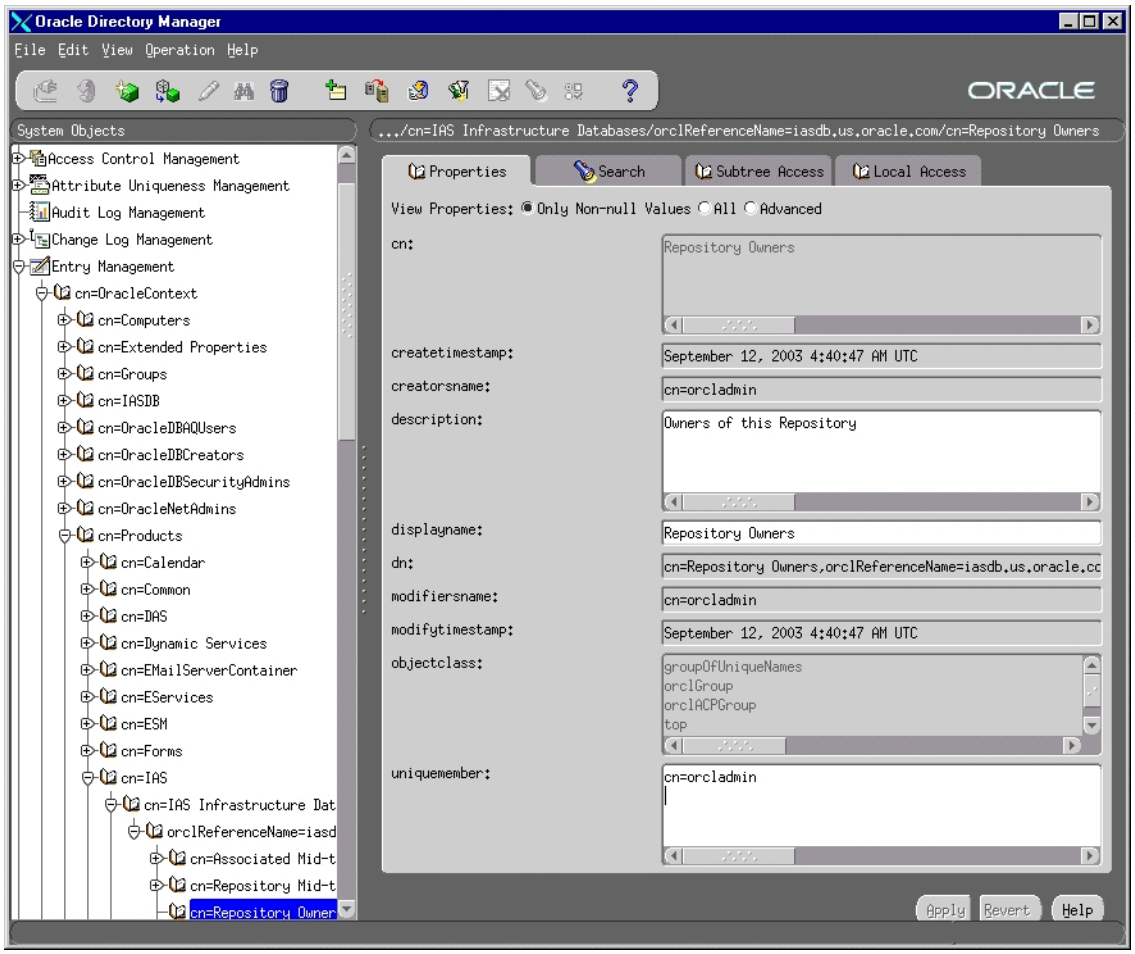
5.8.1.2 Navigating to Metadata Repository Groups

The metadata repository groups are listed in Table 5–2.

The general navigation path is as follows. See Figure 5–4 for a screenshot.

1. Expand the top-level entry, "Oracle Internet Directory Servers".
2. Expand the specific Oracle Internet Directory.
3. Expand the following entries: **Entry Management** > **cn=OracleContext** > **cn=Products** > **cn=IAS** > **cn=IAS Infrastructure Databases** > **orclReferenceName=***dbName*, where *dbName* is the name of the OracleAS Metadata Repository database.
4. Click the group to which you want to add users. Figure 5–4 shows Oracle Directory Manager with the Repository Owners group for the orcl.us.oracle.com database selected.

Figure 5–4 Using Oracle Directory Manager to Add Users to Metadata Repository Groups



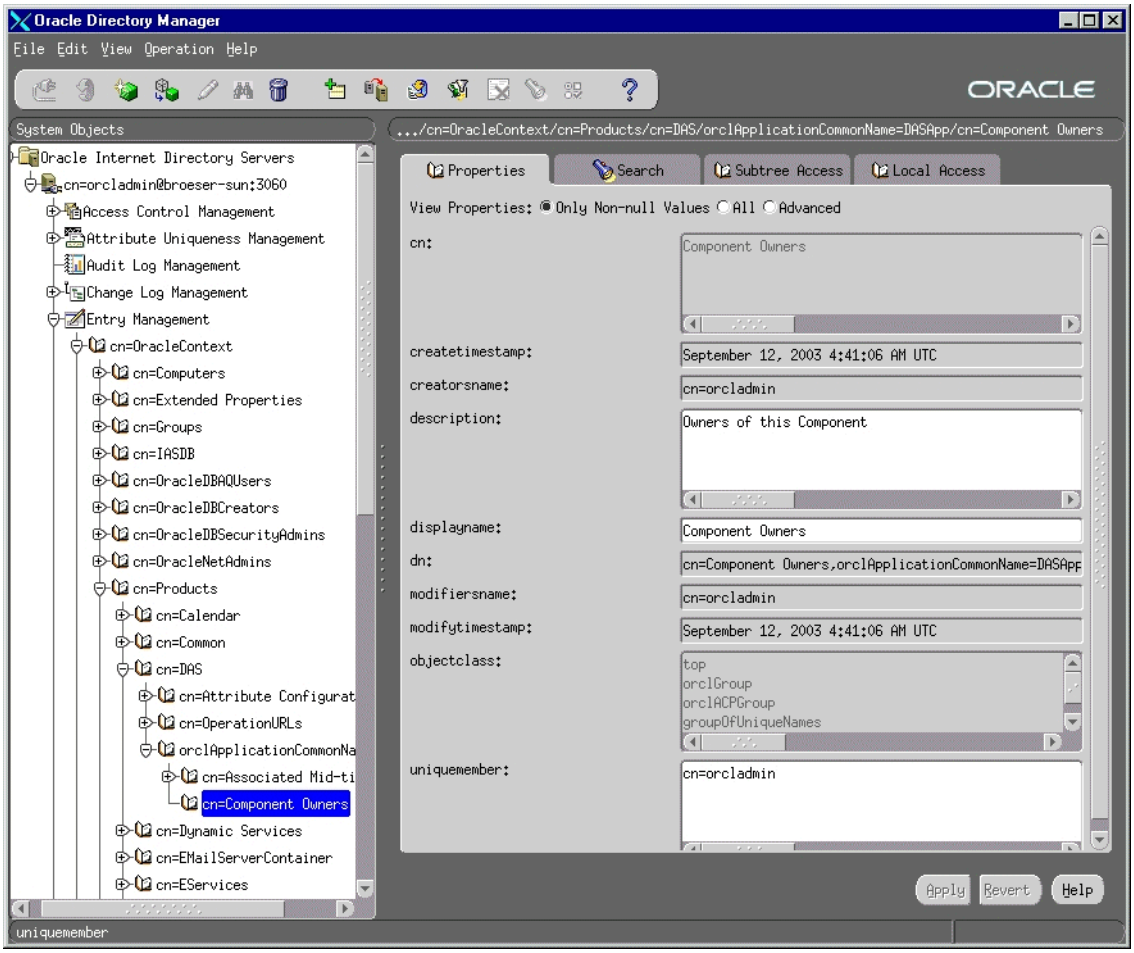
5.8.1.3 Navigating to Component Groups

The component groups are listed in Table 5–3.

The general navigation path is as follows. See Figure 5–5 for a screenshot.

1. Expand the top-level entry, "Oracle Internet Directory Servers".
2. Expand the specific Oracle Internet Directory.
3. Expand the following entries: **Entry Management** > **cn=OracleContext** > **cn=Products**.
4. Expand the particular component (for example, **cn=DAS**) whose groups you want to add users to.
5. Expand **orclApplicationCommonName=***appName*, where *appName* is specific to the component and application server instance. If you have installed multiple instances of a component, you would see multiple instances of this entry.
6. Click the group to which you want to add users. Figure 5–5 shows Oracle Directory Manager with the Component Owners group for Oracle Delegated Administration Services selected.

Figure 5–5 Using Oracle Directory Manager to Add Users to the Component Users Group for the Oracle Delegated Administration Services Component



5.8.2 Using Deployment Delegation Console to Add Users to Groups

Using the Deployment Delegation Console, which is installed as part of Oracle Delegated Administration Services, you can add users to or remove users from the following groups:

- Repository Owners
- Mid-Tier Administrators
- Component Owners

Note: You can add users to these groups only if these groups have existing members other than the `cn=orcladmin` superuser. If the only member of these groups is the superuser, then you have to use Oracle Directory Manager to add users to these groups. See Section 5.8.1, "Using Oracle Directory Manager to Add Users to Groups".

To add users to these groups:

1. Ensure that the Oracle Delegated Administration Services and Oracle Internet Directory are running.
2. Display the Deployment Delegation Console page. The URL is:

   `http://hostname:port/oiddas/ui/oidinstallhome`

   hostname specifies the name of the computer where you installed Oracle Delegated Administration Services.

   port specifies the port on which Oracle HTTP Server is listening.
3. Click **Login**.
4. Enter a username and password to log in to Oracle Internet Directory, and click **Login**. The login user must have sufficient privileges to allow you to add users to the desired group:

To add users to this group:	Log in as a user who belongs to:
Repository Owners	the same Repository Owners group.
Mid-Tier Administrators	the Repository Owners group for the same repository.
Component Owners	the same Component Owners group.

5. Perform the steps to add the user to the desired group:

To add the user to the Repository Owners group	To add the user to the Mid-Tier Administrators group	To add the user to the Component Owners group
1. Click the **Repository** tab. This displays all the metadata repositories for which you are an owner. 2. Select the metadata repository to which you want to add a user, and click **Manage Owners**. 3. On the page that displays the current owners, click **Add**. 4. Enter the first few characters of the user's name in the **Search** field and click **Go**. If you leave the **Search** field empty and click **Go**, you would get a list of all users in Oracle Internet Directory. 5. Select the user that you want to add to the Repository Owners group and click **Select**. 6. Click **Submit** on the Manage Repository Owners page.	1. Click the **Repository** tab. This displays all the metadata repositories for which you are an owner. 2. Select the metadata repository to which you want to add a user, and click **Manage Administrators**. 3. On the page that displays the current administrators, click **Add**. 4. Enter the first few characters of the user's name in the **Search** field and click **Go**. If you leave the **Search** field empty and click **Go**, you would get a list of all users in Oracle Internet Directory. 5. Select the user that you want to add to the Mid-Tier Administrators group and click **Select**. 6. Click **Submit** on the Manage Administrators page.	1. Click the **Components** tab. This displays all the components for which you are an owner. 2. Select the component to which you want to add a user, and click **Manage Owners**. 3. On the page that displays the current component owners, click **Add**. 4. Enter the first few characters of the user's name in the **Search** field and click **Go**. If you leave the **Search** field empty and click **Go**, you would get a list of all users in Oracle Internet Directory. 5. Select the user that you want to add to the Component Owners group and click **Select**. 6. Click **Submit** on the Manage Component Owners page.

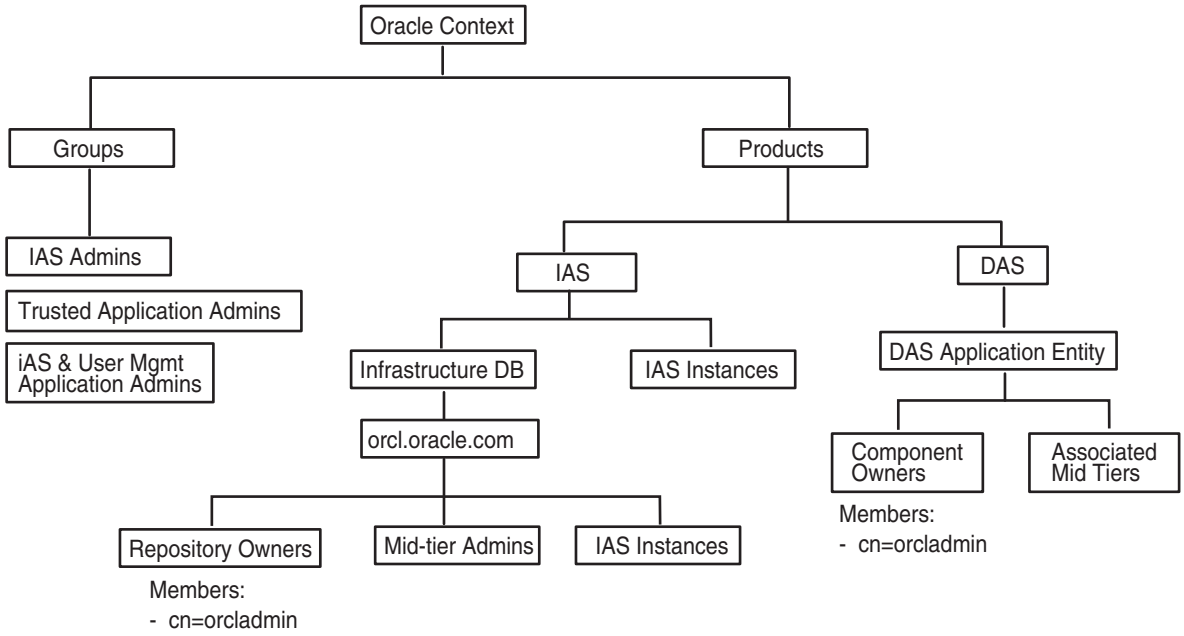
5.9 Contents of a New Oracle Internet Directory

When you install OracleAS Infrastructure with Oracle Internet Directory, OracleAS Metadata Repository, and Oracle Delegated Administration Services, the Oracle Internet Directory contains the following objects (Figure 5–6):

- "Global" groups as listed in Table 5–1
- The `cn=orcladmin` superuser
- The `orcladmin` user belonging to the default realm
- An entry for the metadata repository registered with the Oracle Internet Directory. This metadata repository is associated with the groups listed in Table 5–2. The `cn=orcladmin` superuser is a member of the Repository Owners group.
- An application entity entry for the Oracle Delegated Administration Services component. This component is associated with the groups listed in Table 5–3. The `cn=orcladmin` superuser is a member of the Component Owners group.

  To enable other users to install additional instances of Oracle Delegated Administration Services, log in as `cn=orcladmin` in Oracle Directory Manager and add the users to the Component Owners group. See Section 5.8.1, "Using Oracle Directory Manager to Add Users to Groups".

Figure 5–6 Contents of a New Oracle Internet Directory



5.10 On the Specify Login for Oracle Internet Directory Screen, What Username and Realm Do I Enter?

The installer displays the Specify Login for Oracle Internet Directory screen:

- when you are installing OracleAS Infrastructure and you are using an existing Oracle Internet Directory
- when you are installing a middle tier that requires an infrastructure.

This screen prompts you to enter a username and password to log in to Oracle Internet Directory.

Username

In the Username field, enter either the simple username or the user's DN.

Simple username example: `jdoe`

DN example: `cn=orcladmin`

The user must belong to specific groups for installing and configuring certain components. See Table 5–4 for details.

If you want to specify the superuser, enter `cn=orcladmin`, not just `orcladmin`.

Realm

The Realm field appears only if your Oracle Internet Directory contains more than one realm. The username that you enter is authenticated against the specified realm. If you are unsure what the realm name is, contact your Oracle Internet Directory administrator.

Example 1: in a hosted deployment, the realm name could be similar to the name of the hosted company: `XYZCorp`.

Example 2: within an enterprise, you could have separate realms for internal users and external users. The realm name for the external users could be `externalUsers`.

6

Installing Oracle Internet Directory in Replicated Mode

This chapter describes how to install Oracle Internet Directory in replicated mode, that is, how to install Oracle Internet Directory masters and replicas.

This chapter contains the following topics:

- Section 6.1, "Oracle Internet Directory Replication Overview"
- Section 6.2, "Requirements"
- Section 6.3, "Installation Order"
- Section 6.4, "Installing a Master Oracle Internet Directory"
- Section 6.5, "Installing an Oracle Internet Directory Replica"
- Section 6.6, "Accessing OracleAS Single Sign-On and Oracle Delegated Administration Services"

6.1 Oracle Internet Directory Replication Overview

To run Oracle Internet Directory in a replication environment means that you have more than one Oracle Internet Directory, each with its own OracleAS Metadata Repository. The Oracle Internet Directory instances synchronize the data in the metadata repositories so that the data in the repositories are "loosely consistent". This means that the data in the repositories are not guaranteed to be synchronized in "real time", but the data become identical within an acceptable time interval.

For More Information

This chapter provides information from an installation point of view. For in-depth information on replication, see the following guides:

- For information on Oracle Internet Directory replication concepts and administration, see the *Oracle Internet Directory Administrator's Guide*.
- For information on Oracle Internet Directory replication deployment scenarios, see the *Oracle Identity Management Infrastructure Administrator's Guide*.

Types of Replication

There are two types of replication. During installation, you select the type of replication that you want.

- Section 6.1.1, "Fan-Out Replication (LDAP Replication)"
- Section 6.1.2, "Multimaster Replication (Advanced Replication)"

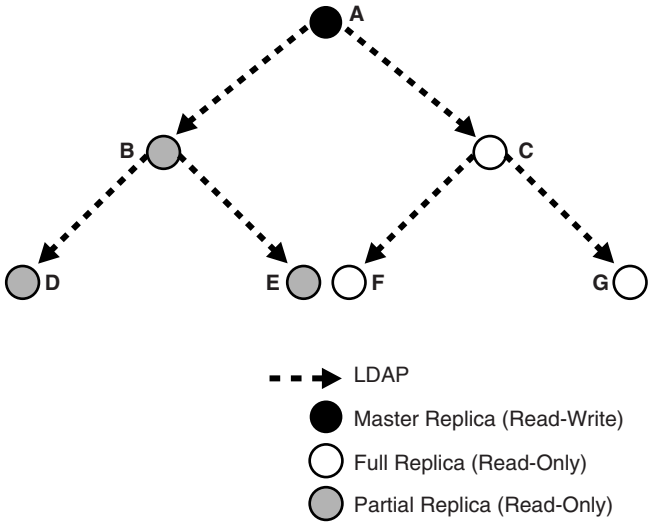
6.1.1 Fan-Out Replication (LDAP Replication)

In fan-out replication, one Oracle Internet Directory is the master, and the other Oracle Internet Directory instances are called the Oracle Internet Directory replicas.

In one-way fan-out replication, clients modify the data in the master Oracle Internet Directory only. The master then propagates the changes to the replicas. These replicas, in turn, can update other Oracle Internet Directory replicas.

In two-way fan-out replication, clients modify the data in the master Oracle Internet Directory and the replicas. Changes made to any node are propagated to the other nodes.

Figure 6–1 Example of One-Way Fan-Out Replication (LDAP Replication)



In fan-out replication, Oracle Internet Directory instances use the LDAP protocol to communicate with each other. The Select Oracle Internet Directory Replication Mode screen in the installer uses the term **LDAP Replication** to refer to fan-out replication.

The procedure for installing a master Oracle Internet Directory is the same as installing a "regular" (non-replicated) Oracle Internet Directory.

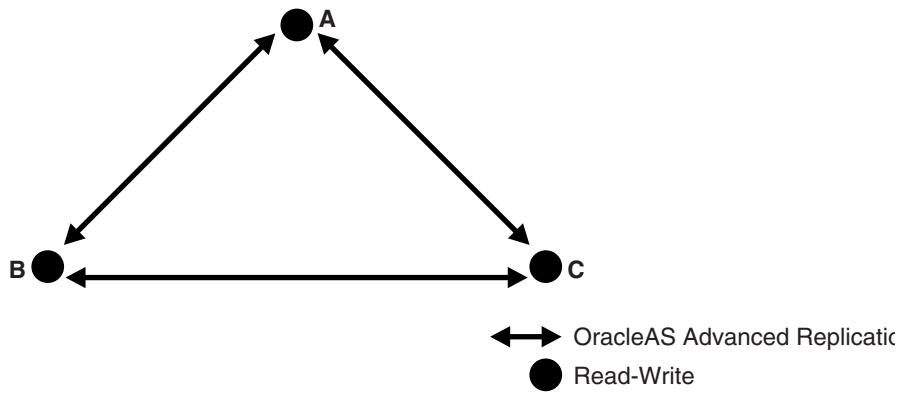
The procedure for installing replicas is different. When installing a replica, you must select the **High Availability and Replication** option in the Select Configuration Options screen, and you need to provide connect information to the master Oracle Internet Directory.

The Oracle Application Server instance that runs the Oracle Internet Directory (master or replica) can also run other Oracle Application Server components, such as the OracleAS Metadata Repository, OracleAS Single Sign-On, Oracle Delegated Administration Services, and/or Oracle Directory Integration Platform.

6.1.2 Multimaster Replication (Advanced Replication)

In multimaster replication, you have one or more master Oracle Internet Directory instances. You can also have other Oracle Internet Directory instances that are replicas. Clients can update data in any Oracle Internet Directory (master or replica). The Oracle Internet Directory instances propagate the changes among themselves.

Figure 6–2 Example of Multimaster Replication (Advanced Replication)



In multimaster replication, Oracle Internet Directory instances use the Oracle Database Advanced Replication protocol to communicate with each other. The Select Oracle Internet Directory Replication Mode screen in the installer uses the term **Advanced Replication** to refer to multimaster replication.

The procedure for installing a master Oracle Internet Directory is the same as installing a "regular" (non-replicated) Oracle Internet Directory.

The procedure for installing replicas is different. When installing a replica, you must select the **High Availability and Replication** option in the Select Configuration Options screen, and you need to provide connect information to the master Oracle Internet Directory.

The Oracle Application Server instance that runs the Oracle Internet Directory (master or replica) can also run other Oracle Application Server components, such as the OracleAS Metadata Repository, OracleAS Single Sign-On, Oracle Delegated Administration Services, and/or Oracle Directory Integration Platform.

6.2 Requirements

Check that you meet the following requirements for installing Oracle Internet Directory in replication mode:

- Section 6.2.1, "Database Requirements"
- Section 6.2.2, "Clock Synchronization"

6.2.1 Database Requirements

Each Oracle Internet Directory, whether master or replica, needs its own OracleAS Metadata Repository. You can install it with a new OracleAS Metadata Repository, or against an existing OracleAS Metadata Repository.

If installing against an existing OracleAS Metadata Repository, you can create an existing OracleAS Metadata Repository in two different ways:

- You can install it by selecting the **OracleAS Metadata Repository** option in the Select Installation Type screen.
- You can install the OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details on how to load the OracleAS Metadata Repository in an existing database.

If you are installing against an existing OracleAS Metadata Repository, the **OracleAS Metadata Repository must not be already registered with another Oracle Internet Directory**. If you specify an OracleAS Metadata Repository that is already registered with an Oracle Internet Directory, the installer assumes you are installing a high availability environment, and it does not display the replication options.

6.2.2 Clock Synchronization

Check that the clocks on the computers running the masters and replicas are within 250 seconds of each other.

6.3 Installation Order

To install Oracle Internet Directory in replicated mode, you need a master Oracle Internet Directory and one or more Oracle Internet Directory replicas. You install them in the following order:

1. Install the master Oracle Internet Directory first.
2. Install the Oracle Internet Directory replicas. The installer will prompt you to enter connect information for the master Oracle Internet Directory.

6.4 Installing a Master Oracle Internet Directory

The procedure for installing a master Oracle Internet Directory is the same as installing a "regular" (non-replicated) Oracle Internet Directory. You can install the master Oracle Internet Directory against an existing database, or you can install it with a new database.

Notes:

- In the Select Configuration Options screen, you must select **Oracle Internet Directory**. You can select other components to configure, as desired.
- Also in the Select Configuration Options screen, you do not need to select **High Availability and Replication**. Select this option only if you are installing this Oracle Application Server instance in a high availability configuration.
- If you select the **High Availability and Replication** option in Select Configuration Options screen, the installer displays the Select High Availability Option screen. In this, **do not** select the **Replication** option, because this option is for installing a replica Oracle Internet Directory, not a master Oracle Internet Directory.

You can use any of the procedures in Chapter 4, "Installing OracleAS Infrastructure" to install a master Oracle Internet Directory. Examples:

- To install a master Oracle Internet Directory with a new database, follow the procedure in Section 4.20, "Installing OracleAS Infrastructure".
- To install a master Oracle Internet Directory with an existing database, follow the procedure in Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)" or Section 4.25, "Installing Oracle Internet Directory Only".

You can also install a master Oracle Internet Directory in high availability environments. See Chapter 8, "Installing in High Availability Environments: OracleAS Cold Failover Cluster" and Chapter 9, "Installing in High Availability Environments: OracleAS Cluster (Identity Management)" for details.

6.5 Installing an Oracle Internet Directory Replica

You can install an Oracle Internet Directory replica against an existing database, or you can install it with a new database.

Contents of this section:

- Section 6.5.1, "Overview of Installing a Replica"
- Section 6.5.2, "Installing an Oracle Internet Directory Replica with a New Database"
- Section 6.5.3, "Installing an Oracle Internet Directory Replica against an Existing Database"

6.5.1 Overview of Installing a Replica

When installing an Oracle Internet Directory replica, remember the following:

- In the Select Configuration Options screen, you must select **Oracle Internet Directory** and **High Availability and Replication**.
- In the Select High Availability Option screen, select **Replication**.
- When the installer prompts you to enter connect information for the master Oracle Internet Directory, you need to connect as the Oracle Internet Directory superuser (`cn=orcladmin`). You need to know the password for the superuser.
- The master Oracle Internet Directory must not already contain a registration for a database with the same global database name or SID as the OracleAS Metadata Repository to be used for the replica.
- The OracleAS Metadata Repository for the replica cannot already be registered with any Oracle Internet Directory.

6.5.2 Installing an Oracle Internet Directory Replica with a New Database

Follow these steps to install an Oracle Internet Directory replica with a new database:

Table 6–1 Installing an Oracle Internet Directory Replica with a New Database

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ▪ In the Select a Product to Install screen, select **Oracle Application Server Infrastructure 10g**. ▪ In the Select Installation Type screen, select **Identity Management and Metadata Repository**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **High Availability and Replication**. The other options on this screen are optional: Select **Oracle Application Server Single Sign-On**, **Oracle Application Server Delegated Administration Services**, **Oracle Directory Integration Platform**, and/or **Oracle Application Server Certificate Authority (OCA)** if you need these components. Click **Next**.

Table 6–1 (Cont.) Installing an Oracle Internet Directory Replica with a New Database

	Screen	Action
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file in the provided field. Click **Next**.
4.	Select High Availability or Replication Option	This screen is required to install a replica. This screen appears only if you selected **High Availability and Replication** in the Select Configuration Options screen. Select **Replication**, and click **Next**.
5.	Select Oracle Internet Directory Replication Mode	Select **One-way LDAP Replication** if you want to use fan-out replication in one direction. Select **Two-way LDAP Replication** if you want to use fan-out replication in both directions. Select **Advanced Replication** if you want multimaster replication. Click **Next**.
6.	Specify Oracle Internet Directory Master Node	**Hostname**: Enter the name of the computer running the master Oracle Internet Directory. **Port**: Enter the port at which the master Oracle Internet Directory is listening. Do not select **Use only SSL connections with this Oracle Internet Directory**. If you want Oracle Internet Directory to run in SSL-only mode, you can make this configuration change after installation. See the *Oracle Application Server Administrator's Guide* for details. Click **Next**.
7.	Specify Master Oracle Internet Directory Login	**Username**: Enter `cn=orcladmin` because you have to connect to the master Oracle Internet Directory as the superuser. **Password**: Enter the password for the superuser. Click **Next**.
8.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
9.	OCA screens	If you selected **Oracle Application Server Certificate Authority (OCA)** in the Select Configuration Options screen, the installer displays screens for configuring OCA. See Section 4.30, "Install Fragment: OCA Screens" for details.

Table 6–1 (Cont.) Installing an Oracle Internet Directory Replica with a New Database

	Screen	Action
10.	Specify Database Configuration Options	**Global Database Name**: Enter a name for the OracleAS Metadata Repository database. Append the domain name of your computer to the database name. Example: `orcl.mydomain.com` **Note**: Ensure that the master Oracle Internet Directory does not already contain a registration for a database with the same global database name or SID. (The installer checks this for you.) **SID**: Enter the system identifier for the OracleAS Metadata Repository database. Typically this is the same as the global database name, but without the domain name. The SID must be unique across all databases. The SID cannot be longer than eight characters. Example: `orcl` **Select Database Character Set**: Select the character set to use. **Specify Database File Location**: Enter the full path to the parent directory for the data files directory. This parent directory must already exist, and you must have write permissions in this directory. The installer will create a subdirectory in this parent directory, and the subdirectory will have the same name as the SID. The data files will be placed in this subdirectory. Example: If you enter `/u02/oradata`, and the SID is `orcl`, then the data files will be located in `/u02/oradata/orcl`. Click **Next**.
11.	Specify Database Schema Passwords	Set the passwords for these privileged database schemas: SYS, SYSTEM, SYSMAN, and DBSNMP. You can set different passwords for each schema, or you can set the same password for all the schemas. See Section 4.14, "Restrictions on the Passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP Users" for rules on setting passwords for these accounts. Click **Next**.
12.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `infra` **ias_admin Password** and **Confirm Password**: Enter and confirm the password for the ias_admin user. This is the administrative user for this infrastructure instance. This password will also become the password for the following users: ▪ the Oracle Internet Directory superuser ("`cn=orcladmin`") ▪ the Oracle Internet Directory database user ("`ods`") ▪ the replication DN, which is the identity used by the replication server. The DN is: "`cn=replication dn, orclreplicaid=`*replica_ID*`, cn=replication configuration`", where *replica_ID* is the replica ID of the Oracle Internet Directory being installed. See Section 3.6, "The ias_admin User and Restrictions on its Password" for password requirements. Example: `welcome99` Click **Next**.
13.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

6.5.3 Installing an Oracle Internet Directory Replica against an Existing Database

Follow these steps to install an Oracle Internet Directory replica against an existing database.

Table 6–2 Installing an Oracle Internet Directory Replica against an Existing Database

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ■ In the Select a Product to Install screen, select **Oracle Application Server Infrastructure 10g**. ■ In the Select Installation Type screen, select **Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **High Availability and Replication**. The other options on this screen are optional: Select **Oracle Application Server Single Sign-On**, **Oracle Application Server Delegated Administration Services**, **Oracle Directory Integration Platform**, and/or **Oracle Application Server Certificate Authority (OCA)** if you need these components. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file in the provided field. Click **Next**.
4.	Specify Repository	Enter information for the OracleAS Metadata Repository that you want to use for the replica. **Notes**: ■ This OracleAS Metadata Repository cannot already be registered with any Oracle Internet Directory. ■ The master Oracle Internet Directory, which you will specify in step 7., must not already contain a registration for a database with the same global database name or SID as this OracleAS Metadata Repository. (**The installer does not check this for you.**) **Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the name of the computer where the database is running, and the port number at which it is listening. Use the format: *`host:port`*. **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Select High Availability or Replication Option	This screen is required to install a replica. If you do not see this screen, return to the Select Configuration Options screen and ensure you selected **High Availability and Replication**. Select **Replication**. Click **Next**.

Table 6–2 (Cont.) Installing an Oracle Internet Directory Replica against an Existing Database

	Screen	Action
6.	Select Oracle Internet Directory Replication Mode	Select **One-way LDAP Replication** if you want to use fan-out replication in one direction. Select **Two-way LDAP Replication** if you want to use fan-out replication in one direction. Select **Advanced Replication** if you want multimaster replication. Click **Next**.
7.	Specify Oracle Internet Directory Master Node	**Hostname**: Enter the name of the computer running the master Oracle Internet Directory. **Port**: Enter the port at which the master Oracle Internet Directory is listening. Do not select **Use only SSL connections with this Oracle Internet Directory**. If you want Oracle Internet Directory to run in SSL-only mode, you can make this configuration change after installation. See the *Oracle Application Server Administrator's Guide* for details. Click **Next**.
8.	Specify Master Oracle Internet Directory Login	**Username**: Enter `cn=orcladmin` because you have to connect to the master Oracle Internet Directory as the superuser. **Password**: Enter the password for the superuser. Click **Next**.
9.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
10.	OCA screens	If you selected **Oracle Application Server Certificate Authority (OCA)** in the Select Configuration Options screen, the installer displays screens for configuring OCA. See Section 4.30, "Install Fragment: OCA Screens" for details.
11.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `id_mgmt` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. This password will also become the password for the following users: ▪ the Oracle Internet Directory superuser ("`cn=orcladmin`") ▪ the Oracle Internet Directory database user ("`ods`") ▪ the replication DN, which is the identity used by the replication server. The DN is: "`cn=replication dn, orclreplicaid=`*replica_ID*`, cn=replication configuration`", where *replica_ID* is the replica ID of the Oracle Internet Directory being installed. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
12.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

6.6 Accessing OracleAS Single Sign-On and Oracle Delegated Administration Services

To access OracleAS Single Sign-On or Oracle Delegated Administration Services on the replica node, you have to use the password for the `orcladmin` user on the master Oracle Internet Directory, not the replica Oracle Internet Directory.

Example:

1. Enter the URL for OracleAS Single Sign-On or Oracle Delegated Administration Services in your browser:

   For OracleAS Single Sign-On, the URL is: `http://`*`host`*`:`*`port`*`/pls/orasso`.

   For Oracle Delegated Administration Services, the URL is: `http://`*`host`*`:`*`port`*`/oiddas`.

   host specifies the name of the computer where you installed the Oracle Internet Directory replica.

   port specifies the port number on which Oracle HTTP Server is listening.

2. To log in, enter `orcladmin` as the user name and the password you entered when you installed the **master Oracle Internet Directory**. If you enter the password for the replica Oracle Internet Directory, the login will not succeed.

7

Installing in High Availability Environments: Overview

This chapter provides an overview of the high availability configurations supported by Oracle Application Server. Subsequent chapters provide the details. This chapter also lists the common requirements.

This chapter contains the following topics:

- Section 7.1, "Overview of High Availability Configurations"
- Section 7.2, "Installation Order for High Availability Configurations"
- Section 7.3, "Requirements for High Availability Configurations"

7.1 Overview of High Availability Configurations

This chapter provides only a brief overview of the high availability configurations in Oracle Application Server. For a complete description of the configurations, see the *Oracle Application Server High Availability Guide*.

Oracle Application Server supports the following types of high availability configurations at installation time. Note that there are multiple variants of each type.

- Section 7.1.1, "OracleAS Cold Failover Cluster"
- Section 7.1.2, "OracleAS Clusters"
- Section 7.1.3, "OracleAS Disaster Recovery"
- Section 7.1.4, "Summary of Differences"

For a quick summary of the high availability configurations, see Section 7.1.4, "Summary of Differences".

7.1.1 OracleAS Cold Failover Cluster

Oracle Application Server provides an active-passive model for its components using OracleAS Cold Failover Clusters. In an OracleAS Cold Failover Cluster topology, two or more Oracle Application Server instances are configured to serve the same application workload but only one instance is active at any particular time. These instances run on two different nodes in a hardware cluster. These two nodes also have access to a shared storage, on which you install the Oracle home for the Oracle Application Server instance.

One of the nodes in the hardware cluster is the active node. It mounts the shared storage and runs the Oracle Application Server instance. The other node is the passive, or standby, node. It runs only when the active node fails. During the failover event, the

passive node mounts the shared storage and runs the Oracle Application Server instance.

The most common properties of an OracleAS Cold Failover Cluster configuration include:

- Shared storage

  The Oracle home for the Oracle Application Server instance is typically installed on storage that is shared by the nodes in the OracleAS Cold Failover Cluster topology. The passive Oracle Application Server instance has access to the same Oracle binaries, configuration files, and data as the active instance.

- Virtual hostname

  During OracleAS Infrastructure installation, you can specify a virtual hostname in the Specify Virtual Hostname screen. This OracleAS Infrastructure virtual hostname can be managed by a hardware cluster or a load balancer and is used by the middle-tier and OracleAS Infrastructure components to access the OracleAS Infrastructure. This is regardless of whether the OracleAS Infrastructure is in a single node installation, in the OracleAS Cold Failover Cluster solution, or in the OracleAS Clusters solution.

  The virtual hostname is associated with a virtual IP. This is the name that gives the Oracle Application Server middle tiers a single system view of the OracleAS Infrastructure with the help of a hardware cluster or load balancer. This name-IP entry must be added to the DNS that the site uses, so that the middle-tier nodes can associate with the OracleAS Infrastructure without having to add this entry into their local `/etc/hosts` (or equivalent) file. For example, if the two physical hostnames of the hardware cluster are `node1.mycompany.com` and `node2.mycompany.com`, the single view of this cluster can be provided by the name `selfservice.mycompany.com`. In the DNS, `selfservice` maps to the virtual IP address of the OracleAS Infrastructure, which either floats between `node1` and `node2` via a hardware cluster or maps to node1 and `node2` by a load balancer, all without the middle tier knowing which physical node is active and actually servicing a particular request.

  See Also: *Oracle Application Server High Availability Guide*

  You cannot specify a virtual hostname during Oracle Application Server middle-tier installation, but you can still use a virtual hostname via a hardware cluster or load balancer by following the post-installation configuration steps for cold failover cluster middle tiers.

- Failover procedure

  An active-passive configuration also includes a set of scripts and procedures to detect failure of the active instance and to failover to the passive instance while minimizing downtime.

The advantages of an OracleAS Cold Failover Cluster configuration include:

- Increased availability

  If the active instance fails for any reason or must be taken offline, an identically configured passive instance is prepared to take over at any time.

- Reduced operating costs

  In an active-passive configuration only one set of processes is up and serving requests. Management of the active instance is generally less than managing an array of active instances.

- Application independence

  Some applications may not be suited to an active-active configuration. This may include applications which rely heavily on application state or on information stored locally. An active-passive configuration has only one instance serving requests at any particular time.

In general, the term OracleAS Cold Failover Cluster describes clustering at the Oracle Application Server instance level. However, if it is necessary to call out the specific type of instances being clustered, this document will use OracleAS Cold Failover Cluster (*type*) to characterize the cluster solution. For example:

- OracleAS Cold Failover Cluster (Identity Management)
- OracleAS Cold Failover Cluster (Infrastructure)

From the entry point of an Oracle Application Server system (content cache) to the back end layer (data sources), all the tiers that are crossed by a client request can be configured in a redundant manner either in an active-active configuration using OracleAS Clusterss or in an active-passive configuration using OracleAS Cold Failover Clusters.

See Chapter 8, "Installing in High Availability Environments: OracleAS Cold Failover Cluster" for installation details.

7.1.2 OracleAS Clusters

Oracle Application Server provides an active-active model for all its components with OracleAS Clusters. In an OracleAS Clusters, two or more Oracle Application Server instances are configured to serve the same application workload. These instances typically run on different nodes.

You need an external load balancer in front of the nodes. Clients direct requests to these nodes through the load balancer, which then sends the requests to one of the nodes for processing. The load balancer uses its own algorithm to decide which node to send a request to.

The most common properties of an OracleAS Clusters configuration include:

- Identical instance configuration

  The instances are meant to serve the same workload or application. Their identical configuration guarantees that they deliver identical responses to the same request. Note that some configuration properties are allowed to be instance-specific, such as local host name information.

- Managed as a virtual single instance

  Changes in configuration made to one instance usually need to be propagated to the other instances in an active-active topology.

- Independent operation

  The loss of one Oracle Application Server instance in an active-active topology should not affect the ability of the other instances to continue to serve requests.

The advantages of an OracleAS Clusters configuration include:

- Increased availability

  An active-active topology has built-in redundancy (multiple Oracle Application Server instances run the same components). Loss of one instance can be tolerated because other instances can continue to serve the same requests.

- Increased scalability and performance

  Multiple identically-configured instances provide the capability to have a distributed workload shared among different machines and processes. New instances can also be added as the demand of the application grows.

In general, the term OracleAS Clusters describes clustering at the Oracle Application Server instance level. However, if it is necessary to call out the specific type of instances being clustered, this document will use OracleAS Clusters (*type*) to characterize the cluster solution. For example:

- two or more Oracle Identity Management instances are known as OracleAS Cluster (Identity Management)

For details on OracleAS Cluster (Identity Management), see Chapter 9, "Installing in High Availability Environments: OracleAS Cluster (Identity Management)".

7.1.3 OracleAS Disaster Recovery

OracleAS Disaster Recovery configurations have the following characteristics:

- A production site and a standby site that mirrors the production site. Typically, these sites are located some distance from each other to guard against site failures such as floods, fires, or earthquakes. During normal operation, the production site handles all the requests. If the production site goes down, the standby site takes over and handles all the requests.
- Each site has all the hardware and software to run. It contains nodes for running OracleAS Infrastructure and the middle tiers; load balancers; and DNS servers.

OracleAS Disaster Recovery includes OracleAS Infrastructure and middle tiers. For details, see Chapter 10, "Installing in High Availability Environments: OracleAS Disaster Recovery".

7.1.4 Summary of Differences

Table 7–1 summarizes the differences among the high availability configurations.

Table 7–1 Differences Among the High Availability Configurations

	OracleAS Cold Failover Cluster	OracleAS Clusters	OracleAS Disaster Recovery
Node configuration	Active-Passive	Active-Active	Active-Passive
Hardware cluster	Yes	No	Optional (hardware cluster required only if you installed the OracleAS Infrastructure in an OracleAS Cold Failover Cluster configuration)
Virtual hostname	Yes	No	Yes
Load balancer	No	Yes	No[1]
Shared storage	Yes	No	No

[1] Geographic load balancer may be used to perform site name switchover.

7.2 Installation Order for High Availability Configurations

For all high availability configurations, you install the components in the following order:

1. OracleAS Metadata Repository
2. Oracle Identity Management components

   If you are distributing the Oracle Identity Management components, you install them in the following order:

   a. Oracle Internet Directory and Oracle Directory Integration Platform
   b. OracleAS Single Sign-On and Oracle Delegated Administration Services
3. Middle tiers

   Note that you can install middle tiers before the other components and reassociate them with the high availability configuration following installation of the other components.

7.3 Requirements for High Availability Configurations

This section describes the requirements common to all high availability configurations. In addition to these common requirements, each configuration has its own specific requirements. See the individual chapters for details.

Note: You still need to meet the requirements listed in Chapter 2, "Requirements", plus requirements specific to the high availability configuration that you plan to use.

The common requirements are:

- Section 7.3.1, "Check Minimum Number of Nodes"
- Section 7.3.2, "Check That Groups Are Defined Identically on All Nodes"
- Section 7.3.3, "Check the Properties of the oracle User"
- Section 7.3.4, "Check for Previous Oracle Installations on All Nodes"

7.3.1 Check Minimum Number of Nodes

You need at least two nodes in a high availability configuration. If a node fails for any reason, the second node takes over.

7.3.2 Check That Groups Are Defined Identically on All Nodes

Check that the `/etc/group` file on all nodes in the cluster contains the operating system groups that you plan to use. You should have one group for the oraInventory directory, and one or two groups for database administration. The group names and the group IDs must be the same for all nodes.

See Section 2.7, "Operating System Groups" for details.

7.3.3 Check the Properties of the oracle User

Check that the `oracle` operating system user, which you log in as to install Oracle Application Server, has the following properties:

- Belongs to the `oinstall` group and to the `osdba` group. The `oinstall` group is for the oraInventory directory, and the `osdba` group is a database administration group. See Section 2.7, "Operating System Groups" for details.

- Has write privileges on remote directories.

7.3.4 Check for Previous Oracle Installations on All Nodes

Check that all the nodes where you want to install Oracle Application Server in a high availability configuration do not have existing oraInventory directories.

You need to do this because you want the installer to prompt you to enter a location for the oraInventory directory. The location of the existing oraInventory directory might not be ideal for the Oracle Application Server instance that you are about to install. For example, in OracleAS Cold Failover Cluster, you want the oraInventory directory to be on the shared storage. If the installer finds an existing oraInventory directory, it will automatically use it and will not prompt you to enter a location.

To check if a node contains an oraInventory directory that could be detected by the installer:

1. On each node, check for the `/var/opt/oracle/oraInst.loc` file.

   If a node does not contain the file, then it does not have an oraInventory directory that will be used by the installer. You can check the next node.

2. For nodes that contain the `oraInst.loc` file, rename the directory to something else so that the installer does not see it. The installer then prompts you to enter a location for the oraInventory directory.

   The following example renames the `oracle` directory to `oracle.orig` (you need to be root to do this):

   ```
   prompt> su
   Password: root_password
   # cd /var/opt
   # mv oracle oracle.orig
   ```

When you run the installer to install Oracle Application Server, the installer creates a new `/var/opt/oracle` directory and new files in it. You might need both `oracle` and `oracle.orig` directories. Do not delete either one or rename one over the other.

The installer uses the `/var/opt/oracle` directory and its files. Be sure that the right `oracle` directory is in place before running the installer (for example, if you are deinstalling or expanding a product).

8

Installing in High Availability Environments: OracleAS Cold Failover Cluster

This chapter describes how to install Oracle Application Server in OracleAS Cold Failover Cluster configurations.

- Section 8.1, "OracleAS Cold Failover Cluster: Introduction"
- Section 8.2, "Pre-Installation Steps for OracleAS Cold Failover Cluster"
- Section 8.3, "Installing an OracleAS Cold Failover Cluster (Infrastructure) Configuration"
- Section 8.4, "Installing a Distributed OracleAS Cold Failover Cluster (Infrastructure) Configuration"
- Section 8.5, "Installing an OracleAS Cold Failover Cluster (Identity Management) Configuration"
- Section 8.6, "Installing a Distributed OracleAS Cold Failover Cluster (Identity Management) Configuration"
- Section 8.7, "Installing Oracle Delegated Administration Services and OracleAS Single Sign-On in an OracleAS Cold Failover Cluster"
- Section 8.8, "Installing Only the OracleAS Metadata Repository in an OracleAS Cold Failover Cluster Environment"
- Section 8.9, "Post-Installation Steps for OracleAS Cold Failover Cluster"
- Section 8.10, "Installing Middle Tiers Against an OracleAS Cold Failover Cluster Infrastructure"
- Section 8.11, "Installing Regular Middle-Tiers on OracleAS Cold Failover Cluster Nodes"

8.1 OracleAS Cold Failover Cluster: Introduction

In OracleAS Cold Failover Cluster configurations, you have an active and a passive node, and shared storage that can be accessed by either node.

During normal operation, the active node runs Oracle Application Server processes and processes requests from clients. If the active node fails, then a failover event occurs. The passive node takes over and becomes the active node. It mounts the shared storage and runs the processes.

Configurations

You can install OracleAS Cold Failover Cluster in these configurations:

- OracleAS Cold Failover Cluster (Infrastructure). See Section 8.3.
- Distributed OracleAS Cold Failover Cluster (Infrastructure). See Section 8.4.
- OracleAS Cold Failover Cluster (Identity Management). See Section 8.5.
- Distributed OracleAS Cold Failover Cluster (Identity Management). See Section 8.6.

8.2 Pre-Installation Steps for OracleAS Cold Failover Cluster

Before installing Oracle Application Server in an OracleAS Cold Failover Cluster, perform these procedures:

- Section 8.2.1, "Map the Virtual Hostname and Virtual IP Address"
- Section 8.2.2, "Set Up a File System That Can Be Mounted from Both Nodes"
- Section 8.2.3, "Review Recommendations for Automatic Storage Management (ASM)"
- Section 8.2.4, "Check That Clusterware Is Running (Automated Failovers only)"
- Section 8.2.5, "Modify listener.ora file for Existing Database"

Note: In addition to the requirements listed in this chapter, ensure that you meet the requirements described in Section 7.3, "Requirements for High Availability Configurations".

8.2.1 Map the Virtual Hostname and Virtual IP Address

Each node in an OracleAS Cold Failover Cluster configuration is associated with its own physical IP address. In addition, the active node in the cluster is associated with a virtual hostname and virtual IP address. This allows clients to access the OracleAS Cold Failover Cluster using the virtual hostname.

Virtual hostnames and virtual IP addresses are any valid hostname and IP address in the context of the subnet containing the hardware cluster.

Note: Map the virtual hostname and virtual IP address only to the active node. Do not map the virtual hostname and IP address to both active and secondary nodes at the same time. When you failover, only then map the virtual hostname and IP address to the secondary node, which is now the active node.

Note: Before attempting to complete this procedure, ask the system or network administrator to review all the steps required. The procedure will reconfigure the network settings on the cluster nodes and may vary with differing network implementations.

The following example configures a virtual hostname called `vhost.mydomain.com`, with a virtual IP of 138.1.12.191:

1. Become the root user.

```
prompt> su
Password: root_password
```

2. Determine the public network interface.

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
lo0:1: flags=1008849<UP,LOOPBACK,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 8232 index
1
        inet 172.16.193.1 netmask ffffffff
ge0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 138.1.13.146 netmask fffffc00 broadcast 138.1.15.255
        ether 8:0:20:fd:1:23
hme0: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index
3
        inet 172.16.1.1 netmask ffffff80 broadcast 172.16.1.127
        ether 8:0:20:fd:1:23
hme0:2: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500
index 3
        inet 172.16.194.6 netmask fffffffc broadcast 172.16.194.7
ge1: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index
4
        inet 172.16.0.129 netmask ffffff80 broadcast 172.16.0.255
        ether 8:0:20:fd:1:23
```

From the output, `ge0` is the public network interface. It is not a loopback interface and not a private interface.

3. Add the virtual IP to the `ge0` network interface.

```
# ifconfig ge0 addif 138.1.12.191 up
```

"ge0" and the IP address are values specific to this example. Replace them with values appropriate for your cluster.

4. Check that new interface was added:

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
lo0:1: flags=1008849<UP,LOOPBACK,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 8232 index
1
        inet 172.16.193.1 netmask ffffffff
ge0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 138.1.13.146 netmask fffffc00 broadcast 138.1.15.255
        ether 8:0:20:fd:1:23
ge0:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 138.1.12.191 netmask ffff0000 broadcast 138.1.255.255
hme0: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index
3
        inet 172.16.1.1 netmask ffffff80 broadcast 172.16.1.127
        ether 8:0:20:fd:1:23
hme0:2: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500
index 3
        inet 172.16.194.6 netmask fffffffc broadcast 172.16.194.7
ge1: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4> mtu 1500 index
4
        inet 172.16.0.129 netmask ffffff80 broadcast 172.16.0.255
        ether 8:0:20:fd:1:23
```

The virtual IP appears in the `ge0:1` entry. During installation, when you enter "vhost.mydomain.com" as the virtual hostname in the Specify Virtual Hostname screen, the installer checks that "vhost.mydomain.com" is a valid interface.

On Failover

If the active node fails, then the secondary node takes over. If you do not have a clusterware agent to map the virtual IP from the failed node to the secondary node, then you have to do it manually. You have to remove the virtual IP mapping from the failed node, and map it to the secondary node.

1. On the failed node, become superuser and remove the virtual IP.

   If the failed node fails completely (that is, it does not boot up), you can skip this step and go to step 2. If the node fails partially (for example, disk or memory problems), and the node is still ping-able, you have to perform this step.

   ```
   prompt> su
   Password: root_password
   # ifconfig ge0 removeif 138.1.12.191
   ```

   "ge0" and the IP address are values specific to this example. Replace them with values appropriate for your cluster.

2. On the secondary node, add the virtual IP to the `ge0` network interface.

   ```
   # ifconfig ge0 addif 138.1.12.191 up
   ```

   "ge0" and the IP address are values specific to this example. Replace them with values appropriate for your cluster.

3. On the secondary node, check that the new interface was added:

   ```
   # ifconfig -a
   ...
   ge0:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
           inet 138.1.12.191 netmask ffff0000 broadcast 138.1.255.255
   ...
   ```

8.2.2 Set Up a File System That Can Be Mounted from Both Nodes

Although the hardware cluster has shared storage, you need to create a file system on this shared storage such that both nodes of the OracleAS Cold Failover Cluster can mount this file system. You will use this file system for the following directories:

- Oracle home directory for the Oracle Application Server instance
- The oraInventory directory

For disk space requirements, see Section 2.2, "System Requirements".

If you are running a volume manager on the cluster to manage the shared storage, refer to the volume manager documentation for steps to create a volume. Once a volume is created, you can create the file system on that volume.

If you do not have a volume manager, you can create a file system on the shared disk directly. Ensure that the hardware vendor supports this, that the file system can be mounted from either node of the OracleAS Cold Failover Cluster, and that the file system is repairable from either node if a node fails.

To check that the file system can be mounted from either node, do the following steps:

1. Set up and mount the file system from node 1.
2. Unmount the file system from node 1.
3. Mount the file system from node 2 using the same mount point that you used in step 1.

4. Unmount it from node 2, and mount it on node 1, because you will be running the installer from node 1.

> **Note:** Only one node of the OracleAS Cold Failover Cluster should mount the file system at any given time. File system configuration files on all nodes of the cluster should not include an entry for the automatic mount of the file system upon a node restart or execution of a global mount command. For example, on UNIX platforms, do not include an entry for this file system in `/etc/vfstab` file.

8.2.3 Review Recommendations for Automatic Storage Management (ASM)

If you plan to use ASM instances for the OracleAS Metadata Repository database, consider these recommendations:

- If you plan to use ASM with Oracle database instances from multiple database homes on the same node, then you should run the ASM instance from an Oracle home that is different from the database homes.
- The ASM home should be installed on every cluster node. This prevents the accidental removal of ASM instances that are in use by databases from other homes during the de-installation of a database Oracle home.

8.2.4 Check That Clusterware Is Running (Automated Failovers only)

If you plan to automate failovers in the OracleAS Cold Failover Cluster, then each node in a cluster must be running hardware vendor clusterware.

To check that the clusterware is running, use the command appropriate for your clusterware.

8.2.5 Modify listener.ora file for Existing Database

If there is an existing database on the system on which you are installing and you are performing an installation that includes OracleAS Metadata Repository, you need to modify the `listener.ora` file for the existing database before proceeding with the installation. Perform the following steps to modify the `listener.ora` file:

1. Make sure you set the `ORACLE_HOME` and `ORACLE_SID` environment variables for the existing database.
2. Stop the listener for the database:

   ```
   prompt> lsnrctl stop
   ```

3. Open the `listener.ora` file, which is located at:

   ORACLE_HOME`/network/admin/listener.ora`

   where *ORACLE_HOME* is the home for the existing database.

4. Locate the `LISTENER` entry in the file:

   ```
   LISTENER =
     (DESCRIPTION_LIST =
       (DESCRIPTION =
         (ADDRESS_LIST =
           (ADDRESS = (PROTOCOL = TCP)(HOST = db_hostname)(PORT = db_port))
         )
   ```

```
...
```

In this example, *db_hostname* is the fully-qualified hostname for the existing database and *db_port* is the port for the existing database.

5. Add an ADDRESS entry to the ADDRESS_LIST entry for the new Oracle Application Server instance:

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS_LIST =
        (ADDRESS = (PROTOCOL = TCP)(HOST = db_hostname)(PORT = db_port))
        (ADDRESS = (PROTOCOL = TCP)(HOST = new_hostname)(PORT = new_port))
      )
...
```

In this example, *new_hostname* is the fully-qualified hostname for the new Oracle Application Server instance and *new_port* is the port for the new Oracle Application Server instance. See Section 2.6.4.1, "If Port 1521 Is In Use by an Existing Oracle Database" for information on ensuring that the database listeners to not conflict.

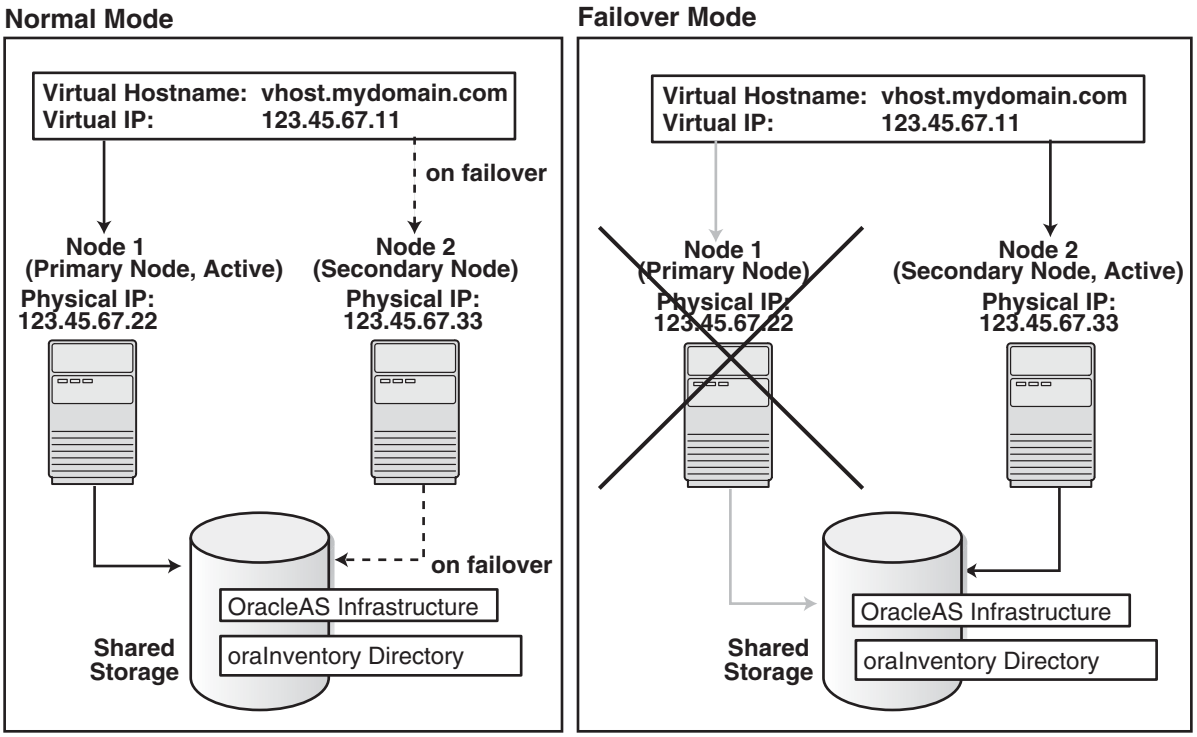
6. Start the listener for the existing database:

```
prompt> lsnrctl start
```

8.3 Installing an OracleAS Cold Failover Cluster (Infrastructure) Configuration

Figure 8–1 shows an OracleAS Cold Failover Cluster (Infrastructure) configuration.

Figure 8–1 OracleAS Cold Failover Cluster (Infrastructure) Configuration



The figure shows:

- two nodes running clusterware
- storage devices local to each node
- storage device that can be accessed by both nodes. You install OracleAS Infrastructure on this shared storage device.

During normal operation, one node ("node 1") acts as the active node. It mounts the shared storage to access the OracleAS Infrastructure files, runs OracleAS Infrastructure processes, and handles all requests.

If the active node goes down for any reason, the clusterware fails over OracleAS Infrastructure processes to the other node ("node 2"), which now becomes the active node. It mounts the shared storage, runs the processes, and handles all requests.

These nodes appear as one computer to clients through the use of a virtual address. To access the OracleAS Infrastructure, clients, including middle-tier components and applications, use the virtual address associated with the cluster. The virtual address is associated with the active node (node 1 during normal operation, node 2 if node 1 goes down). Clients do not need to know which node (node 1 or node 2) is servicing requests.

You use the virtual hostname in URLs that access the infrastructure. For example, if `vhost.mydomain.com` is the virtual hostname, the URLs for the Oracle HTTP Server and the Application Server Control would look like the following:

URL for:	Example URL
Oracle HTTP Server, Welcome page	http://vhost.mydomain.com:7777
Oracle HTTP Server, secure mode	https://vhost.mydomain.com:4443

URL for:	Example URL
Application Server Control	http://vhost.mydomain.com:1156

Oracle Application Server Middle Tiers

You can install and run the middle tiers on other nodes (nodes that are not running OracleAS Infrastructure). During installation, you set up the middle tiers to use services from the OracleAS Infrastructure installed on the shared storage device.

You can also install and run the middle tiers on the cluster nodes without using an OracleAS Cold Failover Cluster configuration for the middle tiers. In this case, you install middle tiers using the regular installation process. If you do this, make sure the middle tier ports will not conflict with the OracleAS Infrastructure ports when a failover occurs.

8.3.1 OracleAS Cold Failover Cluster (Infrastructure): Overview of Installation Steps

To set up an OracleAS Cold Failover Cluster (Infrastructure) configuration, perform these steps:

Table 8–1 Overview of Installation Steps for OracleAS Cold Failover Cluster (Infrastructure)

	Step	Description
1.	Perform Pre-Installation Steps	Pre-installation tasks, described in Section 8.2, include: ▪ Section 8.2.1, "Map the Virtual Hostname and Virtual IP Address" ▪ Section 8.2.2, "Set Up a File System That Can Be Mounted from Both Nodes" ▪ Section 8.2.3, "Review Recommendations for Automatic Storage Management (ASM)"
2.	Install OracleAS Infrastructure	Install OracleAS Infrastructure on the shared storage.
3.	Perform Post-Installation Steps	This post-installation step configures the CSS daemon. This step is required only if you are using ASM (Automatic Storage Management) feature of the Oracle database, and you do not have an existing Oracle database.

8.3.2 OracleAS Cold Failover Cluster (Infrastructure): Details of Installation Steps

This section lists the steps for installing OracleAS Infrastructure in an OracleAS Cold Failover Cluster (Infrastructure) configuration.

Step 1 Perform Pre-Installation Steps

Perform the pre-installation steps listed in Section 8.2, "Pre-Installation Steps for OracleAS Cold Failover Cluster".

Step 2 Install OracleAS Infrastructure

For OracleAS Cold Failover Cluster (Infrastructure), you install both OracleAS Metadata Repository and Oracle Identity Management in the same Oracle home by selecting **Identity Management and Metadata Repository** in the Select Installation Type screen. This option creates a new database for the OracleAS Metadata Repository and a new Oracle Internet Directory.

Note that if there is an existing Oracle Application Server 10*g* database on the system where you plan to install OracleAS Infrastructure, you must perform the steps in Section 8.2.5, "Modify listener.ora file for Existing Database" prior to installation.

Key Points

- The destination directory must be on the shared disk.
- Remember to select **High Availability and Replication** in the Select Configuration Options screen. By default, this option is not selected.
- You enter the virtual hostname in the Specify Virtual Hostname screen.

Installer Screens

Run the installer and follow the screen sequence shown in Table 8–2:

Table 8–2 Installing OracleAS Infrastructure in an OracleAS Cold Failover Cluster (Infrastructure)

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ▪ In the Select Installation Type screen, select **Identity Management and Metadata Repository**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform**. Select **Oracle Application Server Certificate Authority (OCA)** if you want a certificate authority. Select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file in the provided field. Click **Next**.
4.	Select High Availability or Replication Option	Select **Virtual Host**, and click **Next**.
5.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
6.	Specify Virtual Hostname	**Note:** This is a critical screen when installing the infrastructure in an OracleAS Cold Failover Cluster. If you do not see this screen, check the following: ▪ Return to the Select High Availability or Replication Option screen and ensure that you selected **Virtual Host**. ▪ Return to the Select Configuration Options screen and ensure that you selected **High Availability and Replication**. **Virtual Hostname**: Enter the virtual hostname for the OracleAS Cold Failover Cluster configuration. Example: `vhost.mydomain.com` Click **Next**.

Table 8–2 (Cont.) Installing OracleAS Infrastructure in an OracleAS Cold Failover Cluster (Infrastructure)

	Screen	Action
7.	OCA screens	If you selected **Oracle Application Server Certificate Authority (OCA)** in the Select Configuration Options screen, the installer displays screens for configuring OCA. See Section 4.30, "Install Fragment: OCA Screens" for details.
8.	Specify Database Configuration Options	**Global Database Name**: Enter a name for the OracleAS Metadata Repository database. Append a domain name to the database name. This domain name for the global database name can be different from your network domain name. The domain name portion of the global database name has the following naming restrictions: ■ Can contain only alphanumeric, underscore (_), minus (-), and pound (#) characters ■ Must not be longer than 128 characters The database name portion of the global database name has the following naming restrictions: ■ Must contain alphanumeric characters only ■ Must not be longer than eight characters ■ Must not contain `PORT` or `HOST` in uppercase characters. If you want the name to contain "host" or "port", use lowercase characters. Example: `orcl.mydomain.com` **Note:** Be sure that you do not enter two or more periods together, for example, `orcl.mydomain.com`. The installer does not check for this, and this will lead to errors later during the installation process. **SID**: Enter the system identifier for the OracleAS Metadata Repository database. Typically this is the same as the global database name, but without the domain name. The SID must be unique across all databases. SIDs have the following naming restrictions: ■ Must contain alphanumeric characters only ■ Must not be longer than eight characters ■ Must not contain `PORT` or `HOST` in uppercase characters. If you want the name to contain "host" or "port", use lowercase characters. Example: `orcl` **Database Character Set**: Select the character set to use. See also Section 4.15, "Support for NE8ISO8859P10 and CEL8ISO8859P14 Characters Sets". **Database File Location**: Enter the full path to the parent directory for the data files directory. This parent directory must already exist, and you must have write permissions in this directory. The installer will create a subdirectory in this parent directory, and the subdirectory will have the same name as the SID. The data files will be placed in this subdirectory. Example: If you enter `/u02/oradata`, and the SID is `orcl`, then the data files will be located in `/u02/oradata/orcl`. Click **Next**.
9.	Specify Database Schema Passwords	Set the passwords for these privileged database schemas: SYS, SYSTEM, SYSMAN, and DBSNMP. You can set different passwords for each schema, or you can set the same password for all the schemas. See Section 4.14, "Restrictions on the Passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP Users" for rules on setting passwords for these accounts. Click **Next**.

Table 8–2 (Cont.) Installing OracleAS Infrastructure in an OracleAS Cold Failover Cluster (Infrastructure)

	Screen	Action
10.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `infra` **ias_admin Password** and **Confirm Password**: Enter and confirm the password for the ias_admin user. This is the administrative user for this infrastructure instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for password requirements. Example: `welcome99` Click **Next**.
11.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

Step 3 Perform Post-Installation Steps

The following step is required only if you meet **both** of these requirements:

- You plan to use the Automatic Storage Management (ASM) feature of Oracle Database 10*g* for the OracleAS Metadata Repository.
- Your computer does not have an existing Oracle Database 10*g*.

If you meet these requirements, you need to configure the Cluster Synchronization Services (CSS) daemon on the other node. The CSS daemon synchronizes ASM instances with the database instances that use the ASM instances for database file storage.

To configure the CSS daemon:

1. Stop all the processes in the OracleAS Cold Failover Cluster (Infrastructure) home.
2. Stop the CSS daemon. You can do this by running the following command as root.

   ```
   # /etc/init.d/init.cssd stop
   ```

3. Fail over the IP and the disk to the other node.
4. On the other node, run the following command as root:

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

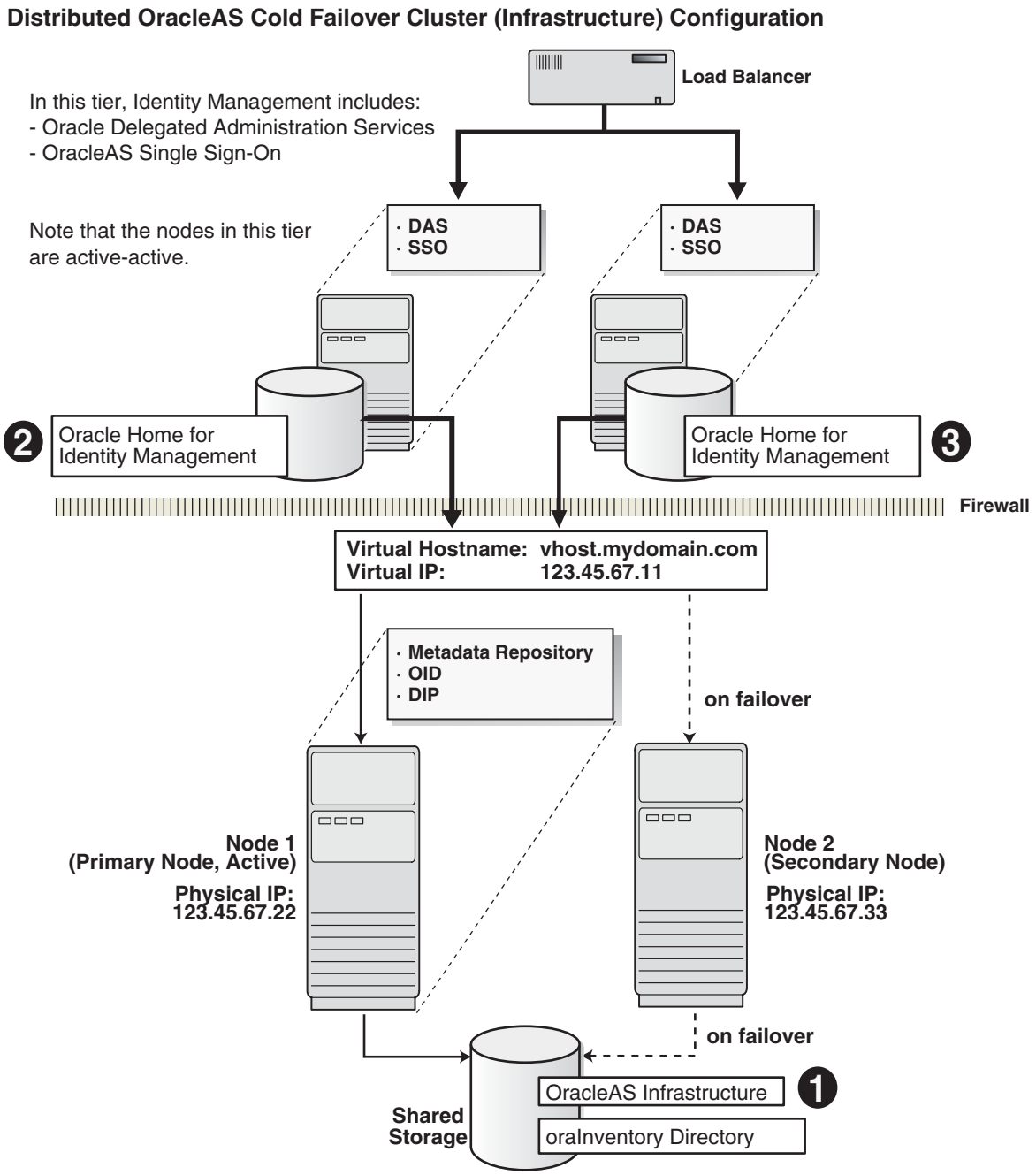
   ORACLE_HOME is where you installed the OracleAS Cold Failover Cluster (Infrastructure).

8.4 Installing a Distributed OracleAS Cold Failover Cluster (Infrastructure) Configuration

Figure 8–2 shows a distributed OracleAS Cold Failover Cluster (Infrastructure) configuration.

This configuration is similar to the configuration described in Section 8.3, "Installing an OracleAS Cold Failover Cluster (Infrastructure) Configuration", except that the OracleAS Single Sign-On and Oracle Delegated Administration Services components are installed separately on other nodes in an active-active configuration.

Figure 8–2 Distributed OracleAS Cold Failover Cluster (Infrastructure) Configuration



In a distributed OracleAS Cold Failover Cluster (Infrastructure) configuration, you run the OracleAS Metadata Repository, Oracle Internet Directory, and Oracle Directory Integration Platform in an *active-passive* configuration.

However, the OracleAS Single Sign-On and Oracle Delegated Administration Services components run in an *active-active* configuration. You have a load balancer to direct requests to the nodes running these components.

8.4.1 Distributed OracleAS Cold Failover Cluster (Infrastructure): Overview of Installation Steps

To set up a distributed OracleAS Cold Failover Cluster (Infrastructure) configuration, perform these steps:

Table 8–3 Overview of Installation Steps for Distributed OracleAS Cold Failover Cluster (Infrastructure)

	Step	Description
1.	Perform Pre-Installation Steps	Pre-installation tasks, described in Section 8.2, include: ▪ Section 8.2.1, "Map the Virtual Hostname and Virtual IP Address" ▪ Section 8.2.2, "Set Up a File System That Can Be Mounted from Both Nodes" ▪ Section 8.2.3, "Review Recommendations for Automatic Storage Management (ASM)"
2.	Install OracleAS Infrastructure	In this step, you install OracleAS Infrastructure on the shared storage. You install all components except OracleAS Single Sign-On, Oracle Delegated Administration Services, and OCA.
3.	Perform Post-Installation Steps	This post-installation step configures the CSS daemon. This step is required only if you are using ASM (Automatic Storage Management) feature of the Oracle database, and you do not have an existing Oracle database.
4.	Install OracleAS Single Sign-On and Oracle Delegated Administration Services	In this step, you install OracleAS Single Sign-On and Oracle Delegated Administration Services.

8.4.2 Distributed OracleAS Cold Failover Cluster (Infrastructure): Details of Installation Steps

Step 1 Perform Pre-Installation Steps

Perform the pre-installation steps listed in Section 8.2, "Pre-Installation Steps for OracleAS Cold Failover Cluster".

Step 2 Install OracleAS Infrastructure

In a distributed OracleAS Cold Failover Cluster (Infrastructure) configuration, you install both OracleAS Metadata Repository and Oracle Identity Management components (except for OracleAS Single Sign-On, Oracle Delegated Administration Services, and OCA) in the same Oracle home by selecting **Identity Management and OracleAS Metadata Repository** in the Select Installation Type screen. This option creates a new database for the OracleAS Metadata Repository and a new Oracle Internet Directory.

The steps are the same as those listed in step 2, "Install OracleAS Infrastructure" on page 8-8, except that in the Select Configuration Options screen, do not select **OracleAS Single Sign-On**, **Oracle Application Server Delegated Administration Services**, and **OracleAS Certificate Authority (OCA)**.

Step 3 Perform Post-Installation Steps

The following step is required only if you meet **both** of these requirements:

- You plan to use the Automatic Storage Management (ASM) feature of Oracle Database 10*g* for the OracleAS Metadata Repository.

- Your computer does not have an existing Oracle Database 10*g*.

If you meet these requirements, you need to configure the CSS daemon on the other node. The CSS daemon synchronizes ASM instances with the database instances that use the ASM instances for database file storage.

To configure the CSS daemon:

1. Stop all the processes in the OracleAS Cold Failover Cluster (Infrastructure) home.
2. Stop the CSS daemon. You can do this by running the following command as root.

   ```
   # /etc/init.d/init.cssd stop
   ```

3. Fail over the IP and the disk to the other node.
4. On the other node, run the following command as root:

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

   ORACLE_HOME is where you installed the OracleAS Cold Failover Cluster (Infrastructure).

Step 4 Install OracleAS Single Sign-On and Oracle Delegated Administration Services

You install OracleAS Single Sign-On and Oracle Delegated Administration Services on the local disks of each node. You perform these installations separately.

Pre-Installation Steps

This installation is actually an OracleAS Cluster (Identity Management) installation. As such, you perform the OracleAS Cluster (Identity Management) setup steps in Chapter 9, "Installing in High Availability Environments: OracleAS Cluster (Identity Management)":

- Section 9.2.1, "Use the Same Path for the Oracle Home Directory (recommended)"
- Section 9.2.2, "Synchronize Clocks on All Nodes"
- Section 9.2.3, "Configure Virtual Server Names and Ports for the Load Balancer"

Installation Steps

The steps are the same as those listed in Section 9.6.5, "Installing OracleAS Single Sign-On and Oracle Delegated Administration Services on Each Node".

8.5 Installing an OracleAS Cold Failover Cluster (Identity Management) Configuration

Figure 8–3 shows an OracleAS Cold Failover Cluster (Identity Management) configuration.

This configuration is suitable if you have the OracleAS Metadata Repository database in a separate highly available environment and you want to use an active-passive configuration for the Oracle Identity Management components. You install the Oracle Identity Management components on a shared disk different from the share disk that contains the OracleAS Metadata Repository database.

This configuration includes:

- two clustered nodes
- storage devices local to each node

- two shared disks that can be accessed by both nodes. One shared disk contains the Oracle home for the database (on which you will load the OracleAS Metadata Repository), and on the other shared disk, you will install Oracle Identity Management.

During normal operation, node 1, which is the primary node, is the active node. It mounts both shared disks to access the Oracle Identity Management and database files, runs the Oracle Identity Management and database processes, and handles all requests.

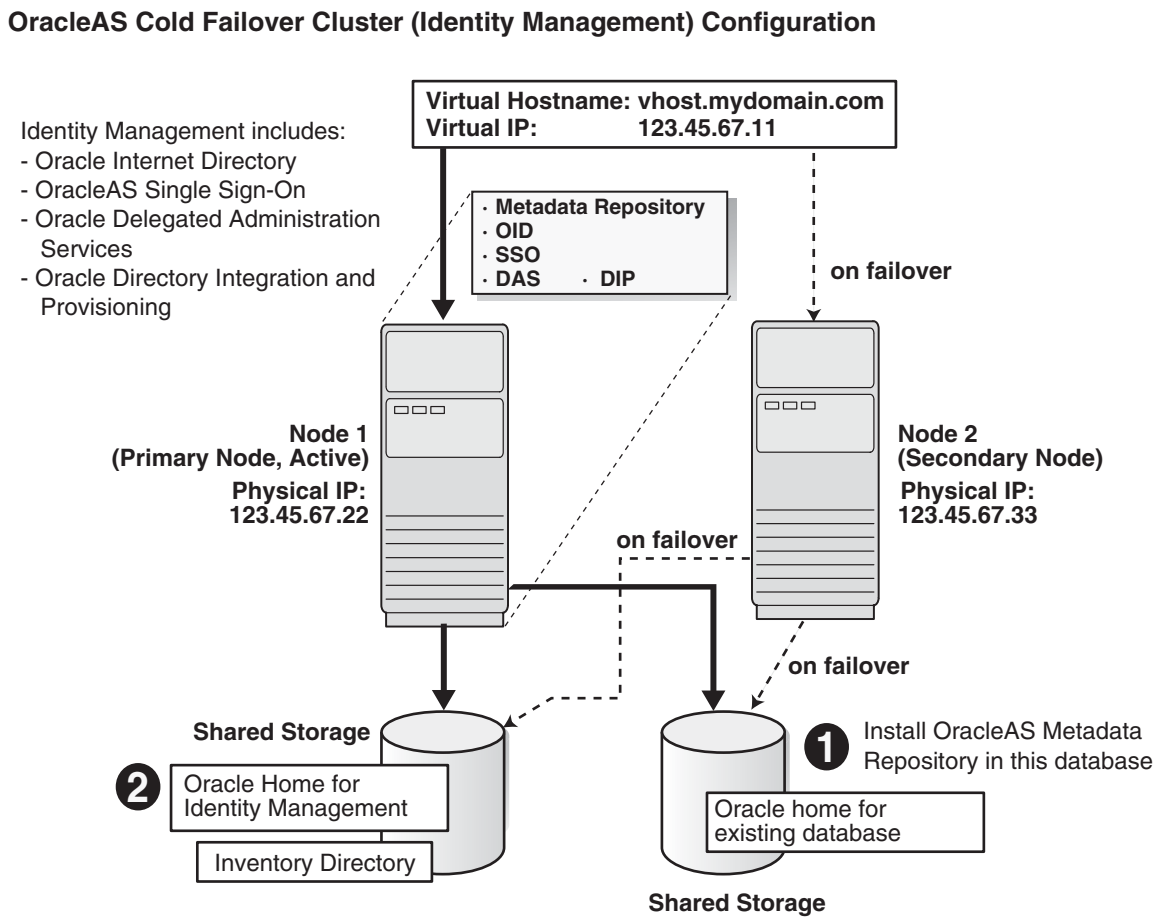
If node 1 goes down for any reason, the clusterware fails over the Oracle Identity Management and database processes to node 2. Node 2 becomes the active node, mounts both shared disks, runs the processes, and handles all requests.

To access the active node in an OracleAS Cold Failover Cluster, clients, including middle-tier components and applications, use the virtual hostname associated with the OracleAS Cold Failover Cluster. The virtual hostname is associated with the active node (node 1 during normal operation, node 2 if node 1 goes down). Clients do not need to know which node (primary or secondary) is servicing requests.

You also use the virtual hostname in URLs that access the infrastructure. For example, if `vhost.mydomain.com` is the name of the virtual host, the URLs for the Oracle HTTP Server and the Application Server Control would look like the following:

URL for:	Example URL
Oracle HTTP Server, Welcome page	http://vhost.mydomain.com:7777
Oracle HTTP Server, secure mode	https://vhost.mydomain.com:4443
Application Server Control	http://vhost.mydomain.com:1156

Figure 8–3 OracleAS Cold Failover Cluster (Identity Management) Configuration



8.5.1 OracleAS Cold Failover Cluster (Identity Management): Overview of Installation Steps

To create an OracleAS Cold Failover Cluster (Identity Management) configuration against an existing cold failover cluster database, perform these steps:

Table 8–4 Overview of Installation Steps for OracleAS Cold Failover Cluster (Identity Management) Configuration

	Step	Description
1.	Perform Pre-Installation Steps	Pre-installation tasks, described in Section 8.2, include: ▪ Section 8.2.1, "Map the Virtual Hostname and Virtual IP Address" ▪ Section 8.2.2, "Set Up a File System That Can Be Mounted from Both Nodes" ▪ Section 8.2.3, "Review Recommendations for Automatic Storage Management (ASM)"
2.	Install OracleAS Metadata Repository	Install OracleAS Metadata Repository on your existing cold failover cluster database.
3.	Install the Oracle Identity Management Components	Install the Oracle Identity Management components.

8.5.2 OracleAS Cold Failover Cluster (Identity Management): Details of Installation Steps

Perform the following steps to install Oracle Application Server in an OracleAS Cold Failover Cluster (Identity Management) configuration.

Step 1 Perform Pre-Installation Steps

Perform the pre-installation steps listed in Section 8.2, "Pre-Installation Steps for OracleAS Cold Failover Cluster".

Step 2 Install OracleAS Metadata Repository

Use the OracleAS RepCA to install the OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

If you do not have an existing database, you can use the installer to create one. Note that you have to create the database with a virtual hostname. The database should run in an active-passive configuration, typically on a hardware cluster. See Section 8.8, "Installing Only the OracleAS Metadata Repository in an OracleAS Cold Failover Cluster Environment" for details.

Step 3 Install the Oracle Identity Management Components

You install the Oracle Identity Management on the other shared disk. Follow the installation steps described in Table 8–5.

Key Points

- When the installer prompts you for the Oracle home path, enter a path on the shared disk. Make sure that both nodes can access this path.
- In the Select High Availability or Replication Option screen, select **Virtual Host**.
- In the Specify Virtual Hostname screen, enter the virtual hostname.

Installer Screens

Table 8–5 Installing Oracle Identity Management Components

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Note: In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform**. Select **Oracle Application Server Certificate Authority (OCA)** if you want a certificate authority. Select **High Availability and Replication**. Click **Next**.

Table 8–5 (Cont.) Installing Oracle Identity Management Components

	Screen	Action
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file in the provided field. Click **Next**.
4.	Specify Repository	**Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the name of the computer where the database is running, and the port number at which it is listening. Use the format: *`host:port`*. **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Select High Availability or Replication Option	Select **Virtual Host**, and click **Next**.
6.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
7.	Specify Virtual Hostname	**Note:** This is a critical screen when installing the infrastructure in an OracleAS Cold Failover Cluster. If you do not see this screen, check the following: ▪ Return to the "Select High Availability or Replication Option" screen and ensure that you selected **Virtual Host**. ▪ Return to the Select Configuration Options screen and ensure that you selected **High Availability and Replication**. **Virtual Hostname**: Enter the virtual hostname for the OracleAS Cold Failover Cluster configuration. Example: `vhost.mydomain.com` Click **Next**.
8.	OCA screens	If you selected **Oracle Application Server Certificate Authority (OCA)** in the Select Configuration Options screen, the installer displays screens for configuring OCA. See Section 4.30, "Install Fragment: OCA Screens" for details.
9.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `id_mgmt` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
10.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

8.6 Installing a Distributed OracleAS Cold Failover Cluster (Identity Management) Configuration

This configuration is suitable:

- if you want to run Oracle Internet Directory and Oracle Directory Integration Platform on the same tier as your database, and Oracle Delegated Administration Services and OracleAS Single Sign-On on a different tier
- if you want to install the OracleAS Metadata Repository in an existing cold failover cluster database

Figure 8–4 shows a distributed OracleAS Cold Failover Cluster (Identity Management) configuration.

It consists of:

- two nodes running Oracle Delegated Administration Services and OracleAS Single Sign-On. These nodes are accessed through a load balancer.
- two nodes running in an active-passive configuration. These nodes will run the existing cold failover cluster database, Oracle Internet Directory, and Oracle Directory Integration Platform.
- storage devices local to each node
- two shared disks. One shared disk contains the database Oracle home. On the other shared disk, you will install Oracle Internet Directory and Oracle Directory Integration Platform.
- firewalls to separate the tiers

Tier Running the Oracle Internet Directory, Oracle Directory Integration Platform, and Database

In this tier, during normal operation, the active node mounts the shared disks to access the Oracle Identity Management and database; runs the Oracle Internet Directory, Oracle Directory Integration Platform, and database processes; and handles all requests.

If the active node goes down for any reason, the clusterware fails over the processes to the secondary node (node 2), which becomes the new active node, mounts the shared disks, runs the processes, and handles all requests.

To access the active node, clients, including middle-tier components and applications, use the virtual hostname. The virtual hostname is associated with the active node (which is the primary node during normal operation, the secondary node upon failover). Clients do not need to know which node (primary or secondary) is servicing requests.

You need to use the virtual hostname in URLs to access the active node. For example, if `vhost.mydomain.com` is the virtual hostname, the URLs for the Oracle HTTP Server and the Application Server Control for this tier would look like the following:

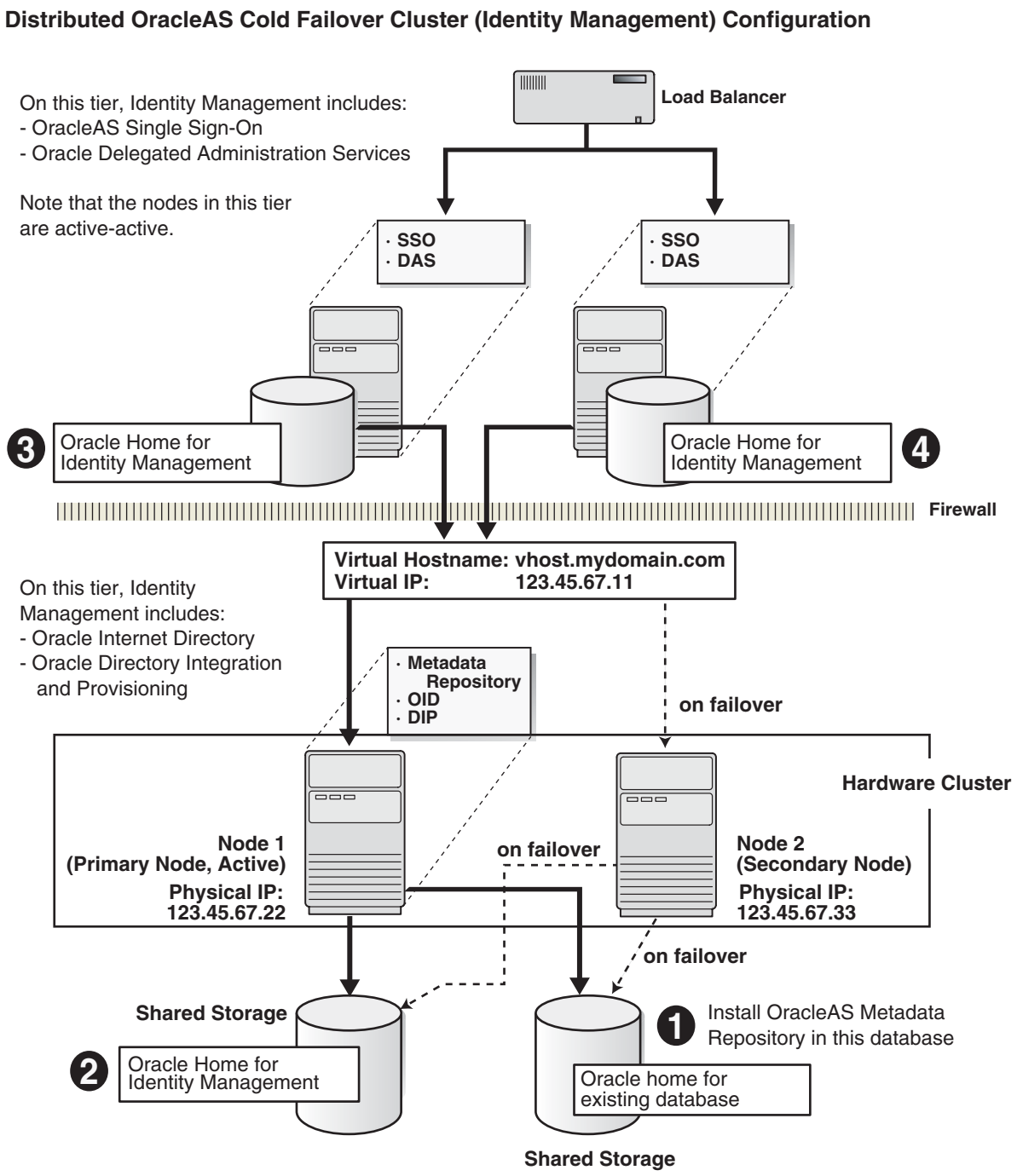
URL for:	Example URL
Oracle HTTP Server, Welcome page	http://vhost.mydomain.com:7777
Oracle HTTP Server, secure mode	https://vhost.mydomain.com:4443
Application Server Control	http://vhost.mydomain.com:1156

Tier Running Oracle Delegated Administration Services and OracleAS Single Sign-On

Note that the nodes in this tier are not clustered. Both nodes are active at the same time, and you install the files locally on each node. To access these nodes, clients go through a load balancer. For example, if the name of the load balancer is `loadbalance1.mydomain.com`, the URLs for the Oracle HTTP Server and the Application Server Control for this tier would look like the following:

URL for:	Example URL
Oracle HTTP Server, Welcome page	http://vhost.mydomain.com:7777
Oracle HTTP Server, secure mode	https://vhost.mydomain.com:4443
Application Server Control	http://vhost.mydomain.com:1156

Figure 8–4 Distributed OracleAS Cold Failover Cluster (Identity Management) Configuration



8.6.1 Distributed OracleAS Cold Failover Cluster (Identity Management): Overview of Installation Steps

To create a distributed OracleAS Cold Failover Cluster (Identity Management) configuration against an existing cold failover cluster database, perform these steps:

Table 8–6 Overview of Installation Steps for Distributed OracleAS Cold Failover Cluster (Identity Management) Configuration

	Step	Description
1.	Perform Pre-Installation Steps	Pre-installation tasks, described in Section 8.2, include: ▪ Section 8.2.1, "Map the Virtual Hostname and Virtual IP Address" ▪ Section 8.2.2, "Set Up a File System That Can Be Mounted from Both Nodes" ▪ Section 8.2.3, "Review Recommendations for Automatic Storage Management (ASM)"
2.	Install OracleAS Metadata Repository	Install OracleAS Metadata Repository on your existing cold failover cluster database.
3.	Install Oracle Internet Directory and Oracle Directory Integration Platform	Install the Oracle Internet Directory and Oracle Directory Integration Platform components.
4.	Install OracleAS Single Sign-On and Oracle Delegated Administration Services	Install the OracleAS Single Sign-On and Oracle Delegated Administration Services components.

8.6.2 Distributed OracleAS Cold Failover Cluster (Identity Management): Details of Installation Steps

Step 1 Perform Pre-Installation Steps

Perform the pre-installation steps listed in Section 8.2, "Pre-Installation Steps for OracleAS Cold Failover Cluster".

Step 2 Install OracleAS Metadata Repository

Use the OracleAS RepCA to install the OracleAS Metadata Repository in an existing database. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

If you do not have an existing database, you can use the installer to create one. Note that you have to create the database with a virtual hostname. See Section 8.8, "Installing Only the OracleAS Metadata Repository in an OracleAS Cold Failover Cluster Environment" for details.

Step 3 Install Oracle Internet Directory and Oracle Directory Integration Platform

Install the Oracle Internet Directory and Oracle Directory Integration Platform components on the other shared disk. Follow the installation steps described in Table 8–7.

Key Points

- In the Select Installation Type screen, select **Identity Management**.
- In the Select Configuration Options screen, select **Oracle Internet Directory**, **Oracle Directory Integration Platform**, and **High Availability and Replication**.
- In the Select High Availability or Replication Option screen, select **Virtual Host**.
- In the Specify Virtual Hostname screen, enter the virtual hostname.

Installer Screens

Table 8–7 Installing Oracle Internet Directory and Oracle Directory Integration Platform

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Note: In the Select Installation Type screen, select **Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Do not select **Oracle Application Server Single Sign-On**. Do not select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform**. Do not select **Oracle Application Server Certificate Authority (OCA)**. Select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	If you want to use default ports for the components, select **Automatic**. If you do not want to use the default ports, and you have created a staticports.ini file, select **Manual** and enter the fullpath to your staticports.ini file in the provided field. Click **Next**.
4.	Specify Repository	**Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the name of the computer where the database is running, and the port number at which it is listening. Use the format: *`host:port`*. **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Select High Availability or Replication Option	Select **Virtual Host**, and click **Next**.
6.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
7.	Specify Virtual Hostname	**Note:** This is a critical screen when installing the infrastructure in an OracleAS Cold Failover Cluster. If you do not see this screen, check the following: ■ Return to the Select High Availability or Replication Option screen and ensure that you selected **Virtual Host**. ■ Return to the Select Configuration Options screen and ensure that you selected **High Availability and Replication**. **Virtual Hostname**: Enter the virtual hostname for the OracleAS Cold Failover Cluster configuration. Example: `vhost.mydomain.com` Click **Next**.

Table 8–7 (Cont.) Installing Oracle Internet Directory and Oracle Directory Integration Platform

	Screen	Action
8.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `oid_dip` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
9.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

Step 4 Install OracleAS Single Sign-On and Oracle Delegated Administration Services

Install these components in an OracleAS Cluster (Identity Management) configuration. In this configuration, you install them on the local disks of each node. You perform these installations separately.

Pre-Installation steps: Because this installation is actually an OracleAS Cluster (Identity Management) installation, you can follow the OracleAS Cluster (Identity Management) setup steps in Chapter 9, "Installing in High Availability Environments: OracleAS Cluster (Identity Management)":

- Section 9.2.1, "Use the Same Path for the Oracle Home Directory (recommended)"
- Section 9.2.2, "Synchronize Clocks on All Nodes"
- Section 9.2.3, "Configure Virtual Server Names and Ports for the Load Balancer"

Installation steps: The installation steps are described in Section 9.6.5, "Installing OracleAS Single Sign-On and Oracle Delegated Administration Services on Each Node".

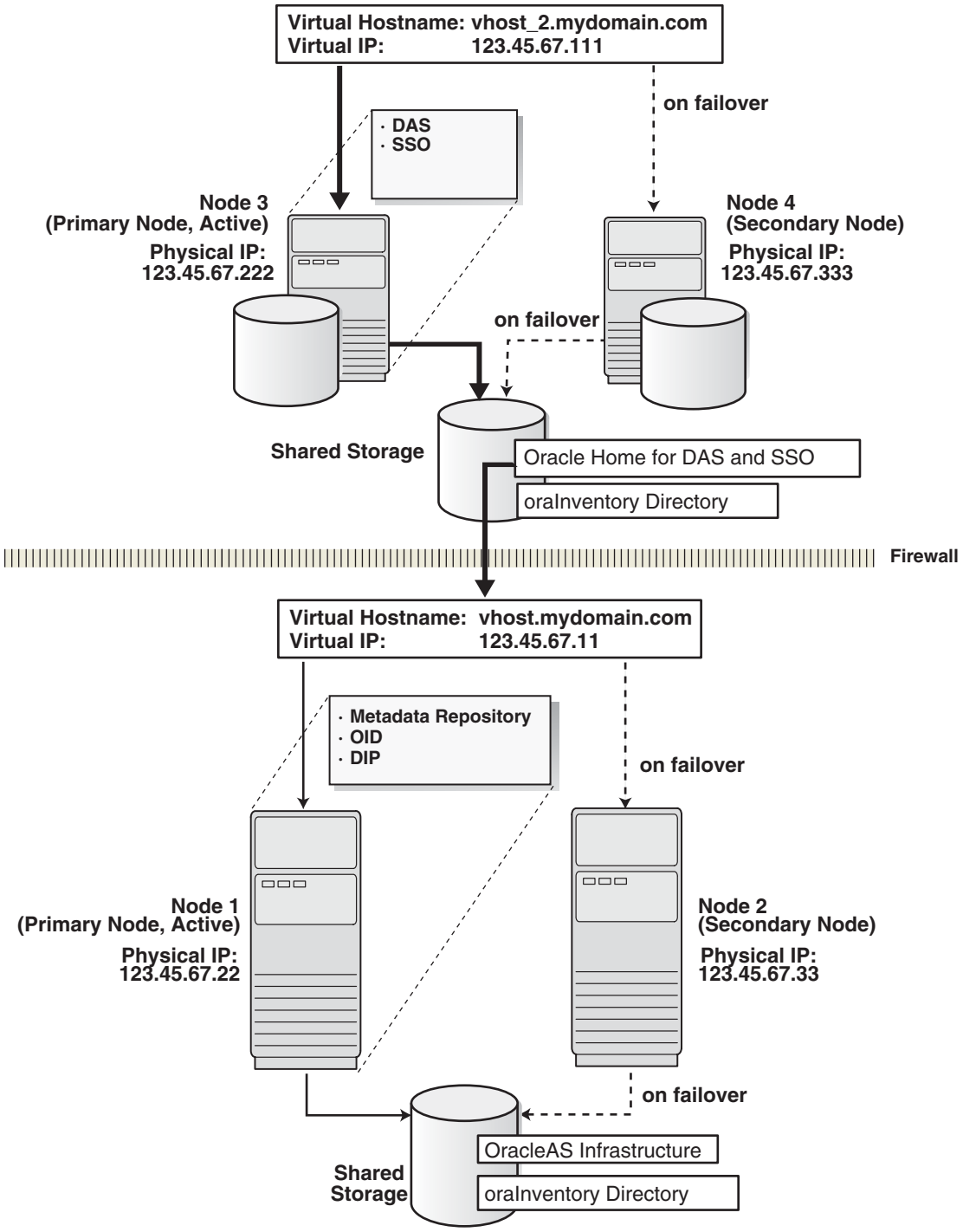
8.7 Installing Oracle Delegated Administration Services and OracleAS Single Sign-On in an OracleAS Cold Failover Cluster

The configuration described in this section is similar to that described in Section 8.4, "Installing a Distributed OracleAS Cold Failover Cluster (Infrastructure) Configuration". The difference is that in the configuration described in this section, OracleAS Single Sign-On and Oracle Delegated Administration Services run in an OracleAS Cold Failover Cluster configuration.

You need two sets of clustered nodes. See Figure 8–5. One set runs the OracleAS Metadata Repository and Oracle Internet Directory, and another set runs Oracle Delegated Administration Services and OracleAS Single Sign-On.

For each set, you need a shared storage and a virtual hostname. You install Oracle homes for the various Oracle Application Server components on the shared storage.

Figure 8–5 Oracle Delegated Administration Services and OracleAS Single Sign-On in a Cold Failover Cluster



8.7.1 Oracle Delegated Administration Services and OracleAS Single Sign-On in OracleAS Cold Failover Cluster: Overview of Installation Steps

Table 8–8 Overview of Steps for Installing Oracle Delegated Administration Services and OracleAS Single Sign-On in an OracleAS Cold Failover Cluster

	Step	Description
1.	Perform Pre-Installation Steps	Pre-installation tasks, described in Section 8.2, include: ▪ Section 8.2.1, "Map the Virtual Hostname and Virtual IP Address". You need two sets of virtual hostnames: one set for OracleAS Metadata Repository and Oracle Internet Directory, and a second set for Oracle Delegated Administration Services and OracleAS Single Sign-On. ▪ Section 8.2.2, "Set Up a File System That Can Be Mounted from Both Nodes". You need two shared disks, one for each set of nodes. ▪ Section 8.2.3, "Review Recommendations for Automatic Storage Management (ASM)"
2.	(optional) Create staticports.ini Files	If you wish, create two staticports.ini files, one for each set of nodes.
3.	Install OracleAS Metadata Repository and Oracle Internet Directory	From node 1, install OracleAS Metadata Repository and Oracle Internet Directory on the shared disk. The steps are the same as those listed in step 2, "Install OracleAS Infrastructure" on page 8-8, except that in the Select Configuration Options screen, do not select **OracleAS Single Sign-On** and **Oracle Application Server Delegated Administration Services**.
4.	Install Oracle Delegated Administration Services and OracleAS Single Sign-On from Node 3	From node 3, install Oracle Delegated Administration Services and OracleAS Single Sign-On on the shared disk.
5.	Stop the OracleAS Infrastructure Processes on Node 1	From node 1, stop the OracleAS Infrastructure processes.
6.	Stop the OracleAS Infrastructure Processes on Node 3	From node 1, stop the OracleAS Infrastructure processes.
7.	Perform Post-Installation Steps	This post-installation step configures the CSS daemon. This step is required only if you are using ASM (Automatic Storage Management) feature of the Oracle database, and you do not have an existing Oracle database.

8.7.2 Oracle Delegated Administration Services and OracleAS Single Sign-On in OracleAS Cold Failover Cluster: Details of Installation Steps

Step 1 Perform Pre-Installation Steps

Perform the pre-installation steps listed in Section 8.2, "Pre-Installation Steps for OracleAS Cold Failover Cluster".

Step 2 (optional) Create staticports.ini Files

If you wish, you may set up two staticports.ini files, one for each set of nodes. For information on staticports.ini, see Section 2.6.3, "Using Custom Port Numbers (the "Static Ports" Feature)".

Step 3 Install OracleAS Metadata Repository and Oracle Internet Directory

Install OracleAS Metadata Repository and Oracle Internet Directory in the same Oracle home by selecting **Identity Management and OracleAS Metadata Repository** in the Select Installation Type screen. This option creates a new database for the OracleAS Metadata Repository and a new Oracle Internet Directory.

The steps are the same as those listed in step 2, "Install OracleAS Infrastructure" on page 8-8, with these differences:

- In the Select Configuration Options screen, select these components/options:
  - **Oracle Internet Directory**
  - **Oracle Directory Integration Platform**
  - **High Availability and Replication**

  Do not select these components:
  - **Oracle Application Server Single Sign-On**
  - **Oracle Application Server Delegated Administration Services**
  - **Oracle Application Server Certificate Authority (OCA)**
- In the Specify Port Configuration Options screen, select **Manual** and enter the fullpath to the staticports.ini file that you created in the previous step.

Step 4 Install Oracle Delegated Administration Services and OracleAS Single Sign-On from Node 3

From node 3, install Oracle Delegated Administration Services and OracleAS Single Sign-On on the shared disk by following the steps in Table 8–9.

Key Points

- When the installer prompts you for the Oracle home path, enter a path on the shared disk. Make sure that both nodes can access this path.
- In the Select High Availability or Replication Option screen, select **Virtual Host**.
- In the Specify Virtual Hostname screen, enter the virtual hostname.

Table 8–9 Installing Oracle Delegated Administration Services and OracleAS Single Sign-On

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Note: In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Do not select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services**. Do not select **Oracle Directory Integration Platform**. Do not select **Oracle Application Server Certificate Authority (OCA)**. Select **High Availability and Replication**. Click **Next**.

Table 8–9 (Cont.) Installing Oracle Delegated Administration Services and OracleAS Single Sign-On

	Screen	Action
3.	Specify Port Configuration Options	Select **Manual** and enter the fullpath to your staticports.ini file in the provided field. You created the staticports.ini file in step 2, "(optional) Create staticports.ini Files" on page 8-26. Click **Next**.
4.	Select High Availability Option	Select **Virtual Host**, and click **Next**.
5.	Register with Oracle Internet Directory	Enter connect information for the Oracle Internet Directory that you installed earlier. **Hostname**: Enter the virtual hostname to access the Oracle Internet Directory host. **SSL Port**: Enter the SSL port on which Oracle Internet Directory is listening. See Section 4.17, "How to Determine Port Numbers Used by Components" if you do not know the port number. Click **Next**.
6.	Specify Oracle Internet Directory Login	**Username**: Enter the username to log in to the Oracle Internet Directory. **Password**: Enter the password for the username. **Realm**: Enter the realm against which to validate the username. This field appears only if your Oracle Internet Directory has multiple realms. Click **Next**.
7.	Specify Virtual Hostname	**Note:** This is a critical screen when installing in an OracleAS Cold Failover Cluster. If you do not see this screen, check the following: ■ Return to the Select High Availability or Replication Option screen and ensure that you selected **Virtual Host**. ■ Return to the Select Configuration Options screen and ensure that you selected **High Availability and Replication**. **Virtual Hostname**: Enter the virtual hostname for the OracleAS Cold Failover Cluster configuration. Example: `vhost_2.mydomain.com` Click **Next**.
8.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for the instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `sso_das` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
9.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

Step 5 Stop the OracleAS Infrastructure Processes on Node 1

Stop the processes that are running in the Oracle home where you installed the OracleAS Metadata Repository and Oracle Internet Directory.

1. Stop the Application Server Control.

```
prompt> ORACLE_HOME/bin/emctl stop iasconsole
```

2. Stop the components.

```
prompt> ORACLE_HOME/opmn/bin/opmnctl stopall
```

3. Stop the OracleAS Metadata Repository.

   a. Set the ORACLE_HOME environment variable to the OracleAS Infrastructure home.

   b. Set the ORACLE_SID environment variable to the SID of the OracleAS Metadata Repository (for example, `orcl`).

   c. Stop the OracleAS Metadata Repository instance.

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

   d. Stop the listener.

```
prompt> ORACLE_HOME/bin/lsnrctl stop
```

   e. Stop the Oracle Enterprise Manager 10*g* 10*g* Database Control.

```
prompt> ORACLE_HOME/bin/emctl stop dbconsole
```

Step 6 Stop the OracleAS Infrastructure Processes on Node 3

Stop the processes that are running in the Oracle home where you installed Oracle Delegated Administration Services and OracleAS Single Sign-On.

1. Stop the Application Server Control.

```
prompt> ORACLE_HOME/bin/emctl stop iasconsole
```

2. Stop the components.

```
prompt> ORACLE_HOME/opmn/bin/opmnctl stopall
```

Step 7 Perform Post-Installation Steps

The following step is required only if you meet **both** of these requirements:

- You plan to use the Automatic Storage Management (ASM) feature of Oracle Database 10*g* for the OracleAS Metadata Repository.
- Your computer does not have an existing Oracle Database 10*g*.

If you meet these requirements, you need to configure the CSS daemon on the other node. The CSS daemon synchronizes ASM instances with the database instances that use the ASM instances for database file storage.

To configure the CSS daemon:

1. Stop all the processes in the OracleAS Cold Failover Cluster (Infrastructure) home.
2. Stop the CSS daemon. You can do this by running the following command as root.

```
# /etc/init.d/init.cssd stop
```

3. Fail over the IP and the disk to the other node.

4. On the other node, run the following command as root:

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

ORACLE_HOME is where you installed the OracleAS Cold Failover Cluster (Infrastructure).

8.8 Installing Only the OracleAS Metadata Repository in an OracleAS Cold Failover Cluster Environment

This section describes how to install the OracleAS Metadata Repository in a new database (that is, the installer will create a new database for you and populate it with the OracleAS Metadata Repository). You can use this database in an OracleAS Cold Failover Cluster environment.

Prerequisites:

- Check that you have configured a virtual hostname and virtual IP.
- If there is an existing Oracle Application Server 10*g* database on the system where you plan to install OracleAS Metadata Repository, you must perform the steps in Section 8.2.5, "Modify listener.ora file for Existing Database" prior to installation.

Table 8–10 Installing the OracleAS Metadata Repository Only

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: ■ In the Select Installation Type screen, select **Metadata Repository**.
2.	Select Configuration Options	Select **High Availability and Replication**. Click **Next**.
3.	Select High Availability Option	Select **Virtual Host**. Click **Next**.
4.	Register Oracle Application Server Metadata Repository	If you already have an Oracle Internet Directory and know its connect information, select **Yes** and enter the name of the computer where Oracle Internet Directory is running and the port number. See Section 4.17, "How to Determine Port Numbers Used by Components" if you do not know the port number. **Use Only SSL Connections with this Oracle Internet Directory**: Select this option if you want Oracle Application Server components to use only SSL to connect to Oracle Internet Directory. If you do not have an Oracle Internet Directory, or do not know its connect information, select **No**. Click **Next**.
5.	Specify Oracle Internet Directory login	This screen appears only if you selected **Yes** in the previous screen. **Username**: Enter the username for logging into Oracle Internet Directory. The user must belong to the iAS Admins group in Oracle Internet Directory. **Password**: Enter the password. **Realm**: This field appears only if your Oracle Internet Directory contains multiple realms. Enter the name of the realm against which to authenticate the user. Click **Next**.
6.	Specify Virtual Hostname	**Virtual Hostname**: Enter the name of the virtual host. Click **Next**.

Table 8–10 (Cont.) Installing the OracleAS Metadata Repository Only

	Screen	Action
7.	Oracle Database screens	Enter information for the OracleAS Metadata Repository database. See Section 4.29, "Install Fragment: Database Screens".
8.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

8.9 Post-Installation Steps for OracleAS Cold Failover Cluster

- Section 8.9.1, "Edit the ORACLE_HOME/Apache/Apache/htdocs/index.html File"
- Section 8.9.2, "Copy the /var/opt/oracle Directory to the Other Node"
- Section 8.9.3, "Running Database Console against a Cold Failover Cluster Database"
- Section 8.9.4, "Create a Clusterware Agent for Automatic Failover"

8.9.1 Edit the ORACLE_HOME/Apache/Apache/htdocs/index.html File

In the `ORACLE_HOME/Apache/Apache/htdocs/index.html` file, change all occurrences of the physical hostname (example: `node1`) to the virtual hostname (example: `vhost`), where `node1` appears as a hostname.

Note that if `node1` is used as part of the Oracle Application Server instance name, do not change it.

8.9.2 Copy the /var/opt/oracle Directory to the Other Node

After the OracleAS Infrastructure installation is complete, copy the `/var/opt/oracle` directory from the node where you performed the installation to the other node in the OracleAS Cold Failover Cluster. This ensures that you can run the installer to update the Oracle home from either node in the cluster.

Be sure to keep the two `/var/opt/oracle` directories in sync. Whenever you run the installer to update the infrastructure, you need to copy the `oracle` directory to the other node.

The `/var/opt/oracle` directory is not used during runtime by Oracle Application Server. It is used only by the installer.

8.9.3 Running Database Console against a Cold Failover Cluster Database

Before you can start, stop or check the status of Database Console against a cold failover cluster database, you need to set the ORACLE_HOSTNAME environment variable to the virtual hostname. For example, in Figure 8–1, the virtual hostname is vhost.mydomain.com. You would set ORACLE_HOSTNAME as follows:

C shell:

```
$ setenv ORACLE_HOSTNAME vhost.mydomain.com
```

Bourne or Korn shell:

```
% ORACLE_HOSTNAME=vhost.mydomain.com
% export ORACLE_HOSTNAME
```

After setting the variable, you can then run the "`emctl` *`action`* `dbconsole`" commands, where *`action`* is `start`, `stop`, or `status` (for example, `emctl start dbconsole`).

8.9.4 Create a Clusterware Agent for Automatic Failover

An OracleAS Cold Failover Cluster environment provides the framework for a manual failover of OracleAS Infrastructure. To achieve automatic failover, you must set up an agent using the clusterware. An example of automatic failover is setting up the secondary node to monitor the heart beat of the primary node and when the secondary node detects that the primary node is down, the virtual IP address, shared storage, and all the OracleAS Infrastructure processes are failed over to the secondary node.

8.10 Installing Middle Tiers Against an OracleAS Cold Failover Cluster Infrastructure

This section describes how to install middle tiers that are not in a cold failover cluster configuration against an OracleAS Cold Failover Cluster infrastructure.

For non-cold failover cluster middle tiers to work with OracleAS Infrastructure in an OracleAS Cold Failover Cluster, you can install the middle tiers on computers outside the cluster, or on nodes within the cluster.

Note: The preferred solution is to install and run the non-cold failover cluster middle tiers on nodes outside the OracleAS Cold Failover Cluster.

8.10.1 If You Plan to Install Middle Tiers on OracleAS Cold Failover Cluster Nodes

If you plan to install a non-cold failover cluster middle tier on an OracleAS Cold Failover Cluster node (primary or secondary), perform these tasks before installing the middle tier:

- Section 8.10.1.1, "Create a staticports.ini File for the Middle Tier"
- Section 8.10.1.2, "Rename the /var/opt/oracle Directory Used for the Infrastructure"

8.10.1.1 Create a staticports.ini File for the Middle Tier

Ensure that the ports used by the middle tier are not the same as the ports used by the infrastructure. The reason is that the infrastructure can fail over from the primary to the secondary node (and vice versa), and there must not be any port conflicts on either node. The same ports must be reserved for the infrastructure on both nodes.

If the infrastructure is running on the same node where you want to install the middle tier, the installer can detect which ports are in use and select different ports for the middle tier. For example, if the infrastructure is running on the primary node, and you run the installer on the primary node to install the middle tier, then the installer can assign different ports for the middle tier.

However, if the infrastructure is running on a node different from where you want to install the middle tier, the installer cannot detect which ports are used by the

infrastructure. For example, if the infrastructure is running on the primary node but you want to install the middle tier on the secondary node, the installer is unable to detect which ports the infrastructure is using. In this situation, you need to set up a `staticports.ini` file to specify port numbers for the middle tier. See Section 2.6.3, "Using Custom Port Numbers (the "Static Ports" Feature)" for details.

To see which ports the infrastructure is using, view the `ORACLE_HOME/install/portlist.ini` file, where ORACLE_HOME refers to the directory where you installed the infrastructure.

8.10.1.2 Rename the /var/opt/oracle Directory Used for the Infrastructure

Set up the environment so that the middle tier will have its own inventory directory, instead of using the same inventory directory used by the infrastructure. To do this, you need to rename the `/var/opt/oracle` directory to something else so that the installer will prompt you to enter a new inventory directory. The following example renames it to `oracle.infra`.

```
prompt> su
Password: root_password
# cd /var/opt
# mv oracle oracle.infra
```

When the installer prompts for the inventory directory, specify a directory on the local storage or on a disk other than the one where you installed the OracleAS Infrastructure.

When the middle-tier installation is complete, do the following rename operations:

```
prompt> su
Password: root_password
# cd /var/opt
# mv oracle oracle.mt see (1)
# mv oracle.infra oracle see (2)
```

(1) This command renames the `oracle` directory created by the installer when it installed the middle tier.

(2) This command renames the `oracle.infra` directory back to `oracle`.

The `/var/opt/oracle directory` is not used during Oracle Application Server runtime. The only time you need it is when you run the installer (for example, to de-install an instance or to expand an instance).

Be sure the correct `oracle` directory is in place before you run the installer.

8.10.2 Procedure for Installing Middle Tiers Against an OracleAS Cold Failover Cluster Infrastructure

To install middle tiers against OracleAS Infrastructure in an OracleAS Cold Failover Cluster, follow the middle tier installation procedures as documented in *Oracle Application Server Installation Guide* for the middle tier release, but with these differences:

- In the Register with Oracle Internet Directory screen, enter the virtual hostname in the **Hostname** field.
- If you are installing the middle tier on an OracleAS Cold Failover Cluster node, you must follow these additional requirements:

- Read Section 8.10.1, "If You Plan to Install Middle Tiers on OracleAS Cold Failover Cluster Nodes".

8.11 Installing Regular Middle-Tiers on OracleAS Cold Failover Cluster Nodes

If you install middle-tiers that are not in a cold failover cluster configuration on the same nodes as an OracleAS Cold Failover Cluster infrastructure, then the ports used for the middle tiers must be different from the ones used for any OracleAS Infrastructure installed on the same cluster. The ports must also be different from those used for other Oracle Homes on the same node. To check the ports assigned to components in any Oracle Home, see the Ports page on the Application Server Control Console.

When you install the middle-tiers, you should use a `staticports.ini` file. See Section 2.6.3, "Using Custom Port Numbers (the "Static Ports" Feature)" for details.

9

Installing in High Availability Environments: OracleAS Cluster (Identity Management)

This chapter describes how to install Oracle Application Server in OracleAS Cluster (Identity Management) configurations.

- Section 9.1, "OracleAS Cluster (Identity Management): Introduction"
- Section 9.2, "Pre-Installation Steps for OracleAS Cluster (Identity Management)"
- Section 9.3, "About Oracle Internet Directory Passwords"
- Section 9.4, "About Configuring SSL and Non-SSL Ports for Oracle HTTP Server"
- Section 9.5, "Installing an OracleAS Cluster (Identity Management) Configuration"
- Section 9.6, "Installing a Distributed OracleAS Cluster (Identity Management) Configuration"
- Section 9.7, "Post-Installation Steps"
- Section 9.8, "Installing Middle Tiers Against OracleAS Cluster (Identity Management) Configurations"

9.1 OracleAS Cluster (Identity Management): Introduction

In OracleAS Cluster (Identity Management) configurations, the Oracle Identity Management components and the OracleAS Metadata Repository run on separate nodes. All the nodes in an OracleAS Cluster (Identity Management) configuration are active. Requests from clients, such as middle tiers, are directed to a load balancer, which then directs the requests to one of the active nodes. See Figure 9–1.

These nodes can belong to a hardware cluster, but this is not required.

These configurations are called "OracleAS Cluster (Identity Management)" because the OracleAS Single Sign-On and Oracle Delegated Administration Services components are clustered. This means that these components are configured identically across nodes.

Database (OracleAS Metadata Repository) Requirement

You need an existing OracleAS Metadata Repository before installing an OracleAS Cluster (Identity Management) configuration. You can install OracleAS Metadata Repository in one of the following methods:

- Install OracleAS Metadata Repository in a new database by using the Oracle Application Server installer.

- Install the OracleAS Metadata Repository in an existing database using the OracleAS RepCA. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for supported database configurations.

For OracleAS Cluster (Identity Management) configurations, Oracle recommends using a high availability database configuration such as Real Application Clusters or cold failover cluster.

You can only install one OracleAS Cluster (Identity Management) on an OracleAS Metadata Repository.

Note: For OracleAS Cluster (Identity Management) configurations, you never select the "**Oracle Identity Management and OracleAS Metadata Repository**" option in the installer. You always select the **Oracle Identity Management** option. This is why you need an existing OracleAS Metadata Repository.

Always Select the Same Components

Because the installer clusters the components in an OracleAS Cluster (Identity Management) configuration, you need to select the same components in the Select Configuration Options screen for all the nodes in the cluster.

For example, if you select Oracle Internet Directory, OracleAS Single Sign-On, and Oracle Delegated Administration Services for the installation on node 1, then you have to select the same set of components in subsequent installations.

Clustering will fail if you select different components in each installation.

Configurations

You can install OracleAS Cluster (Identity Management) in these configurations:

- OracleAS Cluster (Identity Management). See Section 9.5.
- Distributed OracleAS Cluster (Identity Management). See Section 9.6.

9.2 Pre-Installation Steps for OracleAS Cluster (Identity Management)

Before installing an OracleAS Cluster (Identity Management) configuration, you need to set up the following items:

- Section 9.2.1, "Use the Same Path for the Oracle Home Directory (recommended)"
- Section 9.2.2, "Synchronize Clocks on All Nodes"
- Section 9.2.3, "Configure Virtual Server Names and Ports for the Load Balancer"
- Section 9.2.4, "Configure Your LDAP Virtual Server"

9.2.1 Use the Same Path for the Oracle Home Directory (recommended)

For all the nodes that will be running Oracle Identity Management components, use the same full path for the Oracle home. This practice is recommended, but not required.

9.2.2 Synchronize Clocks on All Nodes

Synchronize the system clocks on all nodes so they are running within 250 seconds of each other. When synchronizing the system clocks, make sure the clocks are set to the same time zone.

Note: If you do not synchronize the clocks, then there will be inconsistent operation attributes in the directory entries and inconsistent behavior of the password state policies. As a result, you will see unwanted instance failovers.

9.2.3 Configure Virtual Server Names and Ports for the Load Balancer

Configure your load balancer with two virtual server names and associated ports:

- Configure a virtual server name for LDAP connections. For this virtual server, you need to configure a port for SSL connections.

  Note: It is recommended that the same port you configured for SSL connections on the LDAP virtual server is configured as the SSL port for Oracle Internet Directory on the nodes on which you will be installing Oracle Internet Directory.

- Configure a virtual server name for HTTP connections. For this virtual server, you also need to configure a port for either SSL or non-SSL connections. If you want the client to connect to the load balancer using HTTPS, configure a port for SSL connections. If you want the client to connect to the load balancer using HTTP, configure a port for non-SSL connections.

  Note: The ports for the HTTP virtual server can be different from the Oracle HTTP Server `Listen` ports.

The installer will prompt you for the virtual server names and port numbers. Enter the same virtual server name in the installer that you used to configure the LDAP and HTTP virtual servers. The virtual server name may or may not be fully-qualified. For example, if you used a fully-qualified host name when you configured the LDAP virtual server, then you must enter the same fully-qualified host name in the installer.

Note: The installer does not check the load balancer. Make sure the load balancer is properly configured and enabled before running the installer.

In addition, check the following:

- Check that the virtual server names are associated with IP addresses and are part of your DNS. The nodes that will be running Oracle Application Server must be able to resolve these virtual server names.

9.2.4 Configure Your LDAP Virtual Server

Configure the LDAP virtual server on your load balancer to direct requests to node 1 initially. The procedure to add additional nodes differs depending upon whether or not your load balancer supports LDAP service monitoring.

Note that these procedures apply only to the LDAP virtual server configured on your load balancer. They do not apply to the HTTP virtual server configured on your load balancer.

9.2.4.1 Load Balancer Supports LDAP Service Monitoring

If your load balancer supports LDAP service monitoring, then you can add all the nodes to the LDAP virtual server before starting the installation.

For example, if you have three nodes:

1. Configure the LDAP virtual server to direct requests to node 1 only.
2. Add node 2 to the LDAP virtual server.
3. Add node 3 to the LDAP virtual server.
4. Install Oracle Identity Management components on node 1.
5. Install Oracle Identity Management components on node 2.
6. Install Oracle Identity Management components on node 3.

9.2.4.2 Load Balancer Does Not Support LDAP Service Monitoring

If your load balancer does not support LDAP service monitoring, then configure your LDAP virtual server to direct requests to node 1 only before starting the installation. After you complete an installation on a node, then you can add that node to the virtual server.

For example, if you have three nodes:

1. Configure the LDAP virtual server to direct requests to node 1 only.
2. Install Oracle Identity Management components on node 1.
3. Install Oracle Identity Management components on node 2.
4. Add node 2 to the LDAP virtual server.
5. Install Oracle Identity Management components on node 3.
6. Add node 3 to the LDAP virtual server.

9.3 About Oracle Internet Directory Passwords

In OracleAS Cluster (Identity Management) configurations, you install Oracle Internet Directory on multiple nodes, and in each installation, you enter the instance password in the "Specify Instance Name and ias_admin Password" screen.

The password specified in the first installation is used as the password for the `cn=orcladmin` and `orcladmin` users not just in the first Oracle Internet Directory, but in all Oracle Internet Directory installations in the cluster.

This means that to access the Oracle Internet Directory on any node, you have to use the password that you entered in the first installation. You cannot use the passwords that you entered in subsequent installations.

Accessing the Oracle Internet Directory includes:

- Logging into Oracle Delegated Administration Services (URL: `http://`*`hostname`*`:`*`port`*`/oiddas`)
- Logging into OracleAS Single Sign-On (URL: `http://`*`hostname`*`:`*`port`*`/pls/orasso`)

- Connecting to Oracle Internet Directory using the Oracle Directory Manager

You still need the passwords that you entered in subsequent installations for logging into Application Server Control.

9.4 About Configuring SSL and Non-SSL Ports for Oracle HTTP Server

When you are installing OracleAS Cluster (Identity Management) configurations, the installer displays the "Specify HTTP Load Balancer Host and Listen Ports" screen.

This screen has two sections:

- In the load balancer section, you specify the load balancer's HTTP virtual server name and port number. You also indicate whether the port is for SSL or non-SSL requests.
- In the Oracle HTTP Server section, you specify the port number that you want for the Oracle HTTP Server `Listen` port. You also indicate whether the port is for SSL or non-SSL requests.

  The virtual server and the Oracle HTTP Server `Listen` port can use different port numbers.

You use this screen to set up the type of communication (SSL or non-SSL) between client, load balancer, and Oracle HTTP Server. Three cases are possible:

- Case 1: Communications between clients and the load balancer use HTTP, and communications between the load balancer and Oracle HTTP Server also use HTTP. See Section 9.4.1, "Case 1: Client ---[HTTP]---> Load Balancer ---[HTTP]---> Oracle HTTP Server".
- Case 2: Communications between clients and the load balancer use HTTPS, and communications between the load balancer and Oracle HTTP Server also use HTTPS. See Section 9.4.2, "Case 2: Client ---[HTTPS]---> Load Balancer ---[HTTPS]---> Oracle HTTP Server".
- Case 3: Communications between clients and the load balancer use HTTPS, but communications between the load balancer and Oracle HTTP Server use HTTP. See Section 9.4.3, "Case 3: Client ---[HTTPS]---> Load Balancer ---[HTTP]---> Oracle HTTP Server".

Note: Because the values you specify in this dialog override the values specified in the staticports.ini file, you should not specify port numbers for the Oracle HTTP Server `Listen` port in the staticports.ini file.

9.4.1 Case 1: Client ---[HTTP]---> Load Balancer ---[HTTP]---> Oracle HTTP Server

HTTP Listener: Port: Enter the port number that you want to use as the Oracle HTTP Server `Listen` port. This will be the value of the `Listen` directive in the `httpd.conf` file.
Enable SSL: Do not select this option. The installer tries the default port number for the SSL port.

HTTP Load Balancer: Hostname: Enter the name of the virtual server on the load balancer configured to handle HTTP requests.

HTTP Load Balancer: Port: Enter the port number that the HTTP virtual server listens on. This will be the value of the `Port` directive in the `httpd.conf` file.
Enable SSL: Do not select this option.

Example

Table 9–1 Example for Case 1

Values in Screen	Resulting Values in Configuration Files

HTTP Listener: Port: 8000
Enable SSL: Unchecked
HTTP Load Balancer: Port: 80
Enable SSL: Unchecked
	In **`httpd.conf`**:
	`Port 80`
	`Listen 8000`
	
	In **`ssl.conf`**:
	`Port <default port number assigned by installer>`
	`Listen <default port number assigned by installer>`

9.4.2 Case 2: Client ---[HTTPS]---> Load Balancer ---[HTTPS]---> Oracle HTTP Server

HTTP Listener: Port: Enter the port number that you want Oracle HTTP Server to listen on. This will be the value of the `Listen` directive in the `ssl.conf` file.
Enable SSL: Select this option.

HTTP Load Balancer: Hostname: Enter the name of the virtual server on the load balancer configured to handle HTTPS requests.

HTTP Load Balancer: Port: Enter the port number that the HTTP virtual server listens on. This will be the value of the `Port` directive in the `ssl.conf` file.
Enable SSL: This option has been automatically selected and cannot be deselected. This is because you selected **Enable SSL** for the HTTP Listener.

In `opmn.xml`, the installer sets the `ssl-enabled` line in the Oracle HTTP Server section to `true`.

Example

Table 9–2 Example for Case 2

Values in Screen	Resulting Values in Configuration Files

HTTP Listener: Port: 90
Enable SSL: Checked
HTTP Load Balancer: Port: 443
Enable SSL: Checked
	In **`httpd.conf`**:
	`Port <default port number assigned by installer>`
	`Listen <default port number assigned by installer>`
	
	In **`ssl.conf`**:
	`Port 443`
	`Listen 90`

Note that in this case you will have to perform an additional post-configuration step. See Section 9.7.3, "Update targets.xml (Case 2 only)".

9.4.3 Case 3: Client ---[HTTPS]---> Load Balancer ---[HTTP]---> Oracle HTTP Server

HTTP Listener: Port: Enter the port number that you want Oracle HTTP Server to listen on. This will be the value of the `Listen` directive in the `httpd.conf` file.
Enable SSL: Do not select this option.

HTTP Load Balancer: Hostname: Enter the name of the virtual server on the load balancer configured to handle HTTPS requests.

HTTP Load Balancer: Port: Enter the port number that the HTTP virtual server listens on. This will be the value of the `Port` directive in the `httpd.conf` file.
Enable SSL: Select this option.

Note that in this configuration, the load balancer must have SSL acceleration capabilities, or you must add a separate SSL Accelerator. The conversion from HTTPS to HTTP happens before Oracle HTTP Server receives the request. The SSL accelerator must be properly configured prior to installation. The installer does not check for this.

The installer will change the following lines:

- In `opmn.xml`, the installer sets the `ssl-enabled` line in the Oracle HTTP Server section to `true`.
- In `httpd.conf`, the installer adds the following lines:

```
LoadModule certheaders_module libexec/mod_certheaders.so
SimulateHttps on
```

Example

Table 9–3 Example for Case 3

Values in Screen	Resulting Values in Configuration Files

HTTP Listener: Port: 9000
Enable SSL: Unchecked
HTTP Load Balancer: Port: 443
Enable SSL: Checked
	In **`httpd.conf`**:
	`Port 443`
	`Listen 9000`
	
	In **`ssl.conf`**:
	`Port <default port number assigned by installer>`
	`Listen <default port number assigned by installer>`

9.5 Installing an OracleAS Cluster (Identity Management) Configuration

In this configuration, you need an existing database that is already running in a configuration supported by the OracleAS RepCA. Oracle recommends running the database in a high availability environment, such as a Real Application Clusters database. You also need additional nodes (at least two nodes) to run Oracle Identity Management components. In this configuration, Oracle Internet Directory, OracleAS Single Sign-On, and Oracle Delegated Administration Services run on each node. If you want to distribute these components, see Section 9.6, "Installing a Distributed OracleAS Cluster (Identity Management) Configuration".

These nodes are accessed through a load balancer. See Figure 9–1.

You install the OracleAS Metadata Repository in your existing database, then install Oracle Identity Management components against this database.

Oracle Directory Integration Platform Is Started on the First Node Only

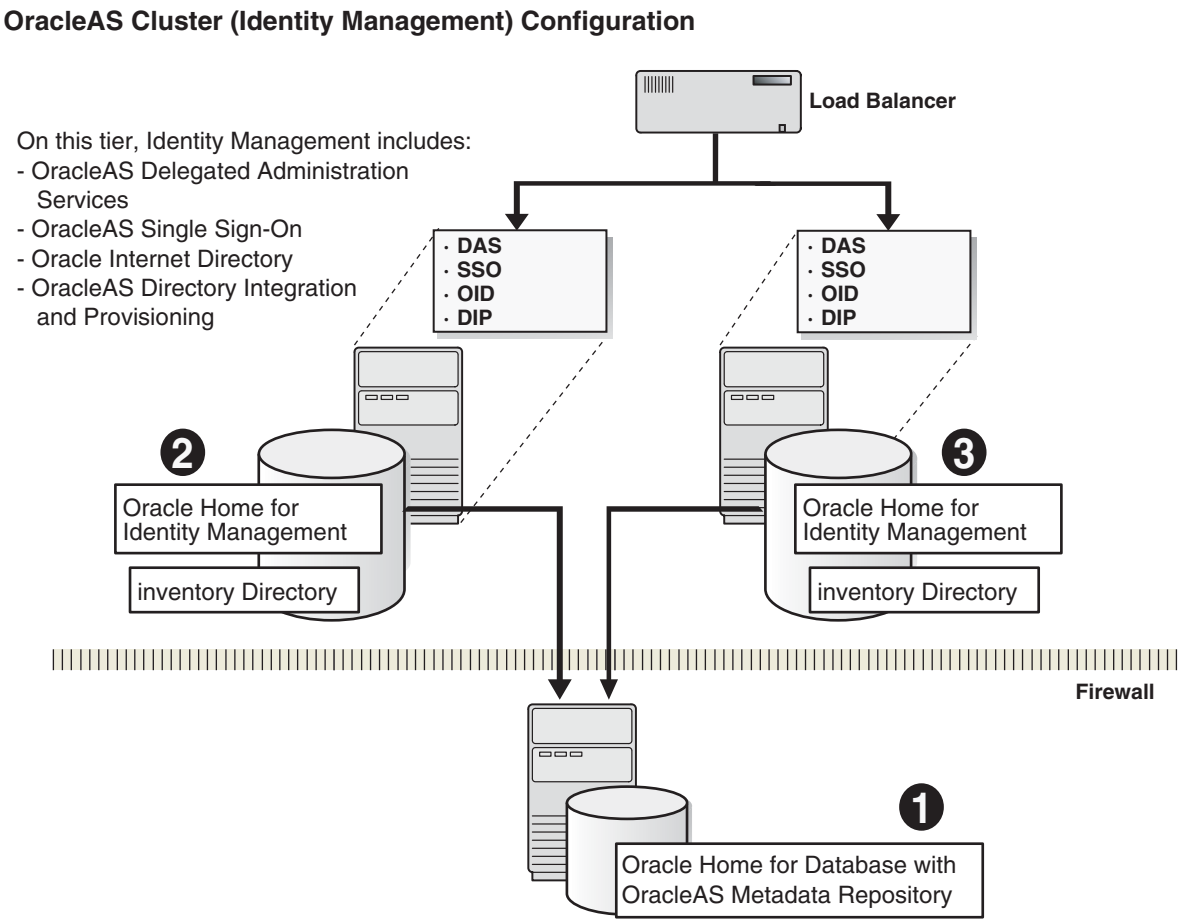
The installer starts Oracle Directory Integration Platform only on the first node, even though you selected it on subsequent nodes as well. On subsequent nodes, the installer configures Oracle Directory Integration Platform, but does not start it.

If You Want Oracle Internet Directory to Listen on SSL Ports Only

If you want Oracle Internet Directory to listen on SSL ports only, perform this configuration after you have installed Oracle Identity Management. You need Oracle

Internet Directory to be listening on both SSL and non-SSL ports when you install OracleAS Single Sign-On and Oracle Delegated Administration Services.

Figure 9–1 OracleAS Cluster (Identity Management) Configuration



Subsections:

- Section 9.5.1, "Installation Order"
- Section 9.5.2, "Installing OracleAS Metadata Repository"
- Section 9.5.3, "Installing OracleAS Cluster (Identity Management) on the First Node"
- Section 9.5.4, "Installing OracleAS Cluster (Identity Management) on Subsequent Nodes"

9.5.1 Installation Order

To create an OracleAS Cluster (Identity Management) configuration:

1. Install the OracleAS Metadata Repository in your existing database.
2. Install the Oracle Identity Management on each node. You run the installer on each node separately.

> **Note:** If you want to configure Oracle Internet Directory to listen on SSL ports only, perform this configuration *after* you have installed Oracle Identity Management. Oracle Internet Directory needs to be listening on both SSL and non-SSL ports when you install OracleAS Single Sign-On and Oracle Delegated Administration Services.

3. Install middle tiers.

9.5.2 Installing OracleAS Metadata Repository

To install the OracleAS Metadata Repository in your existing database, you use the OracleAS RepCA. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

9.5.3 Installing OracleAS Cluster (Identity Management) on the First Node

Run the installer on each node where you want to install Oracle Identity Management components.

Note that the procedure for installing Oracle Identity Management components on the first node is different from installing the components on subsequent nodes. To install the components on subsequent nodes, see Section 9.5.4, "Installing OracleAS Cluster (Identity Management) on Subsequent Nodes".

Subsections:

- Section 9.5.3.1, "Create staticports.ini File"
- Section 9.5.3.2, "Disable TCP Monitoring on Load Balancer for First Node"
- Section 9.5.3.4, "Ensure that the OracleAS Metadata Repository Is Not Registered with any Oracle Internet Directory"
- Section 9.5.3.5, "Select the Same Components for Each Node"
- Section 9.5.3.6, "Run the Installer"

9.5.3.1 Create staticports.ini File

If you want to use custom ports for components other than Oracle HTTP Server or Oracle Internet Directory, you need to create a staticports.ini file for this installation.

If you want custom ports for Oracle HTTP Server or Oracle Internet Directory, you specify them in the "Specify HTTP Load Balancer Host and Listen Ports" and the "Specify Host and Port for LDAP" screens.

If you specify custom ports for Oracle HTTP Server and Oracle Internet Directory also in the staticports.ini file, and you also specify ports in the screens mentioned above, the ports specified in the screens take precedence.

To avoid specifying Oracle HTTP Server and Oracle Internet Directory ports in the staticports.ini file, the staticports.ini file **must not contain these lines**:

```
Oracle HTTP Server port = port_num
Oracle HTTP Server Listen port = port_num
Oracle HTTP Server SSL port = port_num
Oracle HTTP Server Listen (SSL) port = port_num
Oracle Internet Directory port = port_num
Oracle Internet Directory (SSL) port = port_num
```

If you have a staticports.ini file, you should also use the same file for installations on subsequent nodes.

9.5.3.2 Disable TCP Monitoring on Load Balancer for First Node

Before installing on the first node, you must make sure that TCP monitoring is not enabled for the Virtual IP on the first node.

9.5.3.3 Configure the Load Balancer to Return Immediately to the Calling Client

It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the backend services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.

If your load balancer is not configured this way, the Java Security Configuration Assistant may report the following:

```
WARNING: DCM service may not be available at this time to synchronize $ORACLE_
HOME/j2ee/home/config/jazn-data.xml file.
```

Refer to Section F.3.19, "WARNING: DCM service may not be available at this time" for information on how to correct this problem after the installation is finished.

> **See Also:** The *Oracle Application Server High Availability Guide* for more information on load balancer requirements.

9.5.3.4 Ensure that the OracleAS Metadata Repository Is Not Registered with any Oracle Internet Directory

When you perform the installation on the first node, you need to specify an OracleAS Metadata Repository that is not registered with any Oracle Internet Directory. The installer checks for this. If the installer finds that the OracleAS Metadata Repository is already registered with an Oracle Internet Directory, then it assumes that you are installing on subsequent nodes, and that you want to join the cluster that was created when you installed on the first node. It prompts you for the existing cluster name, and the connect information for the Oracle Internet Directory.

9.5.3.5 Select the Same Components for Each Node

You must select the same components in the Select Configuration Options screen when installing on each node. For example, if you select Oracle Internet Directory, OracleAS Single Sign-On, and Oracle Delegated Administration Services on the first node, you must select these same set of components on subsequent nodes.

9.5.3.6 Run the Installer

Follow the steps in Table 9–4.

Key Points for Installing on the First Node

- In the Select Configuration Options screen, select **High Availability and Replication**, in addition to selecting the components.
- In the Select High Availability or Replication Option screen, select **OracleAS Cluster (Identity Management)**.

Table 9–4 Steps for Installing OracleAS Cluster (Identity Management) on the First Node

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: In the Select Installation Type screen, select **Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform**. Do not select **Oracle Application Server Certificate Authority (OCA)**. Select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	Select **Manual** and enter the fullpath to your staticports.ini file in the provided field. You need to use staticports.ini file for OracleAS Cluster (Identity Management) configurations. See Section 9.5.3.1, "Create staticports.ini File". Click **Next**.
4.	Specify Repository	When you install on the first node, you need to specify an OracleAS Metadata Repository that is not registered with an Oracle Internet Directory. When you install on subsequent nodes, then the OracleAS Metadata Repository is registered with the Oracle Internet Directory on the first node. **Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the names of all the nodes where the Real Application Clusters database is running, and the port numbers. Use the format: `host1.domain.com:port1, host2.domain.com:port2, ...` **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Select High Availability or Replication Option	Select **OracleAS Cluster (Identity Management)**, and click **Next**.
6.	Specify New Oracle Application Server Clusters Name	Enter a name for the new OracleAS Cluster (Identity Management). Note that the cluster name is case-sensitive. Oracle recommends that you record the cluster name for use during installations on subsequent nodes. Example: `cluster1` Click **Next**.
7.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.

Table 9–4 (Cont.) Steps for Installing OracleAS Cluster (Identity Management) on the First Node

	Screen	Action
8.	Specify Host and Port for LDAP	The values you enter in this screen depend on your scenario. There are two possible scenarios: Scenario 1: You have configured a virtual server on your load balancer to handle LDAP traffic from Oracle Delegated Administration Services and OracleAS Single Sign-On to Oracle Internet Directory. Scenario 2: You do not have a load balancer. **Hostname**: In scenario 1, enter the name of the virtual server in this field. Enter the same virtual server name that you configured on the load balancer. In scenario 2, if the Oracle Internet Directory is highly available, enter the virtual hostname of the computer running Oracle Internet Directory. For Oracle Internet Directory deployments that are not highly available, enter the physical hostname of the computer running Oracle Internet Directory. Notes on the port values for scenario 2 (see Section 9.2.3, "Configure Virtual Server Names and Ports for the Load Balancer" for details): ▪ The same port numbers will be used for the Oracle Internet Directory on subsequent nodes. **SSL Port**: In scenario 1, enter the port configured on the virtual server to handle SSL LDAP connections. In scenario 2, enter the port that you want Oracle Internet Directory to use for SSL connections. The standard port number for SSL LDAP connections is 636, but you can use any port that you want. Click **Next**.
9.	Specify HTTP Listen Port, Load Balancer Host and Port	See Section 9.4, "About Configuring SSL and Non-SSL Ports for Oracle HTTP Server" for details. **HTTP Listener: Port**: Enter the port number that you want Oracle HTTP Server to listen on. **Enable SSL**: Select this option if you want to configure Oracle HTTP Server for SSL on this port. **HTTP Load Balancer: Hostname**: Enter the name of the HTTP virtual server configured on your load balancer. Enter the same virtual server name that you configured on the load balancer. **HTTP Load Balancer: Port**: Enter the port for the HTTP virtual server. **Enable SSL**: Select this option if this port is for SSL communications only. Click **Next**.
10.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `id_mgmt` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
11.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

9.5.4 Installing OracleAS Cluster (Identity Management) on Subsequent Nodes

You run the installer on each node where you want to install Oracle Identity Management components. Use this procedure to install Oracle Identity Management components on nodes other than the first. For the first node, see Section 9.5.3, "Installing OracleAS Cluster (Identity Management) on the First Node".

Key Points for Installing on Subsequent Nodes

- Use the same staticports.ini file that you used for installing on the first node to ensure that the same component on all nodes uses the same port number.

  Note that the Oracle Internet Directory ports specified in staticports.ini will not be used by the installer. The installer queries the first Oracle Identity Management installation for the Oracle Internet Directory ports.

- In the Specify HTTP Load Balancer Host and Ports screen, enter the name of the HTTP virtual server of the load balancer, and the associated port. You also enter the port number for Oracle HTTP Server on this screen.

Follow the steps in Table 9–5.

Table 9–5 Steps for Installing OracleAS Cluster (Identity Management) on Subsequent Nodes

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform**. Do not select **Oracle Application Server Certificate Authority (OCA)**. Select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	Select **Manual** and enter the fullpath to your staticports.ini file in the provided field. You need to use staticports.ini file for OracleAS Cluster (Identity Management) configurations. See Section 9.5.3.1, "Create staticports.ini File". Click **Next**.
4.	Specify Repository	Specify the OracleAS Metadata Repository that is registered with the Oracle Internet Directory on the first node. **Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the names of all the nodes where the Real Application Clusters database is running, and the port numbers. Use the format: `host1.domain.com:port1, host2.domain.com:port2, ...` **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Warning	This warning reminds you that you are installing this instance as part of an OracleAS Cluster (Identity Management), and that you need to synchronize the clocks on the nodes in the cluster. See Section 9.2.2, "Synchronize Clocks on All Nodes". Click **OK**.

Table 9–5 (Cont.) Steps for Installing OracleAS Cluster (Identity Management) on Subsequent Nodes

	Screen	Action
6.	Specify Existing Oracle Application Server Clusters Name	Specify an existing OracleAS Cluster (Identity Management) for the current instance to join. The cluster was created during a previous identical installation. Note that the cluster name is case-sensitive. Example: `cluster1` Click **Next**.
7.	Specify ODS Password	Enter the password for the ODS schema in the OracleAS Metadata Repository. The ODS schema is the main schema used by Oracle Internet Directory. By default, the ODS password is the same as the ias_admin password (the password that you entered in the Specify Instance Name and ias_admin Password screen). Click **Next**.
8.	Specify Host and Port for LDAP	The values you enter on this screen are the same as the values you entered when you did the installation on the first node. The installer uses these values to connect to the Oracle Internet Directory on the first node. **Hostname**: Enter the LDAP virtual server name of the load balancer. Enter the same virtual server name that you configured on the load balancer. **SSL Port**: Enter the port configured on this load balancer to handle LDAP SSL connections. Click **Next**.
9.	Warning	This warning reminds you to setup the LDAP virtual server to direct requests to existing OracleAS Cluster (Identity Management) nodes, and then add this node to the LDAP virtual server after installation. See Section 9.2.4, "Configure Your LDAP Virtual Server". Click **OK**.
10.	Specify Oracle Internet Directory Login	**Username**: Enter the username to log in to Oracle Internet Directory. You need to log in as the Oracle Internet Directory superuser (`cn=orcladmin`). **Password**: Enter the password for the username. **Realm**: Enter the realm against which to validate the username. This field appears only if your Oracle Internet Directory has multiple realms. Click **Next**.
11.	Specify HTTP Load Balancer Host and Ports	See Section 9.4, "About Configuring SSL and Non-SSL Ports for Oracle HTTP Server" for details. The values you enter on this screen are the same as the values you entered when you did the installation on the first node. **HTTP Listener: Port**: Enter the port number that you want Oracle HTTP Server to listen on. **Enable SSL**: Select this option if you want to configure Oracle HTTP Server for SSL on this port. **HTTP Load Balancer: Hostname**: Enter the name of the HTTP virtual server configured on your load balancer. Enter the same virtual server name that you configured on the load balancer. **HTTP Load Balancer: Port**: Enter the port for the HTTP virtual server. **Enable SSL**: Select this option if this port is for SSL communications only. Click **Next**.

Table 9–5 (Cont.) Steps for Installing OracleAS Cluster (Identity Management) on Subsequent Nodes

	Screen	Action
12.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `id_mgmt` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
13.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

9.6 Installing a Distributed OracleAS Cluster (Identity Management) Configuration

In this configuration, you need an existing database that is already running in a configuration that is supported by OracleAS RepCA. Oracle recommends running the database in a high availability environment, such as a Real Application Clusters database. This database will contain the OracleAS Metadata Repository.

You also need two nodes to run OracleAS Single Sign-On and Oracle Delegated Administration Services components, and two additional nodes to run Oracle Internet Directory. These nodes are accessed through load balancers. See Figure 9–2.

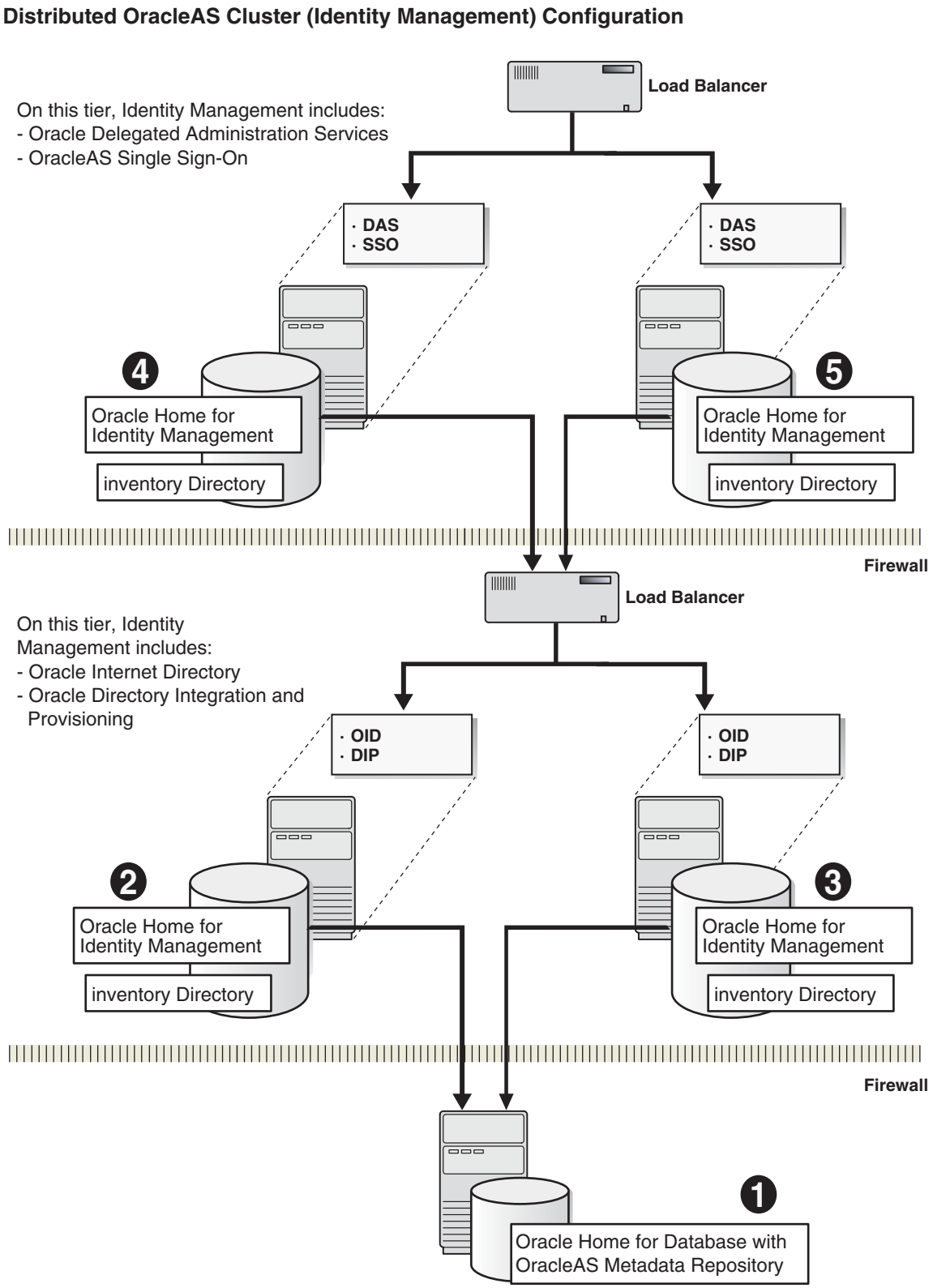
Oracle Directory Integration Platform Is Started on the First Node Only

The installer starts Oracle Directory Integration Platform only on the first node, even though you selected it on subsequent nodes as well. On subsequent nodes, the installer configures Oracle Directory Integration Platform, but does not start it.

If You Want Oracle Internet Directory to Listen on SSL Ports Only

If you want Oracle Internet Directory to listen on SSL ports only, perform this configuration after you have installed OracleAS Single Sign-On and Oracle Delegated Administration Services. You need Oracle Internet Directory to be listening on both SSL and non-SSL ports when you install OracleAS Single Sign-On and Oracle Delegated Administration Services.

Figure 9–2 Distributed OracleAS Cluster (Identity Management) Configuration



Subsections:

- Section 9.6.1, "Installation Order"

- Section 9.6.2, "Installing OracleAS Metadata Repository"
- Section 9.6.3, "Installing Oracle Internet Directory on the First Node"
- Section 9.6.4, "Installing Oracle Internet Directory on Subsequent Nodes"
- Section 9.6.5, "Installing OracleAS Single Sign-On and Oracle Delegated Administration Services on Each Node"

9.6.1 Installation Order

To create a distributed OracleAS Cluster (Identity Management) configuration:

1. Install OracleAS Metadata Repository in your existing database.
2. Install Oracle Internet Directory on each node. You run the installer on each node separately.

   Note: If you want to configure Oracle Internet Directory to listen on SSL ports only, perform this configuration *after* you have installed OracleAS Single Sign-On and Oracle Delegated Administration Services. Oracle Internet Directory needs to be listening on both SSL and non-SSL ports when you install OracleAS Single Sign-On and Oracle Delegated Administration Services.

3. Install OracleAS Single Sign-On and Oracle Delegated Administration Services on each node. You run the installer on each node separately.
4. Install middle tiers.

9.6.2 Installing OracleAS Metadata Repository

To install the OracleAS Metadata Repository in your existing database, you use the OracleAS RepCA. See the *Oracle Application Server Metadata Repository Creation Assistant User's Guide* for details.

9.6.3 Installing Oracle Internet Directory on the First Node

You run the installer on each node separately to install the Oracle Identity Management components.

9.6.3.1 Set up staticports.ini File

When installing Oracle Internet Directory on the first node, you do not need a load balancer. You can set up and configure the load balancer later. However it is recommended that the port numbers used by Oracle Internet Directory and by the load balancer are the same.

To do this, create a staticports.ini file to specify port numbers that you want Oracle Internet Directory to use. Your load balancer will use the same port numbers for LDAP communications. The staticports.ini file should contain these lines:

```
Oracle Internet Directory port = port_num
Oracle Internet Directory (SSL) port = port_num
```

9.6.3.2 Select the Same Components for Each Installation

If you are setting up the second node as a failover to the first node, then you must select the same set of components in the Select Configuration Options screen for each installation. For example, if you select Oracle Internet Directory and Oracle Directory Integration Platform on the first node, you need to select them when installing on subsequent nodes.

9.6.3.3 Start the Installer

To install Oracle Internet Directory on the first node, follow the steps in Table 9–6.

To install Oracle Internet Directory on subsequent nodes, see Section 9.6.4, "Installing Oracle Internet Directory on Subsequent Nodes".

Key Points

- You must select the same components in the Select Configuration Options screen on all nodes. For example, if you select both Oracle Internet Directory and Oracle Directory Integration Platform on the first node, you must select them on subsequent nodes in this tier.

Table 9–6 Steps for Installing Oracle Internet Directory in a Distributed OracleAS Cluster (Identity Management) on the First Node

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Do not select **Oracle Application Server Single Sign-On**. Do not select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform** if you need this component. Do not select **Oracle Application Server Certificate Authority (OCA)**. Select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	Select **Manual** and enter the fullpath to your staticports.ini file in the provided field. You need to use staticports.ini file for OracleAS Cluster (Identity Management) configurations. See Section 9.6.3.1, "Set up staticports.ini File". Click **Next**.
4.	Specify Repository	When you install on the first node, you need to specify an OracleAS Metadata Repository that is not already registered with an Oracle Internet Directory. When you install on subsequent nodes, then the OracleAS Metadata Repository is registered with the Oracle Internet Directory on the first node. **Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the name of the computer where the database is running, and the port number at which it is listening. Use the format: *`host:port`*. **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.

Table 9–6 (Cont.) Steps for Installing Oracle Internet Directory in a Distributed OracleAS Cluster (Identity Management) on the First Node

	Screen	Action
5.	Select High Availability or Replication Option	Select **OracleAS Cluster (Identity Management)**, and click **Next**.
6.	Specify Namespace in Internet Directory	Select the suggested namespace, or enter a custom namespace for the location of the default Oracle Identity Management realm. Ensure the value shown in **Suggested Namespace** meets your deployment needs. If not, enter the desired value in **Custom Namespace**. See Section 4.16, "What Do I Enter in the "Specify Namespace in Internet Directory" Screen?". Click **Next**.
7.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `oid_das` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
8.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

9.6.4 Installing Oracle Internet Directory on Subsequent Nodes

Before performing the steps in this section, you must have installed Oracle Internet Directory on the first node as described in Section 9.6.3, "Installing Oracle Internet Directory on the First Node".

9.6.4.1 Staticports.ini File Not Needed

You do not need a staticports.ini file for this installation because the installer will configure this Oracle Internet Directory to use the same ports as the Oracle Internet Directory on the first node.

The Oracle Internet Directory on the first node must be up and running.

9.6.4.2 Select the Same Components for Each Installation

If you are setting up the second node as a failover to the first node, then you must select the same set of components in the Select Configuration Options screen for each installation. For example, if you select OracleAS Single Sign-On and Oracle Delegated Administration Services on the first node, you need to select them when installing on subsequent nodes.

9.6.4.3 Start the Installer

To install Oracle Internet Directory on subsequent nodes, follow these steps:

Table 9–7 Steps for Installing Oracle Internet Directory in a Distributed OracleAS Cluster (Identity Management) on Subsequent Nodes

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Select **Oracle Internet Directory**. Do not select **Oracle Application Server Single Sign-On**. Do not select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform** if you need this component. Do not select **Oracle Application Server Certificate Authority (OCA)**. Select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	Select **Automatic**. The installer configures Oracle Internet Directory to use the same ports as the Oracle Internet Directory on the first node. Click **Next**.
4.	Specify Repository	Enter the same connect information that you entered for the first Oracle Internet Directory. **Username**: Enter the username to use to log in to the OracleAS Metadata Repository database. The user must have DBA privileges. **Password**: Enter the user's password. **Hostname and Port**: Enter the name of the computer where the database is running, and the port number at which it is listening. Use the format: *`host:port`*. **Service Name**: Enter the service name of the database. Note that the service name must include the database domain name. Example: `orcl.mydomain.com` Click **Next**.
5.	Warning	This warning reminds you that you are installing this instance as part of an OracleAS Cluster (Identity Management), and that you need to synchronize the clocks on the nodes in the cluster. See Section 9.2.2, "Synchronize Clocks on All Nodes". Click **OK**.
6.	Specify ODS Password	Enter the password for the ODS schema in the OracleAS Metadata Repository. The ODS schema is the main schema used by Oracle Internet Directory. By default, the ODS password is the same as the ias_admin password (the password that you entered in the Specify Instance Name and ias_admin Password screen). Click **Next**.

Table 9–7 (Cont.) Steps for Installing Oracle Internet Directory in a Distributed OracleAS Cluster (Identity Management) on Subsequent Nodes

	Screen	Action
7.	Specify Oracle Internet Directory Login	**Username**: Enter the username to log in to the first Oracle Internet Directory. You must log in as the Oracle Internet Directory superuser (`cn=orcladmin`). **Password**: Enter the password for the username. **Realm**: Enter the realm against which to validate the username. This field appears only if your Oracle Internet Directory has multiple realms. Click **Next**.
8.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `oid_das` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.

9.6.5 Installing OracleAS Single Sign-On and Oracle Delegated Administration Services on Each Node

You run the installer on each node separately to install these Oracle Identity Management components.

9.6.5.1 Set up staticports.ini File

If you want to use custom ports for components other than Oracle HTTP Server, you need to create a staticports.ini file for this installation.

If you want custom ports for Oracle HTTP Server, you specify them in the "Specify HTTP Load Balancer Host and Listen Ports" screen.

If you specify custom ports for Oracle HTTP Server also in the staticports.ini file, and you also specify ports in the screen mentioned above, the ports specified in the screen take precedence.

To avoid specifying Oracle HTTP Server ports in the staticports.ini file, the staticports.ini file **must not contain these lines**:

```
Oracle HTTP Server port = port_num
Oracle HTTP Server Listen port = port_num
Oracle HTTP Server SSL port = port_num
Oracle HTTP Server Listen (SSL) port = port_num
```

If you have a staticports.ini file, you should also use the same file for installations on subsequent nodes.

9.6.5.2 Start the Installer

Key Points

- In the Specify OracleAS Cluster screen, for the first node, select **Create a New Cluster**. For the second node, select **Join an Existing Cluster** to join the cluster that you created when installing on the first node.
- In the Specify HTTP Load Balancer Host and Ports screen, enter the name of the HTTP virtual server of the load balancer, and the associated port. You also enter the port number for Oracle HTTP Server on this screen.
- Also in the Specify HTTP Load Balancer Host and Ports screen, you need to specify the same HTTP virtual server name and port number for all nodes. However, you can specify different port numbers for Oracle HTTP Server on each node, as long as your load balancer is configured to communicate with the specified port on that node.

Table 9–8 Steps for Installing Oracle Delegated Administration Services and OracleAS Single Sign-On in a Distributed OracleAS Cluster (Identity Management) Configuration

	Screen	Action
1.	--	Start up the installer and complete the first few screens. See Section 4.27, "Install Fragment: The First Few Screens of the Installation" for details. Notes: In the Select Installation Type screen, select **Oracle Identity Management**.
2.	Select Configuration Options	Do not select **Oracle Internet Directory**. Select **Oracle Application Server Single Sign-On**. Select **Oracle Application Server Delegated Administration Services**. Select **Oracle Directory Integration Platform** if you need this component. Do not select **Oracle Application Server Certificate Authority (OCA)**. Select **High Availability and Replication**. Click **Next**.
3.	Specify Port Configuration Options	Select **Manual** and enter the fullpath to your staticports.ini file in the provided field. You need to use staticports.ini file for OracleAS Cluster (Identity Management) configurations. See Section 9.6.5.1, "Set up staticports.ini File". Click **Next**.
4.	Select High Availability Option	Select **OracleAS Cluster (Identity Management)**, and click **Next**.
5.	Create or Join an OracleAS Cluster (Identity Management)	For the first node, select **Create a New OracleAS Cluster**. For subsequent nodes, select **Join an Existing Cluster**. Click **Next**.
6.	Specify New OracleAS Cluster Name - or - Specify Existing OracleAS Cluster Name	For the first node, enter a name for a new OracleAS Cluster (Identity Management). Example: `cluster1` For subsequent nodes, enter the name of the existing OracleAS Cluster (Identity Management). **Note:** Be very sure that the cluster name you enter is correct. The installer does not perform any checks on this name. **If the name is incorrect, the installation will fail.** Click **Next**.

Table 9–8 (Cont.) Steps for Installing Oracle Delegated Administration Services and OracleAS Single Sign-On in a Distributed OracleAS Cluster (Identity Management) Configuration

	Screen	Action
7.	Specify Host and Port for LDAP	The installer will use the values on this screen to connect to Oracle Internet Directory. **Hostname**: Enter the LDAP virtual server name of the load balancer. Enter the same virtual server name that you configured on the load balancer. **SSL Port**: Enter the port configured on this load balancer to handle LDAP SSL connections. Click **Next**.
8.	Specify Oracle Internet Directory Login	**Username**: Enter the username to log in to Oracle Internet Directory, accessed through the load balancer host and port specified in the previous screen. Log in as the Oracle Internet Directory superuser (`cn=orcladmin`), or as a user who belongs to the necessary groups in Oracle Internet Directory. Which groups are necessary depends on which components you are installing. See Section 5.3, "Groups Required to Configure or Deinstall Components" for details. **Password**: Enter the password for the username. **Realm**: Enter the realm against which to validate the username. This field appears only if your Oracle Internet Directory has multiple realms. Click **Next**.
9.	Specify HTTP Load Balancer Host and Ports	See Section 9.4, "About Configuring SSL and Non-SSL Ports for Oracle HTTP Server" for details. The values entered on this screen should be the same for every node. **HTTP Listener: Port**: Enter the port number that you want Oracle HTTP Server to listen on. **Enable SSL**: Select this option if you want to configure Oracle HTTP Server for SSL on this port. **HTTP Load Balancer: Hostname**: Enter the name of the HTTP virtual server configured on your load balancer. Enter the same virtual server name that you configured on the load balancer. **HTTP Load Balancer: Port**: Enter the port for the HTTP virtual server. **Enable SSL**: Select this option if this port is for SSL communications only. Click **Next**.
10.	Specify Instance Name and ias_admin Password	**Instance Name**: Enter a name for this infrastructure instance. Instance names can contain alphanumeric characters and the _ (underscore) character. If you have more than one Oracle Application Server instance on a computer, the instance names must be unique. See Section 3.5, "Oracle Application Server Instances and Instance Names" for instance name details. Example: `das_sso` **ias_admin Password** and **Confirm Password**: Set the password for the ias_admin user. This is the administrative user for the instance. See Section 3.6, "The ias_admin User and Restrictions on its Password" for restrictions on the password. Example: `welcome99` Click **Next**.
11.	--	Finish the installation. See Section 4.28, "Install Fragment: The Last Few Screens of the Installation" for details.

9.7 Post-Installation Steps

After installing Oracle Identity Management components on all nodes, reconfigure your load balancer to direct requests to all nodes. Before you started the installation, you had configured the load balancer to direct requests to node 1 only. See Section 9.2.4, "Configure Your LDAP Virtual Server".

This section contains the following post-installation steps:

- Section 9.7.1, "Cluster the OC4J_Security Instance for State Replication (First Oracle Delegated Administration Services node only)"
- Section 9.7.2, "Changing the Ports for Oracle Internet Directory"
- Section 9.7.3, "Update targets.xml (Case 2 only)"

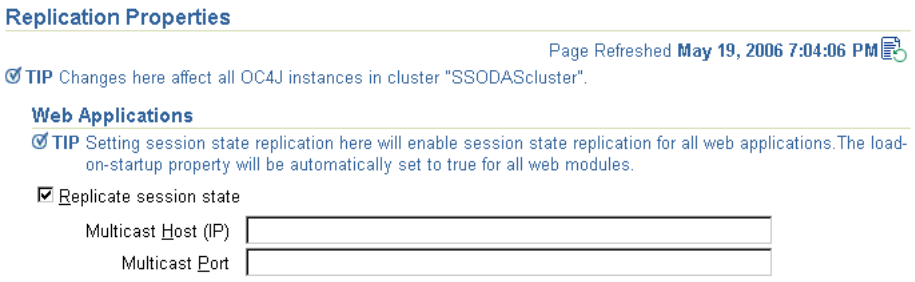
9.7.1 Cluster the OC4J_Security Instance for State Replication (First Oracle Delegated Administration Services node only)

To ensure that Oracle Application Server maintains the state of stateful Web applications across DCM-Managed OracleAS Cluster, you need to configure state replication for the Web applications. Configure state replication only on the first node where Oracle Delegated Administration Services is installed.

To configure state replication for the OC4J_Security instance, do the following:

1. Using the Application Server Control Console, navigate to the Application Server Home page for the instance that contains Oracle Delegated Administration Services.
2. Select the **OC4J_SECURITY** link on the Application Server Home page.
3. Select the **Administration** link on the OC4J Home Page.
4. Select the **Replication Properties** link in the Instance Properties area.
5. Scroll down to the Web Applications section. Figure 9–3 shows this section.

Figure 9–3 Web State Replication Configuration



6. Select the **Replicate session state** checkbox.

   Optionally, you can provide the multicast host IP address and port number. If you do not provide the host and port for the multicast address, it defaults to host IP address 230.230.0.1 and port number 9127. The host IP address must be between 224.0.0.2 through 239.255.255.255. Do not use the same multicast address for both HTTP and EJB multicast addresses.

Note: When choosing a multicast address, ensure that the address does not collide with the addresses listed in:

http://www.iana.org/assignments/multicast-addresses

Also, if the low order 23 bits of an address is the same as the local network control block, 224.0.0.0 – 224.0.0.255, then a collision may occur. To avoid this problem, provide an address that does not have the same bits in the lower 23 bits of the address as the addresses in this range.

9.7.2 Changing the Ports for Oracle Internet Directory

Although it is recommended that the ports for the LDAP virtual server and the Oracle Internet Directory are the same, it is possible for the ports to be different.

See the section "Changing Oracle Internet Directory Ports" in the *Oracle Application Server Administrator's Guide* for details on changing the Oracle Internet Directory ports.

9.7.3 Update targets.xml (Case 2 only)

The following configuration steps are needed only in the installation scenario described in Section 9.4.2, "Case 2: Client ---[HTTPS]---> Load Balancer ---[HTTPS]---> Oracle HTTP Server".

In this case the oracle_sso_server entry in the `targets.xml` file, on each physical host of the cluster, must be reconfigured to monitor the local SSL port.

Note:

Keep in mind that the hostname should remain the same. Please do not change the hostname.

Perform the following steps to update `targets.xml` on each node of the cluster:

1. Back up the `targets.xml` file:

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

2. Open the file and find the oracle_sso_server target type. Within this target entry, locate and edit the following two attributes:
   - HTTPPort - the server SSL port number
   - HTTPProtocol - the server protocol, which in this case is `HTTPS`

     For example, you could update the two attributes this way:

```
<Property NAME="HTTPPort" VALUE="4443"/>
<Property NAME="HTTPProtocol" VALUE="HTTPS"/>
```

3. Save and close the file.
4. Reload the OracleAS console:

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

9.8 Installing Middle Tiers Against OracleAS Cluster (Identity Management) Configurations

Pre-Installation

Before starting the middle-tier installation, configure the LDAP load balancer that you are using for Oracle Internet Directory so that it points to only one Oracle Internet Directory node.

Installation

When installing middle tiers against OracleAS Cluster (Identity Management) configurations, follow the steps for middle tier installation described in *Oracle Application Server Installation Guide* for the middle tier release you are using.

When the installer prompts for the Oracle Internet Directory host and port, enter the LDAP virtual host name configured on the load balancer and the associated port.

Post-Installation

After installing the middle tiers, you can reconfigure the LDAP load balancer to point to all the Oracle Internet Directory nodes.

10

Installing in High Availability Environments: OracleAS Disaster Recovery

This chapter describes how to install Oracle Application Server in OracleAS Disaster Recovery configurations. OracleAS Disaster Recovery is one of the high availability environments supported by Oracle Application Server.

This chapter contains the following topics:

- Section 10.1, "OracleAS Disaster Recovery: Introduction"
- Section 10.2, "Setting up the OracleAS Disaster Recovery Environment"
- Section 10.3, "Installing Oracle Application Server in an OracleAS Disaster Recovery Environment"
- Section 10.4, "Installing the OracleAS 10g (10.1.2.0.2) Standalone Install of OracleAS Guard into Oracle Homes"
- Section 10.5, "Patching OracleAS Guard Release 10.1.2.0.0 with Release 10.1.2.0.2"
- Section 10.6, "What to Read Next"

10.1 OracleAS Disaster Recovery: Introduction

Use the OracleAS Disaster Recovery environment when you want to have two physically separate sites in your environment. One site is the production site, and the other site is the standby site. The production site is active, while the standby site is passive; the standby site becomes active when the production site goes down.

OracleAS Disaster Recovery supports a number of basic topologies for the configuration of the Infrastructure and middle tier on production and standby sites. OracleAS Disaster Recovery supports these basic topologies:

- Symmetrical topologies -- strict mirror of the production site with collocated Oracle Identity Management and OracleAS Metadata Repository Infrastructure
- Asymmetrical topologies -- simple asymmetric standby topology with collocated Oracle Identity Management and OracleAS Metadata Repository Infrastructure
- Separate OracleAS Metadata Repository for OracleAS Portal with collocated Oracle Identity Management and OracleAS Metadata Repository Infrastructure (the Departmental Topology)
- Distributed Application OracleAS metadata Repositories with Non collocated Oracle Identity Management and OracleAS Metadata Repository Infrastructure

In a symmetric topology, each node in the standby site corresponds to a node in the production site. This includes the nodes running both OracleAS Infrastructure and

middle tiers. In an asymmetric topology, the number of instances required on the standby site are fewer than the number on the production site and the number of instances required on the standby site must be the minimum set of instances required to run your site in the event of a switchover or failover operation.

As a small variation to this environment, you can set up the OracleAS Infrastructure on the production site in an OracleAS Cold Failover Cluster environment. See Section 10.2.4, "If You Want to Use OracleAS Cold Failover Cluster on the Production Site" for details.

For these supported topologies, OracleAS Guard will be installed in every Oracle home on every system that is part of your production and standby topology configured for the OracleAS Disaster Recovery solution.

OracleAS Guard can be installed as a standalone install kit located on OracleAS Companion CD #2. See Section 10.4, "Installing the OracleAS 10g (10.1.2.0.2) Standalone Install of OracleAS Guard into Oracle Homes" for more information about when this standalone kit should be installed.

Figure 10–1 shows an example symmetric OracleAS Disaster Recovery environment. Each site has two nodes running middle tiers and a node running OracleAS Infrastructure.

Data Synchronization

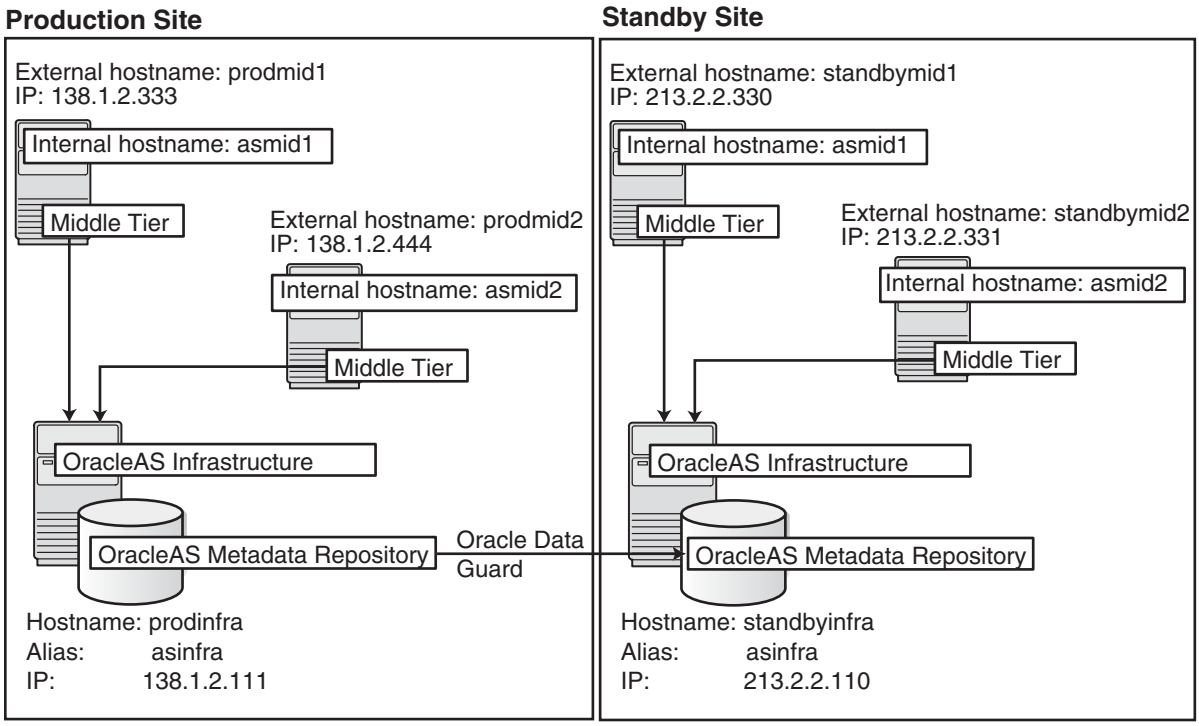
For OracleAS Disaster Recovery to work, data between the production and standby sites must be synchronized so that failover can happen very quickly. Configuration changes done at the production site must be synchronized with the standby site.

You need to synchronize two types of data. The synchronization method depends on the type of data:

- Use Oracle Data Guard to synchronize data in the OracleAS Metadata Repository databases on the production and standby sites. You can configure Oracle Data Guard to perform the synchronization.
- Use the backup and recovery scripts to synchronize data outside of the database (such as data stored in configuration files).

See the *Oracle Application Server High Availability Guide* for details on how to use Oracle Data Guard and the backup and recovery scripts.

Figure 10–1 OracleAS Disaster Recovery Environment



10.2 Setting up the OracleAS Disaster Recovery Environment

Before you can install Oracle Application Server in an OracleAS Disaster Recovery environment, you have to perform these steps:

- Section 10.2.1, "Ensure Nodes Are Identical at the Operating System Level"
- Section 10.2.2, "Set Up staticports.ini File"
- Section 10.2.3, "Set Up Identical Hostnames on Both Production and Standby Sites"
- Section 10.2.4, "If You Want to Use OracleAS Cold Failover Cluster on the Production Site"

10.2.1 Ensure Nodes Are Identical at the Operating System Level

Ensure that the nodes are identical with respect to the following items:

- The nodes are running the same version of the operating system.
- The nodes have the same operating system patches and packages.
- You can install Oracle Application Server in the same directory path on all nodes.

10.2.2 Set Up staticports.ini File

The same component must use the same port number on the production and standby sites. For example, if Oracle HTTP Server is using port 80 on the production site, it must also use port 80 on the standby site. To ensure this is the case, create a `staticports.ini` file for use during installation. This file enables you to specify port numbers for each component. See Section 2.6.3, "Using Custom Port Numbers (the "Static Ports" Feature)" for details.

10.2.3 Set Up Identical Hostnames on Both Production and Standby Sites

The names of the corresponding nodes on the production and standby sites must be identical, so that when you synchronize data between the sites, you do not have to edit the data to fix the hostnames.

For the Infrastructure Nodes

For the node running the infrastructure, set up a virtual name. To do this, specify an alias for the node in the `/etc/hosts` file.

For example, on the infrastructure node on the production site, the following line in the `hosts` file sets the alias to `asinfra`:

```
138.1.2.111   prodinfra   asinfra
```

On the standby site, the following line sets the node's alias to `asinfra`.

```
213.2.2.110   standbyinfra   asinfra
```

When you install OracleAS Infrastructure on the production and standby sites, you specify this alias (`asinfra`) in the Specify Virtual Hostname screen. The configuration data will then contain this alias for the infrastructure nodes.

For the Middle-Tier Nodes

For the nodes running the middle tiers, you cannot set up aliases like you did for the infrastructure nodes because the installer does not display the Specify Virtual Hostname screen for middle-tier installations. When installing middle tiers, the installer determines the hostname automatically by calling the gethostname() function. You want to be sure that for each middle-tier node on the production site, the corresponding node on the standby site returns the same hostname.

To do this, set up a local, or internal, hostname, which could be different from the public, or external, hostname. You can change the names of the nodes on the standby site to match the names of the corresponding nodes on the production site, or you can change the names of the nodes on both production and standby sites to be the same. This depends on other applications that you might be running on the nodes, and whether changing the node name will affect those applications.

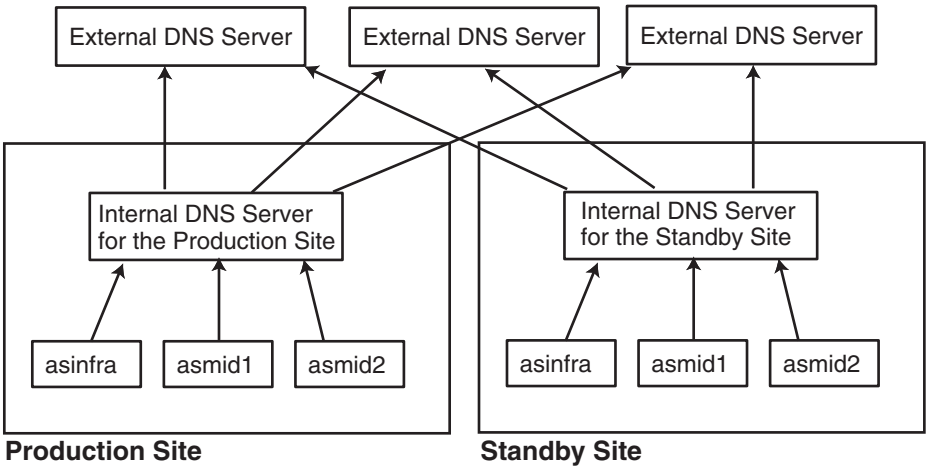
1. On the nodes whose local names you want to change, edit the `/etc/nodename` file to specify the new local fully qualified name. The following example sets the name to `iasmid1.oracle.com`. (The example in Figure 10–1 uses this name.)

   ```
   iasmid1.oracle.com
   ```

2. Enable the other nodes in the OracleAS Disaster Recovery environment to be able to resolve the node using the new local hostname. You can do this in one of two ways:

   Method 1: Set up separate internal DNS servers for the production and standby sites. This configuration allows nodes on each site (production or standby) to resolve hostnames within the site. Above the internal DNS servers are the corporate, or external, DNS servers. The internal DNS servers forward non-authoritative requests to the external DNS servers. The external DNS servers do not know about the existence of the internal DNS servers. See Figure 10–2.

Figure 10–2 Method 1: Using DNS Servers



Method 1 Details

a. Make sure the external DNS names are defined in the external DNS zone. Example:

```
prodmid1.us.oracle.com     IN  A  138.1.2.333
prodmid2.us.oracle.com     IN  A  138.1.2.444
prodinf.us.oracle.com      IN  A  138.1.2.111
standbymid1.us.oracle.com  IN  A  213.2.2.330
standbymid2.us.oracle.com  IN  A  213.2.2.331
standbyinf.us.oracle.com   IN  A  213.2.2.110
```

b. At the production site, create a new zone at the production site using a domain name different from your external domain name. To do this, populate the zone data files with entries for each node in the OracleAS Disaster Recovery environment.

For the infrastructure node, use the virtual name or alias.

For the middle-tier nodes, use the node name (the value in `/etc/nodename`).

The following example uses "asha" as the domain name for the new zone.

```
asmid1.asha    IN  A  138.1.2.333
asmid2.asha    IN  A  138.1.2.444
asinfra.asha   IN  A  138.1.2.111
```

Do the same for the standby site. Use the same domain name that you used for the production site.

```
asmid1.asha    IN  A  213.2.2.330
asmid1.asha    IN  A  213.2.2.331
asinfra.asha   IN  A  213.2.2.110
```

c. Configure the DNS resolver to point to the internal DNS servers instead of the external DNS server.

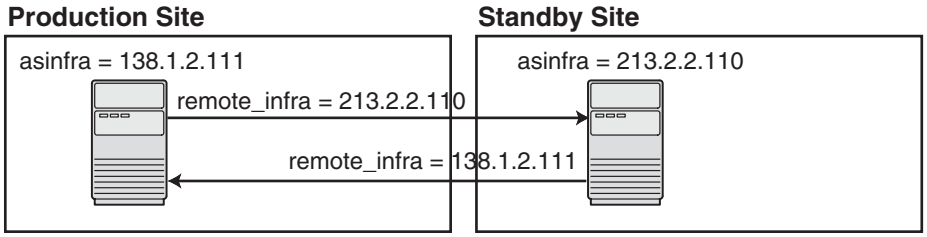
In the `/etc/resolv.conf` file for each node on the production site, replace the existing name server IP address with the IP address of the internal DNS server for the production site.

Do the same for the nodes on the standby site, but use the IP address of the internal DNS server for the standby site.

d. Create a separate entry for Oracle Data Guard in the internal DNS servers. This entry is used by Oracle Data Guard to ship redo data to the database on the standby site.

In the next example, the "remote_infra" entry points to the infrastructure node on the standby site. This name is used by the TNS entries on both the production and standby sites so that if a switchover occurs, the entry does not have to be changed.

Figure 10–3 Entry for Oracle Data Guard in the Internal DNS Servers



On the production site, the DNS entries look like this:

```
asmid1.asha        IN  A  138.1.2.333
asmid2.asha        IN  A  138.1.2.444
asinfra.asha       IN  A  138.1.2.111
remote_infra.asha  IN  A  213.2.2.110
```

On the standby site, the DNS entries look like this:

```
asmid1.asha        IN  A  213.2.2.330
asmid2.asha        IN  A  213.2.2.331
asinfra.asha       IN  A  213.2.2.110
remote_infra.asha  IN  A  138.1.2.111
```

Method 2: Edit the `/etc/hosts` file on each node on both sites. This method does not involve configuring DNS servers, but you have to maintain the `hosts` file on each node in the OracleAS Disaster Recovery environment. For example, if an IP address changes, you have to update the files on all the nodes, and restart the nodes.

Method 2 Details

a. On each node on the production site, include these lines in the `/etc/hosts` file. The IP addresses resolve to nodes on the production site.

Note: In the `hosts` file, be sure that the line that identifies the current node comes *immediately* after the localhost definition (the line with the 127.0.0.1 address).

```
127.0.0.1    localhost
138.1.2.333  asmid1.oracle.com   asmid1
138.1.2.444  asmid2.oracle.com   asmid2
138.1.2.111  asinfra.oracle.com  asinfra
```

b. On each node on the standby site, include these lines in the `hosts` file. The IP addresses resolve to nodes on the standby site.

Note: In the `hosts` file, be sure that the line that identifies the current node comes *immediately* after the localhost definition (the line with the 127.0.0.1 address).

```
127.0.0.1    localhost
213.2.2.330  asmid1.oracle.com   asmid1
213.2.2.331  asmid2.oracle.com   asmid2
213.2.2.110  asinfra.oracle.com  asinfra
```

c. Ensure that the "hosts:" line in the `/etc/nsswitch.conf` file has "files" as the first item:

```
hosts:   files nis dns
```

The entry specifies the ordering of the name resolution. If another method is listed first, then the node will use the other method to resolve the hostname.

Note: Restart the nodes after editing these files.

Verifying that the Nodes Resolve the Hostnames Correctly

After making the changes and restarting the nodes, check that the nodes resolve the hostnames properly by running the following commands:

- On the middle-tier nodes on both sites, run the `hostname` command. This should return the internal hostname. For example, the command should return "asmid1" if you run it on prodmid1 and standbymid1.

```
prompt> hostname
asmid1
```

- On each node, ping the other nodes in the environment using the internal hostname as well as the external hostname. The command should be successful. For example, from the first midtier node, prodmid1, run the following commands (the `-s` option displays the IP address of the node):

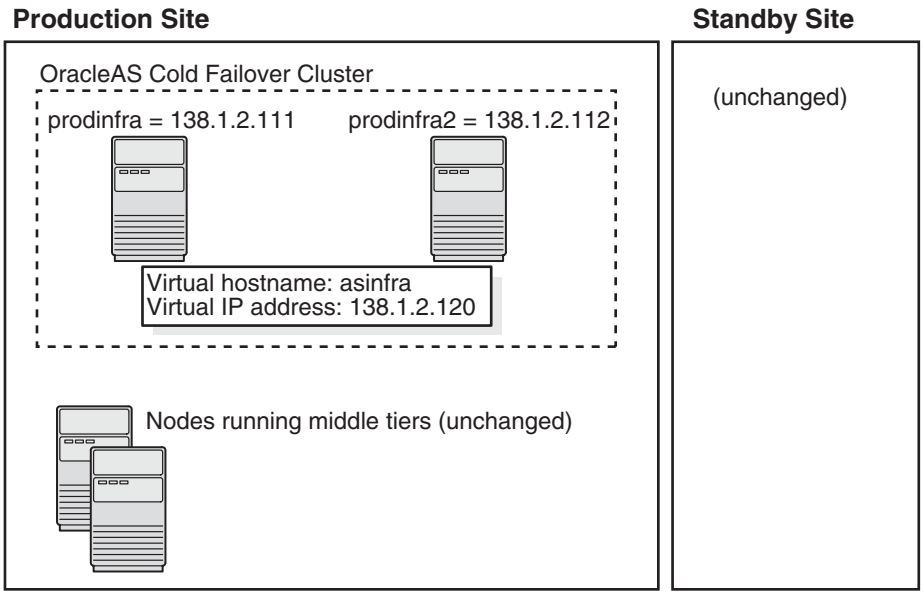
```
prompt> ping -s prodinfra ping the production infrastructure node
PING prodinfra: 56 data byes
64 bytes from prodinfra.oracle.com (138.1.2.111): icmp_seq=0. time=0. ms
^C

prompt> ping -s iasinfra ping the production infrastructure node
PING iasinfra: 56 data byes
64 bytes from iasinfra.oracle.com (138.1.2.111): icmp_seq=0. time=0. ms
^C

prompt> ping -s iasmid2 ping the second production midtier node
PING iasmid2: 56 data byes
64 bytes from iasmid2.oracle.com (138.1.2.444): icmp_seq=0. time=0. ms
^C

prompt> ping -s prodmid2 ping the second production midtier node
PING prodmid2: 56 data byes
64 bytes from prodmid2.oracle.com (138.1.2.444): icmp_seq=0. time=0. ms
^C

prompt> ping -s standbymid1 ping the first standby midtier node
PING standbymid1: 56 data byes
```

```
64 bytes from standbymid1.oracle.com (213.2.2.330): icmp_seq=0. time=0. ms
^C
```

10.2.4 If You Want to Use OracleAS Cold Failover Cluster on the Production Site

On the production site of a OracleAS Disaster Recovery system, you can set up the OracleAS Infrastructure to run in a OracleAS Cold Failover Cluster configuration. In this case, you have two nodes in a hardware cluster, and you install the OracleAS Infrastructure on a shared disk. See Chapter 8, "Installing in High Availability Environments: OracleAS Cold Failover Cluster" for details.

Figure 10–4 Infrastructure in an OracleAS Cold Failover Cluster Configuration



To set up OracleAS Cold Failover Cluster in this environment, use the virtual IP address (instead of the physical IP address) for asinfra.asha on the production site. The following example assumes 138.1.2.120 is the virtual IP address.

```
asmid1.asha          IN  A  138.1.2.333
asmid2.asha          IN  A  138.1.2.444
asinfra.asha         IN  A  138.1.2.120         this is a virtual IP address
remote_infra.asha    IN  A  213.2.2.110
```

On the standby site, you still use the physical IP address for asinfra.asha, but the remote_infra.asha uses the virtual IP address.

```
asmid1.asha          IN  A  213.2.2.330
asmid2.asha          IN  A  213.2.2.331
asinfra.asha         IN  A  213.2.2.110         physical IP address
remote_infra.asha    IN  A  138.1.2.120         virtual IP address
```

10.3 Installing Oracle Application Server in an OracleAS Disaster Recovery Environment

Install Oracle Application Server as follows:

Note: For all of the installations, be sure to use staticports.ini to specify port numbers for the components. See Section 10.2.2, "Set Up staticports.ini File".

---

1. Install OracleAS Infrastructure on the production site.
2. Install OracleAS Infrastructure on the standby site.
3. Start the OracleAS Infrastructure in each site before installing the middle tiers for that site.
4. Install middle tiers on the production site.
5. Install middle tiers on the standby site.

10.3.1 Installing the OracleAS Infrastructure

The installation steps are similar to that for OracleAS Cold Failover Cluster. See Section 8.3, "Installing an OracleAS Cold Failover Cluster (Infrastructure) Configuration" for the screen sequence. Note the following points:

- Select Configuration Options screen: be sure you select **High Availability and Replication**. See Table 8–2, step 2.
- Specify Virtual Hostname screen: enter an alias as the virtual address (for example, asinfra.oracle.com). See Table 8–2, step 6.

10.3.2 Installing Middle Tiers

You can install any type of middle tier that is compatible with Oracle Application Server 10*g* (10.1.4.0.1). See the *Oracle Application Server Upgrade and Compatibility Guide* for more information.

To install a middle tier, see the *Oracle Application Server Installation Guide* for the release.

Note the following points:

- When the installer prompts you to register with Oracle Internet Directory, and asks you for the Oracle Internet Directory hostname, enter the alias of the node running OracleAS Infrastructure (for example, asinfra.oracle.com).

10.4 Installing the OracleAS 10g (10.1.2.0.2) Standalone Install of OracleAS Guard into Oracle Homes

OracleAS 10g (10.1.2.0.2) standalone install of OracleAS Guard is located on Companion CD Disk 2. This standalone install of OracleAS Guard can be installed in the following environments:

- In its own home in the case when you are cloning an instance or topology to a new standby system (see the section on standby site cloning in *Oracle Application Server High Availability Guide* for more information).
- Oracle database server home for an OracleAS Metadata Repository configuration created using OracleAS Metadata Repository Creation Assistant.
- OracleAS Disaster Recovery full site upgrade from OracleAS 10g (9.0.4) to OracleAS 10g (10.1.2.0.2) (see the chapter on OracleAS Disaster Recovery site

upgrade procedure in *Oracle Application Server High Availability Guide* for more information).

- OracleAS Guard patch upgrade from OracleAS 10g (10.1.2.0.0) to OracleAS 10g (10.1.2.0.2) (see Section 10.5, "Patching OracleAS Guard Release 10.1.2.0.0 with Release 10.1.2.0.2" for more information).

If this is an upgrade installation of OracleAS Guard, make a copy of your `dsa.conf` configuration file to save your current settings for your OracleAS Guard environment. After running the OracleAS 10g (10.1.2.0.2) standalone install kit of OracleAS Guard, you can restore your saved `dsa.conf` configuration file with your settings to continue using the same settings for the upgraded OracleAS Guard environment.

To run the OracleAS 10g (10.1.2.0.2) standalone install kit of OracleAS Guard, run the kit in the following directory path:

On UNIX systems:

```
/Disk2/asg/install/runInstaller
```

Choose the type of install that you want. Choose **Typical** for most installations. Choose **Custom or Reinstall** for upgrading from an older release of OracleAS Guard to the current release.

Enter the `ias_admin` account password to continue the installation.

10.5 Patching OracleAS Guard Release 10.1.2.0.0 with Release 10.1.2.0.2

If you already have an OracleAS Disaster Recovery environment set up using OracleAS Guard Release 10.1.2.0.0, you can patch OracleAS Guard in your environment to take advantage of new features and support for the topologies described in Section 10.1, "OracleAS Disaster Recovery: Introduction". To patch your OracleAS Disaster Recovery environment, follow these basic steps:

1. Stop the OracleAS Guard server in all OracleAS 10.1.2.0.0 Oracle homes on both production and standby sites using the following opmnctl command:

   On UNIX systems:

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

2. Install the OracleAS 10g (10.1.2.0.2) standalone install of OracleAS Guard into each Oracle home on the production and standby sites.

   If multiple Oracle homes exist on the same system, ensure that different ports are configured for each of the OracleAS Guard servers in this configuration file.

   Because this is an upgrade installation of OracleAS Guard, make a copy of your `dsa.conf` configuration file to save your current settings for your OracleAS Guard environment. After running the OracleAS 10g (10.1.2.0.2) standalone install kit of OracleAS Guard, you can restore your saved `dsa.conf` configuration file with your settings to continue using the same settings for the upgraded OracleAS Guard environment.

   On UNIX systems:

   ```
   <ORACLE_HOME>/dsa/dsa.conf
   ```

3. Start the OracleAS Guard server in all OracleAS 10.1.2.0.0 Oracle homes on both production and standby sites using the following opmnctl command:

   On UNIX systems:

```
<ORACLE_HOME>/opmn/bin/opmnctl startall
<ORACLE_HOME>/opmn/bin/opmnctl startproc ias-component=DSA
```

10.6 What to Read Next

For information on how to manage your OracleAS Disaster Recovery environment, such as setting up Oracle Data Guard and configuring the OracleAS Metadata Repository database, see the *Oracle Application Server High Availability Guide*.

11

Post-Installation Tasks

This chapter contains the following topics:

- Section 11.1, "State of Oracle Application Server Instances After Installation"
- Section 11.2, "Passwords for Oracle Application Server Components"
- Section 11.3, "NFS Installations"
- Section 11.4, "Backup and Recovery"
- Section 11.5, "SSL"
- Section 11.6, "Operating System Locale and NLS_LANG Environment Variable"
- Section 11.7, "Component Configuration After Installation"
- Section 11.8, "Components that Require Post-Installation Tasks"
- Section 11.9, "What to Do Next"

11.1 State of Oracle Application Server Instances After Installation

After installation, the components that you have configured are started up (unless you have configured them to use ports lower than 1024, in which case you have to start them up manually).

You can view the Welcome page and the Application Server Control page in a browser. The URLs for these pages are shown in the last screen of the installer. You can view the contents of the last screen in the file `ORACLE_HOME/install/setupinfo.txt`.

You can use scripts or you can use the Oracle Enterprise Manager 10*g* Application Server Control to start and stop Oracle Application Server instances. See the *Oracle Application Server Administrator's Guide* for details.

11.2 Passwords for Oracle Application Server Components

By default, all passwords for Oracle Application Server components, with the exception of the OracleAS Metadata Repository schema passwords, are set to be the same as the Oracle Application Server instance password. For security reasons, you should change the passwords of the various components to have different values.

See the *Oracle Application Server Administrator's Guide* and the component guides in the Oracle Application Server Documentation Library for details on how to alter the passwords for the components you have installed.

11.3 NFS Installations

If you installed Oracle Application Server on an NFS disk, you need to edit the `LockFile` directive in the `ORACLE_HOME/Apache/Apache/conf/httpd.conf` file so that it points to a local disk. This file is used by the Oracle HTTP Server component.

See the *Oracle HTTP Server Administrator's Guide* for details.

11.4 Backup and Recovery

After installation would be a good time to start backing up the files, and to set up your backup and recovery strategy. See the *Oracle Application Server Administrator's Guide* for details.

11.5 SSL

By default, most components are not configured for SSL. To enable SSL, see the SSL section in the *Oracle Application Server Administrator's Guide*.

11.6 Operating System Locale and NLS_LANG Environment Variable

If you installed Oracle Application Server in a non-English language environment, please check your settings as described in these sections:

- Section 11.6.1, "Check the Operating System Locale"
- Section 11.6.2, "Check the NLS_LANG Setting"

11.6.1 Check the Operating System Locale

To make sure the default locale is set properly, verify that the LC_ALL or LANG environment variables are set with the appropriate values. To check the current setting, run the `locale` command:

```
prompt> locale
```

11.6.2 Check the NLS_LANG Setting

To check the NLS_LANG setting:

1. Make sure the value of the NLS_LANG environment variable is compatible with the default locale setting of the operating system. See the *Oracle Application Server Globalization Guide* for details, including a list of files that set this variable. You might need to edit the value of the NLS_LANG variable in these files.
2. Check that the NLS_LANG setting in the `ORACLE_HOME/opmn/conf/opmn.xml` file is identical to the NLS_LANG environment variable.

   Example: The NLS_LANG setting in the `opmn.xml` file might look something like this:

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

11.7 Component Configuration After Installation

If you did not configure a component during installation (that is, you did not select the component in the Select Configuration Options screen), you can configure some components after installation. Some components have dependencies that you have to complete before you can configure the component. Section 11.7.1, "Configuring mod_osso (Required for Oracle Delegated Administration Services)" describes how to configure mod_osso, which has to be configured before you can configure Oracle Delegated Administration Services.

11.7.1 Configuring mod_osso (Required for Oracle Delegated Administration Services)

If you did not configure Oracle Delegated Administration Services during installation, you can do it after installation using Oracle Enterprise Manager 10*g* Application Server Control.

Oracle Delegated Administration Services requires OracleAS Single Sign-On and mod_osso. mod_osso is an Oracle HTTP Server module that communicates with the Single Sign-On server. If mod_osso is not configured, you have to configure it before you can configure Oracle Delegated Administration Services. Here are the steps:

1. Ensure that OracleAS Single Sign-On is configured against Oracle Internet Directory. This is done for you if you have installed and configured these two components from the installer.
2. Check if mod_osso is configured in the ORACLE_HOME where you want to configure Oracle Delegated Administration Services.

   Examine the following line in the `ORACLE_HOME/Apache/Apache/conf/httpd.conf` file. ORACLE_HOME refers to the directory where you want to configure Oracle Delegated Administration Services.

   ```
   include "ORACLE_HOME/Apache/Apache/conf/mod_osso.conf"
   ```

   If the line starts with `#`, then it is commented out and mod_osso is not configured in this installation. Perform step 3 to configure mod_osso.

   If the line is not commented out, mod_osso is already configured. You can go ahead and configure Oracle Delegated Administration Services using Application Server Control. Go to step 5.
3. To configure mod_osso manually, perform these steps:
   a. Set the ORACLE_HOME environment variable to the full path of the directory where you want to configure Oracle Delegated Administration Services.
   b. Set the LD_LIBRARY_PATH environment variable to contain `$ORACLE_HOME/lib32` and `$ORACLE_HOME/network/lib`.
   c. Set the LD_LIBRARY_PATH_64 environment variable to contain `$ORACLE_HOME/lib`.
   d. Run the following command (all on one line). **Note:** for the `-classpath` parameter, do not type any space characters after the colon (`:`) characters, as indicated by *<no spaces>*:

   ```
   prompt> $ORACLE_HOME/jdk/bin/java
    -classpath .:$ORACLE_HOME/sso/lib/ossoreg.jar:<no spaces>
    $ORACLE_HOME/jlib/ojmisc.jar:<no spaces>
    $ORACLE_HOME/jlib/repository.jar:<no spaces>
    $ORACLE_HOME/j2ee/home/jazn.jar:$ORACLE_HOME/jdk/lib/dt.jar:<no spaces>
    $ORACLE_HOME/jdk/lib/tools.jar:$ORACLE_HOME/jlib/infratool.jar
   ```

```
oracle.ias.configtool.UseInfrastructure i
-f $ORACLE_HOME/config/infratool_mod_osso.properties
-h OIDhost -p OIDport -u OIDadminName -w OIDclearTextPassword
-o ORACLE_HOME -m ASinstanceName
-infra infraGlobalDBName -mh host -sso true
-sslp sslPort -sslf false
```

Table 11–1 describes the parameters where you have to supply values:

Table 11–1 Parameters for Configuring mod_osso

Parameter	Description
-h *OIDhost*	Specifies the name of the computer where Oracle Internet Directory is running. You can determine this value from the `OIDhost` parameter in the `ORACLE_HOME/config/ias.properties` file.
-p *OIDport*	Specifies the port number on which Oracle Internet Directory is listening. You can determine this value from the `OIDport` parameter in the `ORACLE_HOME/config/ias.properties` file.
-u *OIDadminName*	Specifies the login name for Oracle Internet Directory. Use the superuser: `cn=orcladmin`.
-w *OIDclearTextPassword*	Specifies the password for the Oracle Internet Directory user.
-o *ORACLE_HOME*	Specifies the full path to the directory where you installed OracleAS Infrastructure.
-m *ASinstanceName*	Specifies the name of the OracleAS Infrastructure instance where you want to configure mod_osso. You can determine this value from the `IASname` parameter in the `ORACLE_HOME/config/ias.properties` file.
-infra *infraGlobalDBname*	Specifies the name of the OracleAS Metadata Repository database. You can determine this value from the `InfrastructureDBCommonName` parameter in the `ORACLE_HOME/config/ias.properties` file.
-mh *host*	Specifies the full hostname (including the domain name) of the computer where you want to configure Oracle Delegated Administration Services.
-sslp *sslPort*	Specifies the SSL port for Oracle Internet Directory. You can determine this value from the `OIDsslport` parameter in the `ORACLE_HOME/config/ias.properties` file.

4. Restart OC4J and Oracle HTTP Server. You can do this using the `opmnctl` command.

```
prompt> $ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=OC4J
prompt> $ORACLE_HOME/opmn/bin/opmnctl restartproc ias-component=HTTP_Server
```

5. Once mod_osso is configured, you can configure Oracle Delegated Administration Services using the Application Server Control. See the *Oracle Internet Directory Administrator's Guide* for details.

11.8 Components that Require Post-Installation Tasks

If you plan to use any of the components listed in Table 11–2, you need to perform some steps specific to the component after installation before you can use the component. Table 11–2 lists the component guides that describe the steps.

Table 11–2 Components Requiring Post-Installation Steps

Component	Guide That Describes the Post-Installation Steps
OracleAS Certificate Authority	*Oracle Application Server Certificate Authority Administrator's Guide*

11.9 What to Do Next

After installing Oracle Application Server, you should read the *Oracle Application Server Administrator's Guide*. Specifically, you should read the "Getting Started After Installing Oracle Application Server" chapter.

You should also perform a complete Oracle Application Server environment backup after installing Oracle Application Server. This enables you to restore a working environment in case something goes wrong. For details on how to perform a complete Oracle Application Server environment backup, see the *Oracle Application Server Administrator's Guide*.

You should also perform a complete Oracle Application Server environment backup after each successful patchset upgrade and after each successful configuration change.

A

Installing the Oracle Identity Management Grid Control Plug-in

This appendix describes how to install Oracle Identity Management Grid Control Plug-in and Oracle Identity Management Grid Control Plug-in Agent. It contains the following sections:

- Section A.1, "Installation Requirements"
- Section A.2, "Starting the Grid Control Plug-in Installer"
- Section A.3, "Installing Oracle Identity Management Grid Control Plug-in"
- Section A.4, "Installing Oracle Identity Management Grid Control Plug-in Agent"

A.1 Installation Requirements

Before installing Oracle Identity Management Grid Control Plug-in or Oracle Identity Management Grid Control Plug-in Agent, you must install Oracle Enterprise Manager 10*g* Release 2 Grid Control 10.2.0.1.0 or later.

A.2 Starting the Grid Control Plug-in Installer

1. If you are installing from a CD-ROM or DVD-ROM and your computer does not mount CD-ROMs or DVDs automatically, you need to set the mount point manually. See Section 3.14, "Setting the Mount Point for the CD-ROM or DVD-ROM" for details.
2. Log in as the `oracle` user.
3. If you are installing from your hard drive, go to the next step.

   CD-ROM users: Insert the CD that contains the Grid Control Plug-in into the CD-ROM drive.

   DVD-ROM users: Insert the Oracle Application Server DVD-ROM into the DVD-ROM drive.
4. Run the Oracle Universal Installer using the command shown after the notes:

Notes:

- Be sure you are not logged in as the root user when you start the Oracle Universal Installer. The installer gives an error message if you try to run it as the root user.
- Do not start the installation inside the mount_point directory. If you do, then you may not be able to eject the installation disk. The `cd` command below changes your current directory to your home directory.

CD-ROM:

```
prompt> cd
prompt> mount_point/1014IMGCDisk1/runInstaller
```

DVD-ROM: Locate the Grid Control Plug-in directory and execute `runInstaller`.

Hard Drive:

```
prompt> cd disk1_directory
prompt> runInstaller
```

where *disk1_directory* is the directory where you unzipped the Disk 1 file.

This launches Oracle Universal Installer, through which you can install Oracle Identity Management Grid Control Plug-in.

A.3 Installing Oracle Identity Management Grid Control Plug-in

Before installing the Oracle Identity Management Grid Control Plug-in, you must stop any running Management Service. Stop the Management Service using the following command:

```
prompt> ORACLE_HOME/opmn/bin/opmnctl stopall
```

where *ORACLE_HOME* is the home for Oracle Management Service. After stopping the Management Service, wait at least four minutes before installing the Oracle Identity Management Grid Control Plug-in so that the Management Service can completely shut down.

Perform the following steps to install Oracle Identity Management Grid Control Plug-in:

Table A–1 Steps for Installing Oracle Identity Management Grid Control Plug-in

	Screen	Action
1.	--	Start the installer. See Section A.2, "Starting the Grid Control Plug-in Installer" for details.
2.	Welcome	Click **Next**.
3.	Specify Home Details	**Path**: Select the full path of the directory that contains Oracle Enterprise Manager 10*g* Release 2 Grid Control 10.2.0.1.0 or later from the drop-down box. Note that when you select the path, the **Name** field will be automatically updated with the correct name for the Oracle Home. Click **Next**.

Table A–1 (Cont.) Steps for Installing Oracle Identity Management Grid Control Plug-in

	Screen	Action
4.	Repository Database Administrator Password	**Password**: Enter the password for the SYS user. Click **Next**.
5.	Summary	Verify your selections and click **Install**.
6.	Install Progress	This screen shows the progress of the installation.
7.	Configuration Assistants	This screen shows the progress of the configuration assistants. Configuration assistants configure components. Note that the configuration assistants will take at least 30 minutes to complete.
8.	End of Installation	Click **Exit** to quit the installer.

Following installation, perform the following command to start the Management Service:

```
prompt> ORACLE_HOME/opmn/bin/opmnctl startall
```

where *ORACLE_HOME* is the home for Oracle Enterprise Manager 10*g* Release 2 Grid Control.

A.4 Installing Oracle Identity Management Grid Control Plug-in Agent

The Oracle Identity Management Grid Control Plug-in Agent should always be installed on the same computer as the Oracle Identity Management components. If Oracle Identity Management and Oracle Enterprise Manager Grid Control are not installed on the same host, then the Oracle Management Agent must be installed on the same host as Oracle Identity Management before the Oracle Identity Management Grid Control Plug-in Agent can be installed. See *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for details on installing Oracle Management Agent.

▪

Perform the following steps to install Oracle Identity Management Grid Control Plug-in Agent:

1. Log on to the Oracle Enterprise Manager 10*g* Grid Control Console using the following URL:

   ```
   http://oms_host:oms_port/em
   ```

2. Click the **Deployments** tab.
3. Click **View Patch Cache**.
4. If this is your first time installing the Grid Control Plug-in Agent, click **Upload Patch File**. If you have already uploaded the patch, skip to the next step.

   On the Add Patch File to Patch Cache screen, fill in the following fields:

   Patch File: Enter the location of the Grid Control Plug-in Agent patch.

   Patch Number: Enter "6050709" as the patch number.

   Patch Type: Select **Patch set**.

   Created On: This field is automatically filled in with the current date.

   Description: Enter a description for the patch.

Product Family: Select **Oracle System Management Products**.

Product: Click on the flashlight icon and select **Intelligent Agent** from the box.

Release: Enter "10.2.0.3.0" as the release number. Note that you must enter the numbers manually. Do not use any of the numbers from the list.

Platform: Select the operating system for the patch.

Language: Select your language.

Click **Upload** to upload the patchset.

5. On the Patch Cache screen, select the patchset to be applied and click **Patch**.
6. On the Patch: Select Destination screen, select **Oracle Homes** in the **Destination Type** box.
7. Under **Available Homes**, select the Oracle Home(s) where the patch should be applied and click **Move**.
8. Click **Next**.
9. On the Patch: Set Credentials screen, enter the **Username** and **Password** for the Oracle Home and click **Next**.
10. On the Patch: Stage or Apply screen, click **Next**.
11. On the Patch: Schedule screen, specify when the patch should be applied in the **Schedule Patch Job** section and click **Next**.
12. Review the details on the Patch: Summary screen and click **Next**.

B

Silent and Non-Interactive Installation

This appendix describes how to install Oracle Application Server in silent mode. This appendix contains the following topics:

- Section B.1, "Silent Installation"
- Section B.2, "Non-Interactive Installation"
- Section B.3, "Pre-Installation"
- Section B.4, "Notes for Silent and Non-Interactive Installations"
- Section B.5, "Create the Response File"
- Section B.6, "Start the Installation"
- Section B.7, "Post-Installation"
- Section B.8, "Security Tips for Silent and Non-Interactive Installations"
- Section B.9, "Deinstallation"

B.1 Silent Installation

Silent installation eliminates the need to monitor the Oracle Application Server installation because there is no graphical output and no input by the user.

Silent installation of Oracle Application Server is accomplished by supplying the Oracle Universal Installer with a response file and specifying the `-silent` flag on the command line. The response file is a text file containing variables and parameter values which provide answers to the installer prompts.

If this is a first time installation of Oracle Application Server, you must create the oraInst.loc file before starting. File creation is described in Section B.3, "Pre-Installation".

Following installation of Oracle Application Server, you need to run the `root.sh` script as the root user. The `root.sh` script detects settings of environment variables and enables you to enter the full path of the local bin directory.

Use silent installation of Oracle Application Server when there are similar installations on more than one computer. Additionally, use silent install when performing the Oracle Application Server installation from a remote location using the command line.

B.2 Non-Interactive Installation

Non-interactive installations also use a response file to automate the Oracle Application Server installation. In non-interactive installations, there is graphical output and users may enter input.

Non-interactive installation of Oracle Application Server is also accomplished by supplying the Oracle Universal Installer with a response file but without specifying the `-silent` flag on the command line. The response file is a text file containing variables and parameter values which provide answers to the installer prompts. If you have not provided responses to all of the installer prompts, you need to enter information during the installation.

If this is a first time installation of Oracle Application Server, you must create the oraInst.loc file before starting. File creation is described in Section B.3, "Pre-Installation".

Following installation of Oracle Application Server, you need to run the `root.sh` script as the root user. The `root.sh` script detects settings of environment variables and enables you to enter the full path of the local bin directory.

Use non-interactive installation of Oracle Application Server when there are specific screens you want to observe during installation.

B.3 Pre-Installation

1. Log in as the root user.

   ```
   prompt> su
   ```

2. As root user, create the `/var/opt/oracle` directory, if it does not already exist.

   ```
   # mkdir /var/opt/oracle
   ```

3. Create the `/var/opt/oracle/oraInst.loc` file. This file specifies the inventory directory that the installer will use.

   Using a text editor such as vi or emacs, enter the following line in the file:

   ```
   inventory_loc=oui_inventory_directory
   ```

   Replace *oui_inventory_directory* with the full path to the directory where you want the installer to create the inventory directory. For example:

   ```
   inventory_loc=/opt/oracle/oraInventory
   ```

   Make sure that the `oinstall` operating system group has write permissions to this directory. For more information about the inventory directory and the group that owns it, see Section 2.7.1, "Create a Group for the Inventory Directory".

4. Create an empty `/var/opt/oracle/oratab` file.

   ```
   # touch /var/opt/oracle/oratab
   ```

5. Exit from the root user.

   ```
   # exit
   ```

B.4 Notes for Silent and Non-Interactive Installations

This section describes special cases that are applicable when you are performing silent or non-interactive installations.

- Section B.4.1, "Installing OracleAS Certificate Authority"

B.4.1 Installing OracleAS Certificate Authority

If you are installing OCA, check the following:

- If you are installing OCA against an existing Oracle Internet Directory, make sure the Oracle Internet Directory has OracleAS Single Sign-On configured. If not, the OCA Configuration Assistant will fail.
- If you are installing OCA with a new Oracle Internet Directory, make sure you are also configuring OracleAS Single Sign-On. If not, the OCA Configuration Assistant will fail.

In interactive mode, the installer performs the checks for you and displays a warning if the requirements are not met. However, in silent or non-interactive mode, the installer is not able to display a warning.

B.5 Create the Response File

Before doing a silent or non-interactive installation, you must provide information specific to your installation in a response file. The installer will fail if you attempt an installation using a response file that is not configured correctly. Response files are text files that you can create or edit in a text editor.

B.5.1 Creating Response Files from Templates

Templates for response files are available in the `stage/Response` directory on Disk 1 of the Oracle Application Server CD-ROM. Response file templates are available for the following installation types:

Table B–1 Response File Templates in the stage/Response Directory

Installation Type	Filename
OracleAS Infrastructure: Oracle Identity Management and OracleAS Metadata Repository	`oracle.iappserver.infrastructure.Infrastructure.rsp`
OracleAS Infrastructure: Oracle Identity Management only	`oracle.iappserver.infrastructure.Infrastructure_ID.rsp`
OracleAS Infrastructure: OracleAS Metadata Repository only	`oracle.iappserver.infrastructure.Infrastructure_Meta.rsp`
Oracle Identity Federation	`oracle.iappserver.security.fed.Core.rsp`

See the template files for descriptions of the parameters in the file.

Note: For Boolean parameters, specify either "true" or "false".

B.5.2 Creating Response Files by Using the Record Mode in the Installer

You can run the installer in record mode to save your inputs to a file that you can use later as a response file. This feature is useful if you need to perform the same installation on different computers.

To run the installer in record mode:

1. Start up the installer with the `-record` and `-destinationFile` parameters.

   ```
   prompt> /path/to/runInstaller -record -destinationFile newResponseFile
   ```

   Replace *newResponseFile* with the full path to the response file that you want the installer to create. Example: `/opt/oracle/myInfraResponse.rsp`.

2. Enter your values in the installer screens. The installer will write these values to the file specified in the `-destinationFile` parameter.

   When you get to the Summary screen, the installer automatically writes all your values to the specified file. At this point, you can complete the installation on this computer, or you can exit without performing the installation.

Secure information, such as passwords, is not written to the file, so you must modify the response file before you can use it.

B.5.3 Variables to Modify in the Response Files

For all installation types, modify the following variables:

```
UNIX_GROUP_NAME
FROM_LOCATION
ORACLE_HOME
szl_PortListSelect
oracle.iappserver.instance:szl_InstanceInformation
```

See the response file for descriptions of the parameters in the file.

B.5.4 Example Response Files

The following sections shows example response files for the following Oracle Application Server installation types:

- Section B.5.4.1, "Example Response File for OracleAS Infrastructure: Oracle Identity Management Only"
- Section B.5.4.2, "Example Response File for OracleAS Infrastructure: OracleAS Metadata Repository Only"
- Section B.5.4.3, "Example Response File for OracleAS Infrastructure: Identity Management and OracleAS Metadata Repository"
- Section B.5.4.4, "Example Response File for Oracle Identity Federation"

Note: Be sure that you read the description of each *parameter=value* in the provided sample files, and edit *value* accordingly for your environment.

B.5.4.1 Example Response File for OracleAS Infrastructure: Oracle Identity Management Only

The following shows an example of a response file for a **silent** installation of OracleAS Infrastructure as described in Section 4.23, "Installing Oracle Identity Management Components Only (Including Oracle Internet Directory)".

Note that if you do not copy the CD-ROMs to the hard drive, the installer will prompt you to switch CD-ROMs during installation. To complete the installation without any prompting, you must copy the contents of the CD-ROMs to the hard drive and specify the `LOCATION_FOR_DISK`*n* parameters.

```
RESPONSEFILE_VERSION=2.2.1.0.0
UNIX_GROUP_NAME="dba"
FROM_LOCATION="/mount_point/Disk1/stage/products.xml"
FROM_LOCATION_CD_LABEL="Oracle Application Server 10g"
LOCATION_FOR_DISK2="/path/to/disk2/files"
ORACLE_HOME="/local_location/oracle_home"
ORACLE_HOME_NAME="oracle_imhome_name"
SHOW_SPLASH_SCREEN=false
SHOW_WELCOME_PAGE=false
SHOW_INSTALL_PROGRESS_PAGE=false
SHOW_COMPONENT_LOCATIONS_PAGE=false
SHOW_CUSTOM_TREE_PAGE=false
SHOW_SUMMARY_PAGE=false
SHOW_REQUIRED_CONFIG_TOOL_PAGE=false
SHOW_OPTIONAL_CONFIG_TOOL_PAGE=false
SHOW_RELEASE_NOTES=false
SHOW_ROOTSH_CONFIRMATION=false
SHOW_END_SESSION_PAGE=false
SHOW_EXIT_CONFIRMATION=false
NEXT_SESSION=false
NEXT_SESSION_ON_FAIL=false
SHOW_DEINSTALL_CONFIRMATION=false
SHOW_DEINSTALL_PROGRESS=false
oracle.iappserver.infrastructure:SHOW_IAS_COMPONENT_CONFIG_PAGE=false
ACCEPT_LICENSE_AGREEMENT=true
RESTART_SYSTEM=<Value Unspecified>
CLUSTER_NODES=<Value Unspecified>

OUI_HOSTNAME=im_host.mycompany.com

PreReqConfigSelections=""
n_ValidationPreReqConfigSelections=0
TOPLEVEL_COMPONENT={"oracle.iappserver.infrastructure","10.1.4.0.1"}
DEINSTALL_LIST={"oracle.iappserver.infrastructure","10.1.4.0.1"}
oracle.iappserver.infrastructure:szl_
PortListSelect={"YES","/private/jdoe/mystaticports.ini"}
COMPONENT_LANGUAGES={"en"}
INSTALL_TYPE="Infrastructure_ID"

oracle.iappserver.infrastructure:b_configureMETA=false
oracle.iappserver.infrastructure:b_configureOID=true
oracle.iappserver.infrastructure:b_configureSSO=true
oracle.iappserver.infrastructure:b_configureDAS=true
oracle.iappserver.infrastructure:b_configureDIP=true
oracle.iappserver.infrastructure:b_configureOCA=true
oracle.iappserver.infrastructure:b_configureHA=false
oracle.iappserver.infrastructure:b_launchEMCA=true
oracle.iappserver.infrastructure:b_launchOHS=true
```

```
# Meta Repository Connection Info ( for OID )
oracle.iappserver.iappdialog:szl_RepositoryUserInput={"sys", "syspassword", "mr_
host.mycompany.com:1521", "", "", "mr.mycompany.com", ""}
# Meta Repository Connection Info ( for OCA )
oracle.iappserver.iappdialog:szl_OCARepositoryUserInput={"mr_
host.mycompany.com:1521:mr:mr.mycompany.com"}
szIdentityAdminContext="dc=mycompany,dc=com"
s_dnSelection="Custom DN:"
s_dnCntval="United States"
s_dncustom="CN=My Certificate Authority,OU=MyOrg,O=MyCompany,C=US"
sl_keylengthInfo={"2048"}
sl_ocmInfo={"adminpassword","adminpassword"}

oracle.oid.oidca:s_silentinstallflag="1"

oracle.iappserver.infrastructure:b_configureCentralMon=false

szOIDwithSSLStatus="N"
nValidationOID2=0
nValidationOID=0
nValidationRepository=0

oracle.iappserver.instance:szl_
InstanceInformation={"instancename","instancepassword","instancepassword"}
oracle.iappserver.instance:nValidationInstanceInfo=0
oracle.apache.apache:s_group=dba
oracle.apache.apache:s_groupid=dba
oracle.iappserver.iapptop:szl_InstanceInformation={"instancepassword"}
```

B.5.4.2 Example Response File for OracleAS Infrastructure: OracleAS Metadata Repository Only

The following shows an example of a response file for a **silent** installation of OracleAS Infrastructure as described in Section 4.22, "Installing OracleAS Metadata Repository in a New Database".

Note that if you do not copy the CD-ROMs to the hard drive, the installer will prompt you to switch CD-ROMs during installation. To complete the installation without any prompting, you must copy the contents of the CD-ROMs to the hard drive and specify the `LOCATION_FOR_DISK`*n* parameters.

```
RESPONSEFILE_VERSION=2.2.1.0.0
UNIX_GROUP_NAME="dba"
FROM_LOCATION="/mount_point/Disk1/stage/products.xml"
FROM_LOCATION_CD_LABEL="Oracle Application Server 10g"
LOCATION_FOR_DISK2="/path/to/disk2/files"
ORACLE_HOME="/local_location/oracle_home"
ORACLE_HOME_NAME="oracle_mrhome_name"
SHOW_SPLASH_SCREEN=false
SHOW_WELCOME_PAGE=false
SHOW_INSTALL_PROGRESS_PAGE=false
SHOW_COMPONENT_LOCATIONS_PAGE=false
SHOW_CUSTOM_TREE_PAGE=false
SHOW_SUMMARY_PAGE=false
SHOW_REQUIRED_CONFIG_TOOL_PAGE=false
SHOW_OPTIONAL_CONFIG_TOOL_PAGE=false
SHOW_RELEASE_NOTES=false
SHOW_ROOTSH_CONFIRMATION=false
SHOW_END_SESSION_PAGE=false
SHOW_EXIT_CONFIRMATION=false
```

```
NEXT_SESSION=false
NEXT_SESSION_ON_FAIL=false
SHOW_DEINSTALL_CONFIRMATION=false
SHOW_DEINSTALL_PROGRESS=false
oracle.iappserver.infrastructure:SHOW_IAS_COMPONENT_CONFIG_PAGE=false
ACCEPT_LICENSE_AGREEMENT=true
RESTART_SYSTEM=<Value Unspecified>
CLUSTER_NODES=<Value Unspecified>

OUI_HOSTNAME=mr_host.mycompany.com

PreReqConfigSelections=""
n_ValidationPreReqConfigSelections=0
TOPLEVEL_COMPONENT={"oracle.iappserver.infrastructure","10.1.4.0.1"}
DEINSTALL_LIST={"oracle.iappserver.infrastructure","10.1.4.0.1"}
oracle.iappserver.infrastructure:szl_
PortListSelect={"YES","/private/jdoe/mystaticports.ini"}
COMPONENT_LANGUAGES={"en"}
INSTALL_TYPE="Infrastructure_Meta"

oracle.iappserver.infrastructure:b_configureMETA=true
oracle.iappserver.infrastructure:b_configureOID=false
oracle.iappserver.infrastructure:b_configureSSO=false
oracle.iappserver.infrastructure:b_configureSSO=false
oracle.iappserver.infrastructure:b_configureDAS=false
oracle.iappserver.infrastructure:b_configureDIP=false
oracle.iappserver.infrastructure:b_configureOCA=false
oracle.iappserver.infrastructure:b_launchEMCA=false
oracle.iappserver.infrastructure:b_launchOHS=true
szRegisterMetaStatus="N"
szIdentityAdminContext="dc=mycompany,dc=com"
s_dnSelection="Custom DN:"
s_dnCntval="United States"
s_dncustom="CN=AS Certificate Authority,OU=MyOrg,O=MyCompany,C=US"
sl_keylengthInfo={"2048"}
sl_ocmInfo={"adminpassword","adminpassword"}


s_nameForDBAGrp="dba"
s_nameForOPERGrp="dba"
## Specify Database Configuration Options
s_dbRetChar="Unicode standard UTF-8 AL32UTF8"
s_dbSid=mr
s_globalDBName=mr.mycompany.com
b_loadExampleSchemas=false

## Specify Database Management Option
s_dlgEMEmailNotificationSelected="N"
s_dlgEMOptionSelected="Use Database Control for Database Management"
s_dlgEMCentralAgentSelected="No Agents Found"
s_dlgEMSMTPServer=""
s_dlgEMEmailAddress=""

## Specify Database File Storage Option
s_DataorASMret="File System"
s_mountPoint=/local_location/oradata

## Specify Backup and Recovery Options
s_dlgRBOEnableAutoBackups="Do not enable Automated backups"
```

```
## Specify Database Schema Passwords
s_superAdminPasswdType="S"
s_superAdminSamePasswd="schemapassword"
s_superAdminSamePasswdAgain="schemapassword"

## Select Database Configuration
s_dlgStarterDBConfigCreateStarterDB="Create a starter database"
s_dlgStarterDBConfigOptionSelected="General Purpose"

oracle.oid.oidca:s_silentinstallflag="1"

oracle.iappserver.infrastructure:b_configureCentralMon=false

szOIDwithSSLStatus="N"
nValidationOID2=0
nValidationOID=0
nValidationRepository=0

oracle.iappserver.instance:szl_
InstanceInformation={"instancename","instancepassword","instancepassword"}
oracle.iappserver.instance:nValidationInstanceInfo=0
oracle.apache.apache:s_group=dba
oracle.apache.apache:s_groupid=dba
oracle.iappserver.iapptop:szl_InstanceInformation={"instancepassword"}
```

B.5.4.3 Example Response File for OracleAS Infrastructure: Identity Management and OracleAS Metadata Repository

The following shows an example of a response file for a **silent** installation of OracleAS Infrastructure as described in Section 4.20, "Installing OracleAS Infrastructure".

Note that if you do not copy the CD-ROMs to the hard drive, the installer will prompt you to switch CD-ROMs during installation. To complete the installation without any prompting, you must copy the contents of the CD-ROMs to the hard drive and specify the `LOCATION_FOR_DISK`*n* parameters.

```
RESPONSEFILE_VERSION=2.2.1.0.0
UNIX_GROUP_NAME="dba"
FROM_LOCATION="/mount_point/Disk1/stage/products.xml"
FROM_LOCATION_CD_LABEL="Oracle Application Server 10g"
LOCATION_FOR_DISK2="/path/to/disk2/files"
ORACLE_HOME="/local_location/oracle_home"
ORACLE_HOME_NAME="oracle_infrahome_name"
SHOW_SPLASH_SCREEN=false
SHOW_WELCOME_PAGE=false
SHOW_INSTALL_PROGRESS_PAGE=false
SHOW_COMPONENT_LOCATIONS_PAGE=false
SHOW_CUSTOM_TREE_PAGE=false
SHOW_SUMMARY_PAGE=false
SHOW_REQUIRED_CONFIG_TOOL_PAGE=false
SHOW_OPTIONAL_CONFIG_TOOL_PAGE=false
SHOW_RELEASE_NOTES=false
SHOW_ROOTSH_CONFIRMATION=false
SHOW_END_SESSION_PAGE=false
SHOW_EXIT_CONFIRMATION=false
NEXT_SESSION=false
NEXT_SESSION_ON_FAIL=false
SHOW_DEINSTALL_CONFIRMATION=false
SHOW_DEINSTALL_PROGRESS=false
oracle.iappserver.infrastructure:SHOW_IAS_COMPONENT_CONFIG_PAGE=false
```

```
ACCEPT_LICENSE_AGREEMENT=true
RESTART_SYSTEM=<Value Unspecified>
CLUSTER_NODES=<Value Unspecified>

OUI_HOSTNAME=infra_host.mycompany.com

PreReqConfigSelections=""
n_ValidationPreReqConfigSelections=0
TOPLEVEL_COMPONENT={"oracle.iappserver.infrastructure","10.1.4.0.1"}
DEINSTALL_LIST={"oracle.iappserver.infrastructure","10.1.4.0.1"}
oracle.iappserver.infrastructure:szl_
PortListSelect={"YES","/private/jdoe/mystaticports.ini"}
COMPONENT_LANGUAGES={"en"}
INSTALL_TYPE="Infrastructure"

oracle.iappserver.infrastructure:b_configureMETA=true
oracle.iappserver.infrastructure:b_configureOID=true
oracle.iappserver.infrastructure:b_configureSSO=true
oracle.iappserver.infrastructure:b_configureDAS=true
oracle.iappserver.infrastructure:b_configureDIP=true
oracle.iappserver.infrastructure:b_configureOCA=true
oracle.iappserver.infrastructure:b_configureHA=false
oracle.iappserver.infrastructure:b_launchEMCA=true
oracle.iappserver.infrastructure:b_launchOHS=true
szRegisterMetaStatus="N"
szIdentityAdminContext="dc=mycompany,dc=com"
s_dnSelection="Custom DN:"
s_dnCntval="United States"
s_dncustom="CN=My Certificate Authority,OU=MyOrg,O=MyCompany,C=US"
sl_keylengthInfo={"2048"}
sl_ocmInfo={"adminpassword","adminpassword"}


s_nameForDBAGrp="dba"
s_nameForOPERGrp="dba"
## Specify Database Configuration Options
s_dbRetChar="Unicode standard UTF-8 AL32UTF8"
s_dbSid=inf7296
s_globalDBName=infra_host.mycompany.com
b_loadExampleSchemas=false

## Specify Database Management Option
s_dlgEMEmailNotificationSelected="N"
s_dlgEMOptionSelected="Use Database Control for Database Management"
s_dlgEMCentralAgentSelected="No Agents Found"
s_dlgEMSMTPServer=""
s_dlgEMEmailAddress=""

## Specify Database File Storage Option
s_DataorASMret="File System"
s_mountPoint=/local_location/oradata

## Specify Backup and Recovery Options
s_dlgRBOEnableAutoBackups="Do not enable Automated backups"

## Specify Database Schema Passwords
s_superAdminPasswdType="S"
s_superAdminSamePasswd="schemapassword"
s_superAdminSamePasswdAgain="schemapassword"
```

```
## Select Database Configuration
s_dlgStarterDBConfigCreateStarterDB="Create a starter database"
s_dlgStarterDBConfigOptionSelected="General Purpose"

oracle.oid.oidca:s_silentinstallflag="1"

oracle.iappserver.infrastructure:b_configureCentralMon=false

szOIDwithSSLStatus="N"
nValidationOID2=0
nValidationOID=0
nValidationRepository=0

oracle.iappserver.instance:szl_
InstanceInformation={"instancename","instancepassword","instancepassword"}
oracle.iappserver.instance:nValidationInstanceInfo=0
oracle.apache.apache:s_group=dba
oracle.apache.apache:s_groupid=dba
oracle.iappserver.iapptop:szl_InstanceInformation={"instancepassword"}
```

B.5.4.4 Example Response File for Oracle Identity Federation

The following shows an example of a response file for a **silent** installation of Oracle Identity Federation as described in *Oracle Identity Federation Administrator's Guide*.

Note that if you do not copy the CD-ROMs to the hard drive, the installer will prompt you to switch CD-ROMs during installation. To complete the installation without any prompting, you must copy the contents of the CD-ROMs to the hard drive and specify the `LOCATION_FOR_DISK`*n* parameters.

```
RESPONSEFILE_VERSION=2.2.1.0.0
UNIX_GROUP_NAME="dba"
FROM_LOCATION="/mount_point/Disk1/stage/products.xml"
FROM_LOCATION_CD_LABEL="Oracle Application Server 10g"
LOCATION_FOR_DISK2="/path/to/disk2/files"
ORACLE_HOME="/local_location/oracle_home"
ORACLE_HOME_NAME="oracle_fedhome_name"
SHOW_SPLASH_SCREEN=false
SHOW_WELCOME_PAGE=false
SHOW_INSTALL_PROGRESS_PAGE=false
SHOW_COMPONENT_LOCATIONS_PAGE=false
SHOW_CUSTOM_TREE_PAGE=false
SHOW_SUMMARY_PAGE=false
SHOW_REQUIRED_CONFIG_TOOL_PAGE=false
SHOW_OPTIONAL_CONFIG_TOOL_PAGE=false
SHOW_RELEASE_NOTES=false
SHOW_ROOTSH_CONFIRMATION=false
SHOW_END_SESSION_PAGE=false
SHOW_EXIT_CONFIRMATION=false
NEXT_SESSION=false
NEXT_SESSION_ON_FAIL=false
SHOW_DEINSTALL_CONFIRMATION=false
SHOW_DEINSTALL_PROGRESS=false
oracle.iappserver.security.fed:SHOW_IAS_COMPONENT_CONFIG_PAGE=false
ACCEPT_LICENSE_AGREEMENT=true
RESTART_SYSTEM=<Value Unspecified>
CLUSTER_NODES=<Value Unspecified>

OUI_HOSTNAME=fed_host.mycompany.com
```

```
PreReqConfigSelections=""
n_ValidationPreReqConfigSelections=0
TOPLEVEL_COMPONENT={"oracle.iappserver.security.fed","10.1.4.0.1"}
DEINSTALL_LIST={"oracle.iappserver.security.fed","10.1.4.0.1"}
SELECTED_LANGUAGES={"en"}

#INSTALL_TYPE="Basic"
n_DefAdvTypeInstall=0
nValidationConfigSelection=0
#startupProcesses="Federation Record Store in LDAP Server"

iASinstanceName="fed"
s_OSFSserverID="fed.fed_host.mycompany.com"
iASinstancePW="instancepassword"
iASinstancePWConfirm="instancepassword"
```

B.6 Start the Installation

To make the installer use the response file, specify the location of the response file that you want to use as a parameter when starting the installer.

To perform a non-interactive installation:

```
prompt> setenv DISPLAY hostname:0.0
prompt> runInstaller -responseFile absolute_path_and_filename
```

To perform a silent installation, use the `-silent` parameter:

```
prompt> runInstaller -silent -responseFile absolute_path_and_filename
```

B.7 Post-Installation

The success or failure of the non-interactive and silent installations is logged in the `installActions<time_stamp>.log` file. Additionally, the silent installation creates the `silentInstall<time_stamp>.log` file. The log files are created in the `oraInventory` directory.

The `silentInstall<time_stamp>.log` file contains the following line if the installation was successful:

```
The installation of OracleAS <Installation Type> was successful.
```

The `installActions<time_stamp>.log` file contains specific information for each Oracle Application Server installation type.

See Also: Appendix E, "Configuration Assistants"

Note: Application Server Control Configuration Assistant and DCM Repository Backup Assistant success messages appear for first time installation of Oracle Application Server.

B.8 Security Tips for Silent and Non-Interactive Installations

One of the pieces of information in the response file is the installation password. The password information is in clear text.

To minimize security issues regarding the password in the response file, follow these guidelines:

- Set the permissions on the response files so that they are readable only by the operating system user who will be performing the silent or non-interactive installation.
- If possible, remove the response files from the system after the silent or non-interactive installation is completed.

If you are installing the OracleAS Metadata Repository in silent or non-interactive mode, the installer creates these log files:

- `ORACLE_HOME/admin/<ORACLE_SID>/create/<ORACLE_SID>.log`
- `ORACLE_HOME/cfgtoollogs/<ORACLE_SID>.log`

where `<ORACLE_SID>` is the value of your database SID.

These log files contain database password information. If possible, you should remove these files from the system after reviewing their contents. These log files are not required for the operation of OracleAS Metadata Repository.

B.9 Deinstallation

You can perform a silent deinstallation of Oracle Application Server by supplying a silent deinstallation parameter to the response file you used for installation.

Add the following parameter to your installation response file:

```
REMOVE_HOMES={"<ORACLE_HOME to be removed>"}
```

For example:

```
REMOVE_HOME="/local_location/oracle_home"
```

> **Note:** You still need to follow the deinstallation steps described in Appendix D, "Deinstallation and Reinstallation". One of the key steps is to run the deconfig tool before running the silent deinstallation command. The silent deinstallation command only replaces the step where you run the installer interactively to deinstall the instance.

To perform a silent deinstallation, use the `-deinstall` parameter when entering the command:

```
prompt> runInstaller -silent -deinstall -responseFile absolute_path_and_filename
```

C

Default Port Numbers

By default, the installer assigns port numbers to components from a set of default port numbers. This appendix contains a list of these port numbers.

If you want to use a different set of port numbers, you have to create a file called staticports.ini, in which you list the port numbers that you want to use. See Section 2.6.3, "Using Custom Port Numbers (the "Static Ports" Feature)" for details.

This appendix contains the following sections:

- Section C.1, "Method of Assigning Default Port Numbers"
- Section C.2, "Default Port Numbers"
- Section C.3, "Ports to Open in Firewalls"

C.1 Method of Assigning Default Port Numbers

The installer assigns default port numbers to each component using the following method:

1. The installer checks if the default port number is in use. If it is not in use, the installer assigns it to the component.
2. If the default port number is already in use by an Oracle product or by any running application, the installer tries the lowest number in the port number range. It keeps trying the port numbers in the range until it finds one that is available.

C.2 Default Port Numbers

Table C–1 lists the default port numbers for components. The last column, Name in staticports.ini, specifies the component name as it appears in the `staticports.ini` file, which enables you to override the default port numbers. See Section 2.6.3, "Using Custom Port Numbers (the "Static Ports" Feature)" for details.

Table C–1 Default Port Numbers and Ranges (Grouped by Component)

Component	Default Port	Port Number Range	Name in staticports.ini
Oracle Process Manager and Notification Server (OPMN)			
Oracle Notification Server Request Port	6003	6003 - 6099	`Oracle Notification Server Request port`
Oracle Notification Server Local Port	6100	6100 - 6199	`Oracle Notification Server Local port`
Oracle Notification Server Remote Port	6200	6200 - 6299	`Oracle Notification Server Remote port`
Oracle Application Server Containers for J2EE (OC4J)			
OC4J AJP	12501	12501 - 12600	Not settable through staticports.ini
OC4J RMI	12401	12401 - 12500	Not settable through staticports.ini
JMS	12601	12601 - 12700	Not settable through staticports.ini
IIOP	13301	13301 - 13400	Not settable through staticports.ini
IIOPS1	13401	13401 - 13500	Not settable through staticports.ini
IIOPS2	13501	13501 -13600	Not settable through staticports.ini
Oracle HTTP Server			
Oracle HTTP Server Listen Port	7777	7777 - 7877	`Oracle HTTP Server Listen port`
Oracle HTTP Server Listen (SSL)	4443	4443-4543, 8250-8350	`Oracle HTTP Server Listen (SSL) port`
Oracle HTTP Server Port	7777	7777 - 7877	`Oracle HTTP Server port`
Oracle HTTP Server SSL Port	4443	443, 4443-4543, 8250-8350	`Oracle HTTP Server SSL port`
Java Object Cache	7000	7000 - 7099	`Java Object Cache port`
DCM Discovery	7100	7100-7199	`DCM Discovery port`
Port Tunneling	7501	7501 - 7599	Not settable through staticports.ini
Oracle HTTP Server Diagnostic port	7200	7200 - 7299	`Oracle HTTP Server Diagnostic port`
OracleAS Single Sign-On			
OracleAS Single Sign-On	--	--	Uses the same port as Oracle HTTP Server Listener.
Oracle Enterprise Manager 10*g* Application Server Control			
Application Server Control Console	1156	1156; 1810 - 1829, 18100 - 18119	`Application Server Control port`

Table C–1 (Cont.) Default Port Numbers and Ranges (Grouped by Component)

Component	Default Port	Port Number Range	Name in staticports.ini
Oracle Management Agent	1157	1157; 18120 - 18139	`Oracle Management Agent port`
Application Server Control - RMI	1850	1850-1869, 18140 - 18159	`Application Server Control RMI port`
Application Server Control Console - SSL	1156	1156; 1810 - 1829, 18100 - 18119	This port number is assigned after installation, when you configure Application Server Control for SSL. See the *Oracle Application Server Administrator's Guide* for details.
Enterprise Manager Console HTTP port (orcl)	5500	5500 - 5559	Not settable through staticports.ini
Enterprise Manager Agent port (orcl)	1831		Not settable through staticports.ini
Log Loader	44000	44000 - 44099	`Log Loader port`
Oracle Internet Directory			
Oracle Internet Directory	389 (but see the Note on page 2-13)	389, 13060 - 13129	`Oracle Internet Directory port`
Oracle Internet Directory (SSL)	636 (but see the Note on page 2-13)	636, 13130 - 13159, 13161-13199	`Oracle Internet Directory (SSL) port`
Oracle Application Server Certificate Authority (OCA)			
Server Authentication Virtual Host (SSL)	6600	6600 - 6619	`Oracle Certificate Authority SSL Server Authentication port`
Mutual Authentication Virtual Host (SSL)	6601	6600 - 6619	`Oracle Certificate Authority SSL Mutual Authentication port`
Oracle Application Server Guard			
Oracle Application Server Guard	7890	7890-7895	`ASG port`
OracleAS Metadata Repository			
Oracle Net Listener	1521	1521	Not settable through staticports.ini
Oracle Identity Federation			
Oracle Identity Federation	--	--	Uses the same port as Oracle HTTP Server Listener.

C.3 Ports to Open in Firewalls

If you plan to install Oracle Application Server behind a firewall, you need to open certain ports in the firewall during installation and during runtime.

For a 10*g* (10.1.4.0.1) instance, you need access to Oracle Internet Directory, OracleAS Metadata Repository, Oracle Notification Server, and SJP ports. You need to open the following ports used by these components in the firewall

- LDAP: port 389
- LDAP SSL: port 636
- SQL*Net 2: port 1521
- OPMN ONS remote: port 6200
- OC4J AJP: port 12501

Note: The port numbers listed here are the default ports for the components. You may have different ports in your environment.

D

Deinstallation and Reinstallation

This appendix guides you through the deinstallation and reinstallation process for Oracle Application Server.

- Section D.1, "Deconfig Tool"
- Section D.2, "Deinstallation Procedure: Overview"
- Section D.3, "Deinstalling OracleAS Cold Failover Cluster Installations"
- Section D.4, "Deinstalling OracleAS Single Sign-On Instances in OracleAS Cluster (Identity Management)"
- Section D.5, "Deinstalling OracleAS Cluster (Identity Management)"
- Section D.6, "Deinstalling OracleAS Infrastructure"
- Section D.7, "Harmless Errors in the Log File"
- Section D.8, "Cleaning Up Oracle Application Server Processes"
- Section D.9, "Reinstallation"
- Section D.10, "Troubleshooting"

D.1 Deconfig Tool

In this release, there is a tool called the Deconfig tool that you need to run as part of the deinstallation procedure. This tool removes entries in OracleAS Metadata Repository and Oracle Internet Directory for the Oracle Application Server instance that you want to deinstall.

The Deconfig tool does not remove partner application entries. If you need to remove partner application entries, follow the steps in Section F.4.1, "Obsolete Partner URLs Still Remain on the OracleAS Single Sign-On Administration Screen".

The Deconfig tool does not remove OracleAS Clusters from the farm. If you are deinstalling OracleAS Clusters, you will need to run the `dcmctl removecluster` command after deinstalling the instances. See Section D.5, "Deinstalling OracleAS Cluster (Identity Management)"for details.

To run the Deconfig tool, run the Perl interpreter on the `ORACLE_HOME/bin/deconfig.pl` script. Use the Perl interpreter provided with Oracle Application Server.

```
prompt> cd $ORACLE_HOME/bin
prompt> $ORACLE_HOME/perl/bin/perl deconfig.pl [-u oid_user]
            [-w password] [-r realm] [-dbp sys_db_password]
```

If you run it without all of the parameters, the tool prompts you for the necessary information.

> **Note:** For security reasons, it is not recommended that you specify the password on the command line. The Deconfig tool will prompt you for the password if you do not specify it on the command line.

D.1.1 Parameters

-u *oid_user*

Specify the Oracle Internet Directory user.

You can specify the Oracle Internet Directory user using the user's simple name or the user's distinguished name (DN). For example, the user's simple name can be `jdoe@mycompany.com`, which corresponds to the DN `cn=jdoe,l=us,dc=mycompany,dc=com`.

The Oracle Internet Directory user needs to have privileges for deinstalling the components that are configured in the Oracle Application Server instance that you want to deinstall. These privileges are the same as for installing and configuring the component.

For example, if you are deinstalling an OracleAS Infrastructure instance that is running Oracle Delegated Administration Services and OracleAS Single Sign-On, make sure the user has privileges to configure these components. For a list of components and groups that grant the privileges, see Section 5.3, "Groups Required to Configure or Deinstall Components".

If you want to run the tool as the Oracle Internet Directory superuser, be sure to use `cn=orcladmin`, and not just `orcladmin`. These are two different users. If you want more details about these users, see Section 5.1, "Default Users in Oracle Internet Directory".

-w *password*

Specify the password for the Oracle Internet Directory user.

-r *realm*

Specify the realm in which to authenticate the user. This value is required only if your Oracle Internet Directory has more than one realm.

-dbp *sys_db_password*

Specify the password for the SYS user in the database. This is the OracleAS Metadata Repository database used by Oracle Internet Directory.

This value is required only if you are deinstalling an Oracle Identity Management-only instance that has Oracle Internet Directory configured.

If you specify this parameter and it is not needed, the password value is simply not used.

-help or -h

You can also run the Deconfig tool with the `-h` or `-help` parameter to display help:

```
prompt> $ORACLE_HOME/perl/bin/perl deconfig.pl -h
 - or -
prompt> $ORACLE_HOME/perl/bin/perl deconfig.pl -help
```

D.1.2 Log Files Generated by the Deconfig Tool

The Deconfig tool writes its log file to the `ORACLE_HOME/cfgtoollogs/DeconfigureWrapper.log` file.

D.2 Deinstallation Procedure: Overview

Follow these high-level steps to deinstall Oracle Application Server:

1. Deinstall middle-tier instances first. See *Oracle Application Server Installation Guide* for the middle-tier platform and release for deinstallation instructions.
   a. Run the Deconfig tool on the instance.
   b. Run the installer and click the **Deinstall Products** button.
   c. Clean up any remaining files.
2. Then deinstall OracleAS Infrastructure instances. The deinstallation details are provided later in this chapter.
   a. Run the Deconfig tool on the instance.
   b. Run the installer and click the **Deinstall Products** button.
   c. Clean up any remaining files.

Notes:

- If you used OracleAS RepCA to install the OracleAS Metadata Repository on an existing database, and you want to remove the OracleAS Metadata Repository, select the "Remove" option in OracleAS RepCA. You can also use OracleAS RepCA to remove the registration from Oracle Internet Directory.
- If you remove an infrastructure instance, all middle-tier instances that depend on that infrastructure will no longer work.

  If you want to keep the middle-tier instances, you can configure them to use services from another infrastructure. See the *Oracle Application Server Administrator's Guide* for details.

Items to Remove or Clean Up

To deinstall Oracle Application Server instances, you have to clean up the items listed in Table D–1. The procedures are described later in this appendix.

Table D–1 Items to Deinstall

Item to Clean Up	Tool to Use
Files from the Oracle home directory	Installer If the installer does not remove all the files, you can remove the remaining files using the `rm` command.
Entries for the deleted instance in the Inventory directory	Installer

Table D–1 (Cont.) Items to Deinstall

Item to Clean Up	Tool to Use
Instance name from Farm page	Installer
Entries for the deleted instance in the `/var/opt/oracle` directory	You have to remove the entries manually. See: ▪ Step 9 on page D-7 if you are deinstalling OracleAS Infrastructure.
Entries for the deleted instance in Oracle Internet Directory	Deconfig tool

The installer does not permit custom deinstallation of individual components.

D.3 Deinstalling OracleAS Cold Failover Cluster Installations

If you are deinstalling an OracleAS Cold Failover Cluster installation:

1. Stop the clusterware agents or packages that monitor and fail over the environment. See your clusterware documentation for details.
2. Then perform the steps described in this appendix.

If you do not take the resources offline, the installer will hang during the deinstallation because the clusterware agents are trying to fail over the resources.

D.4 Deinstalling OracleAS Single Sign-On Instances in OracleAS Cluster (Identity Management)

If you have multiple OracleAS Single Sign-On instances installed in a cluster against the same Oracle Internet Directory and you would like to deinstall some of the instances but keep others running, perform the following steps before running the Deconfig tool.

Note that if the OracleAS Single Sign-On instance that you wish to deinstall was the last instance to be installed against the Oracle Internet Directory, you should not perform this step. Instead, perform the steps in Section D.6, "Deinstalling OracleAS Infrastructure".

1. Open the file located at *ORACLE_HOME*`/deconfig/DeconfigWrapper.properties` for editing.
2. Search for the line that begins with "`SSO=`". For example, the line might look like the following:

   ```
   SSO=/OraHome_1/jdk/bin/java -jar /OraHome_1/sso/lib/ossoca.jar deinstall
   /OraHome_1 "%OID_USER%" %OID_PASSWORD%
   ```

3. Comment out the line by adding a pound (#) character at the beginning of the line. In the example above, the line would be changed to look like the following:

   ```
   # SSO=/OraHome_1/jdk/bin/java -jar /OraHome_1/sso/lib/ossoca.jar deinstall
   /OraHome_1 "%OID_USER%" %OID_PASSWORD%
   ```

After modifying the file, perform the steps in Section D.6, "Deinstalling OracleAS Infrastructure" to complete the deinstallation.

D.5 Deinstalling OracleAS Cluster (Identity Management)

To deinstall an OracleAS Cluster (Identity Management), perform the following steps.

1. Deinstall all instances that contain OracleAS Single Sign-On except for the last instance installed. Use the steps in Section D.4, "Deinstalling OracleAS Single Sign-On Instances in OracleAS Cluster (Identity Management)" to perform the deinstallation.
2. Deinstall the last OracleAS Single Sign-On instance using the steps in Section D.6, "Deinstalling OracleAS Infrastructure".
3. If you are using a Distributed OracleAS Cluster (Identity Management), deinstall the Oracle Internet Directory instances using the steps in Section D.6, "Deinstalling OracleAS Infrastructure".
4. After deinstalling all instances, remove the OracleAS Cluster (Identity Management) from its farm by running the `dcmctl removecluster` command:

```
prompt> $ORACLE_HOME/dcm/bin/dcmctl removecluster -cl cluster_name
```

D.6 Deinstalling OracleAS Infrastructure

This section describes how to deinstall OracleAS Infrastructure instances.

D.6.1 Deinstallation Order

The OracleAS Infrastructure instance could contain all the OracleAS Infrastructure components, or it could contain only a subset of the components, because you have a distributed OracleAS Infrastructure installation. Here are some common scenarios and their deinstallation order:

If you have an Oracle Identity Management + OracleAS Metadata Repository instance, you have only one instance to deinstall.

If you installed Oracle Identity Management and OracleAS Metadata Repository separately:

1. Deinstall the Oracle Identity Management instance.
2. Deinstall the OracleAS Metadata Repository.

If you have a distributed Oracle Identity Management:

1. Deinstall the instance(s) that are running OracleAS Single Sign-On, Oracle Delegated Administration Services, Oracle Directory Integration Platform, and/or OCA.
2. Deinstall the instance running Oracle Internet Directory.
3. Deinstall the OracleAS Metadata Repository.

D.6.2 Deinstallation Steps

1. Log in as the operating system user who installed the instance you want to deinstall.
2. If OCA is configured on the instance you want to deinstall, run the following commands:

```
prompt> $ORACLE_HOME/oca/bin/ocactl stop
prompt> $ORACLE_HOME/oca/bin/cmdeinst ocaAdminPassword oidAdminPassword
```

Replace *ocaAdminPassword* with the password of the OCA administrator.

Replace *oidAdminPassword* with the password of the Oracle Internet Directory user who installed OCA. The user must belong to the following groups:

- Trusted Application Admins
- iAS Admins
- Repository Owners group for the metadata repository used by OCA

The "`ocactl stop`" command stops OCA services. The `cmdeinst` command performs the following actions:

- removes OCA entries from Oracle Internet Directory
- removes data from tables in the `oca` schema
- removes OCA files created by the OCA Configuration Assistant during installation

3. If Oracle Directory Integration Platform is configured and running in the instance you want to deinstall, stop the Oracle Directory Integration Platform server.

   Ensure that Oracle Internet Directory is running.

   You can stop Oracle Directory Integration Platform by running the following command:

   ```
   prompt> cd $ORACLE_HOME/bin
   prompt> oidctl connect=db_connect_string server=odisrv instance=1 stop
   ```

   db_connect_string is the TNS alias as listed in the file `ORACLE_HOME/network/admin/tnsnames.ora`.

   For any additional Oracle Directory Integration Platform servers that you started, you must stop them too. See the instructions in the *Oracle Identity Management Integration Guide*.

4. If Oracle Internet Directory is configured as a replica, you need to delete this node from the directory replication group (DRG). See Chapter 25, "Oracle Internet Directory Replication Administration", in the *Oracle Internet Directory Administrator's Guide* for steps.

5. Run the Deconfig tool.

   ```
   prompt> cd $ORACLE_HOME/bin
   prompt> $ORACLE_HOME/perl/bin/perl deconfig.pl [parameters]
   ```

   See Section D.1, "Deconfig Tool" for parameter details. **Note:** If you are deinstalling an instance that includes the Oracle Internet Directory or OracleAS Single Sign-On components, you need to run the Deconfig tool as the Oracle Internet Directory superuser (`cn=orcladmin`). If the instance does not include Oracle Internet Directory or OracleAS Single Sign-On, then you need to run the tool as a user with the proper privileges, as shown in Table 5–4.

6. Start the installer.

   ```
   prompt> $ORACLE_HOME/oui/bin/runInstaller
   ```

7. Follow these steps in the installer.

   a. Welcome screen: Click **Deinstall Products**.

   b. Inventory screen: Select the instance you want to deinstall, and click **Remove**.

c. Confirmation screen: Verify the components selected for deinstallation. Click **Yes** to continue.

d. Deinstallation Progress screen: Monitor the progress of the deinstallation.

e. Exit the installer when the deinstallation is complete.

8. Delete any remaining files in the deleted instance's Oracle home directory.

```
prompt> rm -rf $ORACLE_HOME
```

9. Remove lines for the deinstalled infrastructure instance from the `/var/opt/oracle/oratab` file.

   Towards the end of the file, you should see lines that specify the Oracle home directory. If you are deinstalling an infrastructure instance that contains a metadata repository, there will be two lines in the file:

   - one line that begins with a `*`
   - one line that begins with the database SID

   You need to remove both lines.

   For example, if the infrastructure instance is installed in `/private1/infra`, and it includes a metadata repository whose SID is `orcl`, the lines would look like the following:

```
orcl:/private1/infra:N
*:/private1/infra:N
```

D.7 Harmless Errors in the Log File

If you get the following "unable to delete file" and "unable to find make file" errors in the `oraInstall`*`timestamp`*`.err` file after you deinstall J2EE and Web Cache or Portal and Wireless instances, these are harmless error messages.

```
Ignoring Exception during de-install
oracle.sysman.oii.oiil.OiilDeinstallException:
An error occurred during runtime. oracle.sysman.oii.oiil.OiilDeinstallException:
An error occurred during runtime.
...
Ignoring Exception during de-install
oracle.sysman.oii.oiil.OiilDeinstallException:
Unable to delete file
/home/j2ee/sysman/emd/targets.xml
oracle.sysman.oii.oiil.OiilDeinstallException: Unable to delete file
/home/j2ee/sysman/emd/targets.xml
at instantiateFileEx.deinstallAction(instantiateFileEx.java:935)
...
Ignoring Exception during de-installoracle.sysman.oii.oiil.OiilDeinstallException:
Unable to find make file:
/home/j2ee/network/lib/ins_net_client.mk
oracle.sysman.oii.oiil.OiilDeinstallException: Unable to find make file:
/home/j2ee/network/lib/ins_net_client.mk
at ssmakeux.deinstallAction(ssmakeux.java:246)
...
```

D.8 Cleaning Up Oracle Application Server Processes

If you forgot to shut down Oracle Application Server processes before starting the installation, you have to kill the processes because the files for these processes are deleted. To check for processes that are still running, run the `ps` command:

```
prompt> ps -ef
```

To kill a process, use the kill command:

```
prompt> kill -9 process_id
```

You can determine the *process_id* from the `ps` command.

If you need to shut down the `dcmctl` shell process, you can try exiting the shell by typing `exit`.

D.9 Reinstallation

The installer does not allow reinstallation of an Oracle Application Server instance in a directory that already contains an Oracle Application Server instance. To reinstall Oracle Application Server in the same directory, you have to deinstall and then install it.

D.10 Troubleshooting

See Section F.4, "Deinstallation Problems and Solutions" for help with common deinstallation problems.

E

Configuration Assistants

This appendix lists the configuration assistants and the location of their log files.

- Section E.1, "Troubleshooting Configuration Assistants"
- Section E.2, "Description of Oracle Application Server Configuration Assistants"

E.1 Troubleshooting Configuration Assistants

This section contains the following topics:

- Section E.1.1, "General Tips"
- Section E.1.2, "Configuration Assistant Result Codes"

E.1.1 General Tips

If a configuration assistant fails, try the following steps to correct the problem:

1. Review the installation log files listed in Section F.1, "Log Files".
2. Review the log files for the failed configuration assistant. Configuration assistant log files are listed in Section E.2, "Description of Oracle Application Server Configuration Assistants". Try to fix the issue that caused the error.
3. If the failed configuration assistant has any dependencies, then run the dependencies again. You must do this even if the dependency completed successfully.
4. Run the failed configuration assistant again by selecting the configuration assistant in the installer and clicking **Retry**.

   If the configuration assistant fails again after you click **Retry**, remove the `/tmp/EM_CONFIG_INSTALL.lk` file and re-run the configuration assistant again.

   If the configuration assistant fails again after you click **Retry**, remove the component entry from the `ORACLE_HOME/sysman/emd/targets.xml` file. For example, the following lines show the Oracle Containers for J2EE entry in the `targets.xml` file:

```
<Target TYPE="oc4j" NAME="instance2.domain.com_home" DISPLAY_NAME="home"
VERSION="1.3" DISABLED="TRUE">
   <Property NAME="HTTPMachine" VALUE="stacu02.us.oracle.com"/>
   <Property NAME="OracleHome" VALUE="/local_host/oracle/product/10.1.4IM/
OracleAS"/>
   <Property NAME="version" VALUE="9.0.4"/>
   <AssocTargetInstance ASSOC_TARGET="ias" TYPE="oracle_ias"
NAME="instance2.domain.com"/>
   <CompositeMembership>
```

```
      <MemberOf TYPE="oracle_ias" NAME="instance2.domain.com"/>
   </CompositeMembership>
</Target>
```

5. If an optional configuration assistant fails, and it does not have any dependencies, run the remaining configuration assistants. Uncheck the cancelled optional configuration assistant, highlight and check the next listed configuration assistant, and click **Retry**.
6. If configuration assistant failure occurs when running configuration assistant execution commands on the command line, then re-run the configuration assistant execution command again.

   You can use the generated script file named `configtoolcmds.pl` located in the `ORACLE_HOME/bin` directory to execute the failed configuration assistant again. The `configtoolcmds.pl` script is generated after you exit the installer. During silent or non-interactive installation, the `configtoolcmds.pl` script is generated immediately after configuration assistant failure.
7. If you see a "Fatal Error. Reinstall" message, find the cause of the problem by analyzing the log files. You cannot recover from a fatal error by correcting the problem and continuing. You must remove the current installation and reinstall Oracle Application Server. The following tasks describe the recovery procedure:
   a. Deinstall the failed installation using the procedure described in Appendix D, "Deinstallation and Reinstallation".
   b. Correct the cause of the fatal error.
   c. Reinstall Oracle Application Server.
   d. If the fatal error reoccurs, then you must remove all Oracle installations from your computer.

E.1.2 Configuration Assistant Result Codes

If a configuration assistant fails, the bottom half of the installation screen displays the error message, and the configuration assistant writes its result code (Table E–1) to the following log file:

oraInventory`/logs/installActions`*timestamp*`.log`

Table E–1 Result Codes for Configuration Assistants

Result Code	Description
0	Configuration assistant succeeded
1	Configuration assistant failed
-1	Configuration assistant cancelled

E.2 Description of Oracle Application Server Configuration Assistants

Table E–2 lists the Oracle Application Server configuration assistants in alphabetical order. Different installations use different configuration assistants depending on installation type and configuration options you selected.

Note that the paths below use "/" as the directory delimiter. You might need to change it for your system. For example, use "\" if you are on a Windows system.

Table E–2 Oracle Application Server Configuration Assistants

Configuration Assistant	Description	Log File Location
Application Server Control Configuration Assistant	Starts the Oracle Management Agent and the Application Server Control to deploy applications through the Oracle Enterprise Manager 10*g* Application Server Control.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
Database Configuration Assistant	Configures the OracleAS Metadata Repository for OracleAS Infrastructure.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
Database Migration Assistant	Migrates an older version of the infrastructure database to the current version of the infrastructure database. Before running this migration assistant, make sure the database is up and running.	`ORACLE_HOME/assistants/dbma/logs`
Database-managed OracleAS Cluster Assistant	Enables cluster configuration for selected databases.	`ORACLE_HOME/config/infratool_dcm_repository.log` `ORACLE_HOME/cfgtoollogs/infratool_dcm_repository.log`
DCM Repository Backup Assistant	Enables you to back up your DCM repository.	`ORACLE_HOME/dcm/logs`
Delegated Administration Service Configuration Assistant	Sets up the Oracle Delegated Administration Services URL in Oracle Internet Directory and adds the necessary access control privileges to the DAS entity. Before running this configuration assistant, make sure the Infrastructure Instance Configuration Assistant was run successfully.	`ORACLE_HOME/cfgtoollogs/dasca.log`
Directory Integration Platform Configuration Assistant	Registers and starts the directory integration server when configured with Oracle Internet Directory. Before running this configuration assistant, make sure Oracle Internet Directory is properly configured.	`ORACLE_HOME/cfgtoollogs/dipca.log`

HTTP Server Configuration Assistant	Configures Oracle HTTP Server, registers it with Oracle Enterprise Manager 10*g* Application Server Control, and adds an entry to the `ORACLE_HOME/sysman/emd/targets.xml` file.	`ORACLE_HOME/Apache/Apache/logs`
		`ORACLE_HOME/Apache/Apache/httpd.log`
		`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`

Infrastructure Database Registration Assistant	Registers the OracleAS Metadata Repository with Oracle Internet Directory.	`ORACLE_HOME/cfgtoollogs/infratool_ldaporacfg.log`

Table E–2 (Cont.) Oracle Application Server Configuration Assistants

Configuration Assistant	Description	Log File Location
Infrastructure Instance Configuration Assistant	Updates the `ORACLE_HOME/config/ias.properties` file, registers the instance with Oracle Internet Directory, and creates the `ldap.ora` file with Oracle Internet Directory credentials in the `ORACLE_HOME/network/admin` file. Before running this configuration assistant, check that: ▪ the LD_LIBRARY_PATH environment variable includes `ORACLE_HOME/lib32` and `ORACLE_HOME/network/lib` ▪ the LD_LIBRARY_PATH_64 environment variable includes `ORACLE_HOME/lib` ▪ the PATH environment variable includes `ORACLE_HOME/lib` and `ORACLE_HOME/network/lib`	`ORACLE_HOME/config/infratool_instance_jazn.log` `ORACLE_HOME/cfgtoollogs/infratool_instance_jazn.log`
Infrastructure mod_osso Configuration Assistant.	Registers mod_osso, plugs mod_osso into Oracle HTTP Server, and provides integration with OracleAS Single Sign-On to authenticate users. The registration enables Oracle HTTP Server installed with OracleAS Infrastructure to act as a partner application to OracleAS Single Sign-On. Applications that run under Oracle HTTP Server can register and protect their URL with mod_osso. When the URL is requested, mod_osso authenticates the user with OracleAS Single Sign-On to allow access to the URL.	`ORACLE_HOME/config/infratool_mod_osso.log` `ORACLE_HOME/cfgtoollogs/infratool_mod_osso.log`
Infrastructure Schema Configuration Assistant	Registers the Infrastructure schemas with Oracle Internet Directory. Before running this configuration assistant, check that: ▪ the LD_LIBRARY_PATH environment variable includes `ORACLE_HOME/lib32` and `ORACLE_HOME/network/lib` ▪ the LD_LIBRARY_PATH_64 environment variable includes `ORACLE_HOME/lib` ▪ the PATH environment variable includes `ORACLE_HOME/lib` and `ORACLE_HOME/network/lib` ▪ the Internet Directory Configuration Assistant and the Database Configuration Assistant were run successfully	`ORACLE_HOME/config/schemaload.log` `ORACLE_HOME/cfgtoollogs/schemaload.log`
Infrastructure Upgrade Instance Configuration Assistant	Removes ACL entries on the `SSO` schema. Before running this configuration assistant, check that: ▪ the LD_LIBRARY_PATH environment variable includes `ORACLE_HOME/lib32` and `ORACLE_HOME/network/lib` ▪ the LD_LIBRARY_PATH_64 environment variable includes `ORACLE_HOME/lib`	`ORACLE_HOME/config/infratool_infra_upgrade.log`

Table E–2 (Cont.) Oracle Application Server Configuration Assistants

Configuration Assistant	Description	Log File Location
Internet Directory Configuration Assistant	Starts up Oracle Internet Directory, loads the LDAP schemas, and sets up the Oracle Identity Management realm. Before running this configuration assistant, check that the database was created successfully, the listener is up and running, and the `tnsnames.ora` file is configured.	`ORACLE_HOME/cfgtoollogs/oidca.log`
Java Security Configuration Assistant	Changes the default password, and sets or reassigns new passwords for JAAS security.	`ORACLE_HOME/cfgtoollogs/jaznca.log`
OC4J Configuration Assistant	Integrates OC4J with Application Server Control. It performs the following steps: ■ Add entries to the `targets.xml` file. ■ Add entries to the `iasadmin.properties` file. This configuration assistant requires the `deploy.ini` file.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
OC4J Instance Configuration Assistant	Configures OC4J instances for deployed Oracle Application Server applications.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`

OPMN Configuration Assistant	Starts OPMN and OPMN-managed processes.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
		`ORACLE_HOME/cfgtoollogs/ipm.log`
		`ORACLE_HOME/cfgtoollogs/ons.log`

OPMN Configuration Assistant - start DAS instance	Starts Oracle Delegated Administration Services instance through OPMN.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
		`ORACLE_HOME/cfgtoollogs/ipm.log`
		`ORACLE_HOME/cfgtoollogs/ons.log`

OPMN Configuration Assistant - start OCA	Starts OCA through OPMN.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
		`ORACLE_HOME/cfgtoollogs/ipm.log`
		`ORACLE_HOME/cfgtoollogs/ons.log`

OPMN Configuration Assistant - start Oracle HTTP Server	Starts Oracle HTTP Server through OPMN.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log` `ORACLE_HOME/cfgtoollogs/HTTP_Server~1`
OCA Configuration Assistant	Configures a self-signed certificate authority, integrated with OracleAS Single Sign-On for authentication. Before running this configuration assistant, check that Oracle Internet Directory, OracleAS Metadata Repository, OracleAS Single Sign-On, and the Repository API are configured.	`ORACLE_HOME/cfgtoollogs/oca_install.log`

Table E–2 (Cont.) Oracle Application Server Configuration Assistants

Configuration Assistant	Description	Log File Location
OracleAS Instance Configuration Assistant	Adds an entry for the instance to the `ORACLE_HOME/config/target2add.xml` file.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
OracleAS Randomize Password Configuration Assistant	Changes the default password of all schemas.	None
Oracle Identity Management oneoff Patch Configuration Assistant	Automatically applies the OC4J and database patches using the OPatch tool.	`ORACLE_HOME/cfgtoollogs/imoneoffpatchca`*`timestamp`*`.log`

Oracle mod_osso Configuration Assistant	Registers mod_osso during installation, plugs mod_osso into Oracle HTTP Server, and provides integration with OracleAS Single Sign-On to authenticate users. The registration enables Oracle HTTP Server installed with the Oracle Application Server middle tier to act as a partner application to OracleAS Single Sign-On.
	
	Applications running under Oracle HTTP Server can register and protect their URL with mod_osso. When the URL is requested, mod_osso authenticates the user with OracleAS Single Sign-On to allow access to the URL.
		`ORACLE_HOME/config/j2ee_mod_osso.log`
		
		`ORACLE_HOME/cfgtoollogs/j2ee_mod_osso.log`

Oracle Net Configuration Assistant	Configures the database listener and the middle tiers to use LDAP naming by default.	`ORACLE_HOME/cfgtoollogs/installActions`*`timestamp`*`.log`

Register DCM Plug-Ins With Oracle Enterprise Manager 10*g* Configuration Assistant	Registers DCM plug-ins with Oracle Enterprise Manager 10*g*.	`ORACLE_HOME/cfgtoollogs/configtools`*`timestamp`*`.log`
		
		`ORACLE_HOME/dcm/logs/dcmctl_logs`

Replication Configuration Assistant	For ASR replica installations, it writes the new Oracle Internet Directory metadata to the master Oracle Internet Directory. For LDAP replica installations, it configures LDAP-based replication between the master Oracle Internet Directory and the new Oracle Internet Directory replica with default configuration. It then starts the Oracle Internet Directory replication server and helps configure Oracle Internet Directory replication. Before running this configuration assistant, check that the Oracle Internet Directory servers for the master and the new replica are up and running.	`ORACLE_HOME/ldap/log/remtool.log`

Table E–2 (Cont.) Oracle Application Server Configuration Assistants

Configuration Assistant	Description	Log File Location
Single Sign-On Configuration Assistant	Configures OracleAS Single Sign-On. Before running this configuration assistant, check that Oracle Internet Directory, OracleAS Metadata Repository, and the Repository API are configured.	`ORACLE_HOME/sso/log/ssoca.log` `ORACLE_HOME/sso/log/ssoreg.log`
Unlock Metadata Repository Schemas Configuration Assistant	Unlocks the schemas in the OracleAS Metadata Repository. This configuration assistant is run for Oracle Identity Management installations.	`ORACLE_HOME/config/infratool_unlock_schema.log`
Use Infrastructure Configuration Assistant	Updates the `ORACLE_HOME/config/ias.properties` file, registers the instance with Oracle Internet Directory, and creates the `ldap.ora` file with Oracle Internet Directory credentials in the `ORACLE_HOME/network/admin` directory. Before running this configuration assistant, check that the PATH environment variable includes the `ORACLE_HOME/lib` and ORACLE_HOME directories.	`ORACLE_HOME/config/j2ee_instance_jazn.log` `ORACLE_HOME/cfgtoollogs/j2ee_instance_jazn.log`

F

Troubleshooting

This appendix describes solutions to common problems that you might encounter when installing Oracle Application Server. It contains the following sections:

- Section F.1, "Log Files"
- Section F.2, "General Troubleshooting Tips"
- Section F.3, "Installation Problems and Solutions"
- Section F.4, "Deinstallation Problems and Solutions"
- Section F.5, "Need More Help?"

F.1 Log Files

The installer writes the following log files:

- *oraInventory_location*/logs/installActions*timestamp*.log
- *oraInventory_location*/logs/oraInstall*timestamp*.err
- *oraInventory_location*/logs/oraInstall*timestamp*.out

F.2 General Troubleshooting Tips

If you encounter an error during installation:

- Read the *Oracle Application Server Release Notes* for the latest updates. The release notes are available with the platform-specific documentation. The most current version of the release notes is available on Oracle Technology Network (http://www.oracle.com/technology/documentation).
- Verify that your computer meets the requirements specified in Chapter 2, "Requirements".
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- If a configuration assistant failed, check the log file for that configuration assistant. Section E.2, "Description of Oracle Application Server Configuration Assistants" lists the configuration assistants and the location of their log files. If you do not see log files from some configuration assistants in the ORACLE_HOME/cfgtoollogs directory, exit the installer. This causes the installer to copy the log files to that directory.
- If an error occurred while the installer is copying or linking files:
  1. Note the error and review the installation log files.

2. Remove the failed installation by following the steps in Appendix D, "Deinstallation and Reinstallation".
3. Correct the issue that caused the error.
4. Restart the installation.

F.3 Installation Problems and Solutions

This section describes common installation problems and solutions:

- Section F.3.1, "Location of Log Files"
- Section F.3.2, "Linking Failed, ORA Errors"
- Section F.3.3, "Prerequisite Checks Fail at the Start of Installation"
- Section F.3.4, "Message About Installing in a Non-Empty Directory"
- Section F.3.5, "Messages About SHMMAX and SEMMSL"
- Section F.3.6, "Installer Disappears After Running the Pre-Installation Checks"
- Section F.3.7, "Unable to Clean Up a Failed Installation"
- Section F.3.8, "Forgot the Password for the cn=orcladmin Account"
- Section F.3.9, "cn=orcladmin Account Becomes Locked"
- Section F.3.10, "User Interface Does Not Display in the Desired Language, or Does Not Display Properly"
- Section F.3.11, "Installer Does Not Display Correct Database Name for OracleAS Metadata Repository"
- Section F.3.12, "Configuration Assistant Failures - General"
- Section F.3.13, "OracleAS Randomize Password Configuration Assistant Failures"
- Section F.3.14, "Database Configuration Assistant (DBCA) Failures"
- Section F.3.15, "Harmless Error Message from Database Configuration Assistant (DBCA)"
- Section F.3.16, "OPMN Configuration Assistant - Start HTTP Server Failures"
- Section F.3.17, "OPMN Configuration Assistant - Start DAS Instance Failures"
- Section F.3.18, "OPMN Configuration Assistant - Start OCA Failures"
- Section F.3.19, "WARNING: DCM service may not be available at this time"
- Section F.3.20, "OracleAS Cluster (Identity Management)- Cluster Configuration Assistant Fails"
- Section F.3.21, "OracleAS Cluster (Identity Management) - Installation Fails on Second Oracle Internet Directory Node"
- Section F.3.22, "OracleAS Cluster (Identity Management) - Installation Fails on Second Oracle Delegated Administration Services and OracleAS Single Sign-On Node"

F.3.1 Location of Log Files

There are two sets of log files:

- The installer writes the following log files:

  - *oraInventory_location*/logs/installActions*timestamp*.log
  - *oraInventory_location*/logs/oraInstall*timestamp*.err
  - *oraInventory_location*/logs/oraInstall*timestamp*.out
  - *Oracle_Home*/install/make.log
- The configuration assistants write log files in the ORACLE_HOME/cfgtoollogs directory.

  Note that if you want to access the log files created by the configuration assistants, you need to exit the installer first. The log files are inaccessible if the installer is still in use.

F.3.2 Linking Failed, ORA Errors

Problem

Linking failed, and ORA errors were displayed during installation

Solution

Exit the installer and check the log files for any error message. In particular, check the ORACLE_HOME/install/make.log file.

Remove the failed installation. Before reinstalling Oracle Application Server, make sure that your computer meets all the requirements listed in Chapter 2, "Requirements".

Check especially the following requirements:

- Check that the kernel parameters are set to the proper values. Note that if you change the value of a kernel parameter, you must exit the installer and restart your computer for the new value to take effect.
- Check that you are installing Oracle Application Server in a valid directory. For example, you cannot install Oracle Application Server in a database Oracle home. See Table 2–11 for a complete list.

F.3.3 Prerequisite Checks Fail at the Start of Installation

Problem

The prerequisite checks that are run at the start of installation failed

Solution

If the prerequisite checks display warnings about missing operating system patches or patch bundles, the patch may actually be missing, or it may have been superseded. If your computer contains the patch that supersedes it, you can ignore the warning.

F.3.4 Message About Installing in a Non-Empty Directory

Problem

The installer displays a message that you are installing into a non-empty directory.

Solution

If you started an installation and went beyond the Specify File Locations screen, but did not complete the installation, the installer has already created the Oracle home

directory that you specified. If you later try to install again in the same directory, which contains some files created by the installer, the installer gives a warning that the directory is not empty.

Steps to take:

1. In the warning dialog, click **No** to return to the Specify File Locations screen.
2. In the Specify File Locations screen, click **Installed Products**. This displays the Inventory screen.

   If your Oracle home is listed in the Inventory screen, then you have to deinstall the Oracle home. See Appendix D, "Deinstallation and Reinstallation" for details.

   If your Oracle home is not listed in the Inventory screen, then you can just delete the files from the Oracle home and continue with the installation.

F.3.5 Messages About SHMMAX and SEMMSL

Problem

The installer displays messages about SHMMAX and SEMMSL when installing the OracleAS Metadata Repository

Solution

Check the following in the `/etc/system` file:

- The installer does not recognize commented-out entries in the `/etc/system` file for kernel parameters. It reads the commented-out entries and fails if the commented lines are below the required values. You have to remove such lines from the file.
- The installer ignores entries in the file that have syntax errors. Make sure that the lines for the required kernel parameters do not have any syntax errors.
- The installer does not read very large values (greater than 2 GB) correctly. It interprets the very large values as small values. Make sure the values for the required kernel parameters are under 2 GB.

F.3.6 Installer Disappears After Running the Pre-Installation Checks

Problem

The installer disappears after running pre-installation checks

Solution

The directory that is the mount point of the CD-ROM or DVD-ROM was mounted with incorrect permissions, and this caused the `pwd` command to not work correctly. When you run `pwd`, it returns "cannot determine current directory".

To fix:

1. Unmount the CD-ROM.
2. Change permissions of the mount directory to 755.
3. Remount the CD-ROM.

The installer should now run correctly.

F.3.7 Unable to Clean Up a Failed Installation

If your installation was not successful, you have to deinstall it first before you can install Oracle Application Server again. Refer to Appendix D, "Deinstallation and Reinstallation" for instructions.

F.3.8 Forgot the Password for the cn=orcladmin Account

Problem

You forgot the password for the cn=orcladmin account.

Solution

You can reset the password in the database. The DSE root attribute name is `orclsupassword`.

Note that after a certain number of failed attempts to connect, the cn=orcladmin account becomes locked. In this case, you have to unlock the account. See the next section, Section F.3.9, "cn=orcladmin Account Becomes Locked", for instructions on how to unlock the account.

F.3.9 cn=orcladmin Account Becomes Locked

Problem

The cn=orcladmin account becomes locked after ten failed attempts to connect. This is controlled by the password policy. Ten failed attempts is the default value.

Solution

If you know the cn=orcladmin password, you can unlock the account by running the following command:

```
prompt> ORACLE_HOME/bin/oidpasswd connect=dbsid unlock_su_acct=true
```

where *dbsid* is the SID for the database. For example:

```
prompt> ORACLE_HOME/bin/oidpasswd connect=orcl unlock_su_acct=true
OID DB user password: enter_ODS_password
OID superuser account unlocked successfully.
```

The command prompts for the password of the ODS schema. By default, the ODS password is the same as for the cn=orcladmin and ias_admin accounts, which you entered during installation.

To change the password policy, see the *Oracle Internet Directory Administrator's Guide*.

F.3.10 User Interface Does Not Display in the Desired Language, or Does Not Display Properly

Problem

Messages do not appear in the desired language, or messages are not displayed correctly

Solution

Currently Oracle Application Server does not support adding or removing languages after installation.

If you are serving non-English content, be sure you add all the languages that you need during installation. To add languages during installation, click the **Product Languages** button in the "Select a Product to Install" screen. To see which languages are installed by default, see Section 3.4, "Installing Additional Languages".

If you are serving non-English content and forgot to click the Product Languages in the installation, the user interface might not display properly because the required fonts were not installed. You can fix this by installing the fonts from the "OracleAS Metadata Repository Upgrade Assistant and Utilities" CD-ROM or from the Oracle Application Server DVD-ROM.

1. Insert and mount the "OracleAS Metadata Repository Upgrade Assistant and Utilities" CD-ROM or the Oracle Application Server DVD-ROM.
2. CD-ROM: Copy the contents of the `utilities/fonts` directory on the CD-ROM to the `ORACLE_HOME/jdk/jre/lib/fonts` directory.

   DVD-ROM: Copy the contents of the `repca_utilities/utilities/fonts` directory on the DVD-ROM to the `ORACLE_HOME/jdk/jre/lib/fonts` directory.

F.3.11 Installer Does Not Display Correct Database Name for OracleAS Metadata Repository

Problem

During middle-tier installation, in the Select OracleAS Metadata Repository screen, which is the screen where you select the OracleAS Metadata Repository that you want to use for the middle tier, the installer does not display correctly the names of the available OracleAS Metadata Repository databases.

Solution

Check the log file *`oraInventory`*`/logs/installActions`*`timestamp`*`.log`. If you see these lines:

```
*** Select OracleAS Metadata Repository Page***
Error:*** Alert: Error validating repository on multiple hosts and ports.
A database hostname or port is missing.
```

it means that your OracleAS Metadata Repository database name contains `PORT` or `HOST` in uppercase characters. To fix the problem, change the name of the database so that it does not contain `PORT` or `HOST` in uppercase characters.

F.3.12 Configuration Assistant Failures - General

This section describes general tips for troubleshooting configuration assistant failures. See the next sections for specific configuration assistant failures. See also Appendix E, "Configuration Assistants".

Problem

Configuration assistant failed

Solution

Configuration assistants fail from a variety of causes. Some things you can check are:

- Check that the listener, database, and Oracle Internet Directory associated with the OracleAS Infrastructure are up and running. If not, start them up and click the **Retry** button to rerun the configuration assistant that failed.
- Check the log files for the failed configuration assistant to determine the problem. The log files are located in the `ORACLE_HOME/cfgtoollogs` directory.

  Fix the problem indicated in the log file, and click **Retry** to rerun the failed configuration assistant.

F.3.13 OracleAS Randomize Password Configuration Assistant Failures

Before rerunning OracleAS Randomize Password Configuration Assistant, you need to perform these steps:

1. Start Oracle Directory Manager.
2. Enter the Oracle Internet Directory hostname, port, user name, and password.
3. Expand **Entry Management** > **cn=OracleContext** > **cn=Products** > **cn=IAS** > **cn=IAS Infrastructure Databases**.
4. Select **orclreferencename=***your_globaldb_name*.
5. For each schema under the *your_globaldb_name* tree, there is an `orclreferencename` entry. For the `orclreferencename` entry:
   - Change the value of the `orclpassword` attribute to the schema name. For example, if `wireless` is the schema name, change the `orclpassword` attribute value to `wireless`.
   - Change `orclflexattribute1` to **false**.

   Click **Apply**.

   Perform these steps for all the schemas except `ODS` and `OEM_REPOSITORY`.
6. Using SQL*Plus, log in to the database where the OracleAS Randomize Password Configuration Assistant failure is occurring, and run the following script.

   ```
   prompt> sqlplus "sys/password as sysdba"
   SQL> @ORACLE_HOME/assistants/dbca/admin/unlock.sql
   ```

   password specifies the password for the SYS user.
7. Rerun the OracleAS Randomize Password Configuration Assistant.

F.3.14 Database Configuration Assistant (DBCA) Failures

Problem

DBCA fails with the following error:

```
Open wallet failedoracle.net.config.ServiceAliasException
at oracle.net.config.ServiceAlias.<init>(Compiled Code)
at oracle.net.config.Service.<init>(Compiled Code)
at oracle.net.config.DatabaseService.<init>(Compiled Code)
at oracle.sysman.assistants.util.NetworkUtils.registerDBWithDirSrvc(NetworkUtils.j
ava:1137)
at oracle.sysman.assistants.dbca.backend.DirServiceStep.executePreReqImpl(Compiled
Code)
at oracle.sysman.assistants.dbca.backend.PrerequisiteStep.executeImpl(Prerequisite
Step.java:149)
at oracle.sysman.assistants.dbca.backend.Step.execute(Compiled Code)
```

```
at oracle.sysman.assistants.dbca.backend.PostDBCreationStep.executeImpl(Compiled
Code)
at oracle.sysman.assistants.dbca.backend.Step.execute(Compiled Code)
at oracle.sysman.assistants.dbca.backend.Host$ModeRunner.run(Compiled Code)
at java.lang.Thread.run(Thread.java:466)
ERROR :oracle.sysman.assistants.util.NetAPIException
```

Solution

This error occurs if the TNS_ADMIN environment variable is set. The TNS_ADMIN environment variable should not be set (see Section 2.9.5, "TNS_ADMIN"). If it is set, unset it and rerun DBCA by clicking the **Retry** button in the Configuration Assistants screen.

F.3.15 Harmless Error Message from Database Configuration Assistant (DBCA)

If you see the following "error copying OC4J config files" message in your log file, the message is harmless and can be ignored.

```
Nov 25, 2004 9:07:30 PM oracle.sysman.emcp.EMConfig updateReposVars
INFO: Updating file /ASInstalls/ASInfra/sysman/emdrep/config/repository.variables
...
Nov 25, 2004 9:07:35 PM oracle.sysman.emcp.EMConfig addPortEntries
INFO: Updating file /ASInstalls/ASInfra/install/portlist.ini ...
Nov 25, 2004 9:07:35 PM oracle.sysman.emcp.EMConfig updateEmdProps
INFO: Updating file /ASInstalls/ASInfra/sysman/config/emd.properties ...
Nov 25, 2004 9:07:35 PM oracle.sysman.emcp.EMConfig updateConfigFiles
INFO: targets.xml file is updated successfully
Nov 25, 2004 9:07:35 PM oracle.sysman.emcp.EMConfig updateEmomsProps
INFO: Updating file
/ASInstalls/ASInfra/sysman/config/emoms.properties ...
Nov 25, 2004 9:07:35 PM oracle.sysman.emcp.EMConfig updateConfigFiles
INFO: emoms.properties file is updated successfully
Nov 25, 2004 9:07:40 PM oracle.sysman.emcp.EMConfig copyOC4JDir
WARNING: Error copying OC4J config files from
/ASInstalls/ASInfra/oc4j/j2ee/OC4J_DBConsole to
/ASInstalls/ASInfra/oc4j/j2ee/OC4J_DBConsole_hostname.domain_portaldb
Nov 25, 2004 9:07:40 PM oracle.sysman.emcp.EMConfig startOMS
INFO: Starting the DBConsole ...
Nov 25, 2004 9:08:26 PM oracle.sysman.emcp.EMConfig perform
INFO: DBConsole is started successfully
```

F.3.16 OPMN Configuration Assistant - Start HTTP Server Failures

Problem

The OPMN Configuration Assistant - Start HTTP Server fails when you re-run it.

Solution

The problem is that Oracle HTTP Server is already running. Before re-running the configuration assistant, stop Oracle HTTP Server with the following command:

```
prompt> $ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=HTTP_Server
```

Then re-run the OPMN Configuration Assistant - Start HTTP Server.

F.3.17 OPMN Configuration Assistant - Start DAS Instance Failures

Problem

The OPMN Configuration Assistant - Start DAS Instance fails when you re-run it.

Solution

The problem is that the Oracle Delegated Administration Services instance is already running. Before re-running the configuration assistant, stop the Oracle Delegated Administration Services instance with the following command:

```
prompt> $ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J_Security
```

Then re-run the OPMN Configuration Assistant - Start DAS Instance.

F.3.18 OPMN Configuration Assistant - Start OCA Failures

Problem

The OPMN Configuration Assistant - Start OCA fails when you re-run it.

Solution

The problem is that the OCA instance is already running. Before re-running the configuration assistant, stop the OCA instance with the following command:

```
prompt> $ORACLE_HOME/opmn/bin/opmnctl stopproc ias-component=OC4J instancename=oca
```

Then re-run the OPMN Configuration Assistant - Start OCA.

F.3.19 WARNING: DCM service may not be available at this time

Problem

When installing the first node of an OracleAS Cluster (Identity Management), the Java Security Configuration Assistant may return the following message:

```
WARNING: DCM service may not be available at this time to synchronize $ORACLE_
HOME/j2ee/home/config/jazn-data.xml file.
```

This is due to a failure in updating the DCM repository and could happen if your load balancer virtual server is not configured to return immediately to the calling client when the backend services to which it forwards traffic are unavailable.

Solution

Perform the following steps to correct the problem:

1. Run the following command after installation completes:

   ```
   prompt> $ORACLE_HOME/dcm/bin/dcmctl updateConfig -ct jazn
   ```

2. Verify that the `dcmctl updateConfig` command did not return any errors.
3. Use the following command to verify that the password is correct:

   ```
   prompt> $ORACLE_HOME/jdk/bin/java
                   -Doracle.security.jazn.config=./jazn/install/jazn.xml
                   -jar jazn.jar -checkpasswd jazn.com admin -pw admin_password
   ```

F.3.20 OracleAS Cluster (Identity Management)- Cluster Configuration Assistant Fails

Problem

During the installation of OracleAS Cluster (Identity Management), the Cluster Configuration Assistant failed because the cluster name was typed incorrectly or the cluster was not available.

Solution

To cluster the instance, you must use the "`dcmctl joincluster`" command instead of Application Server Control. You cannot use Application Server Control in this case because Application Server Control cannot cluster instances that contain disabled components. In this case, the "home" OC4J instance is disabled.

F.3.21 OracleAS Cluster (Identity Management) - Installation Fails on Second Oracle Internet Directory Node

Problem

After successfully installing Oracle Internet Directory on the first node of an OracleAS Cluster (Identity Management), the installation of Oracle Internet Directory fails on the second node.

Solution

Perform the following steps to correct the problem:

1. Run the following command to connect to the database:

   ```
   prompt> sqlplus ods/password
   ```

2. Remove the registry information for node 2 from the `IMCFREGISTRY` table:

   ```
   SQL> delete from IMCFREGISTRY where IASINSTANCE='node2_instance_name';
   ```

3. Remove the PROCESS information from ODS_PROCESS:

   ```
   SQL> delete from ods_process where hostname='node2_hostname';
   ```

4. Remove OIDMON information from ODS_SHM:

   ```
   SQL> delete from ods_shm where NODENAME='node2_hostname';
   ```

5. Commit the changes to the database and exit:

   ```
   SQL> commit;
   SQL> exit
   ```

F.3.22 OracleAS Cluster (Identity Management) - Installation Fails on Second Oracle Delegated Administration Services and OracleAS Single Sign-On Node

Problem

After successfully installing Oracle Delegated Administration Services and OracleAS Single Sign-On on the first node of an OracleAS Cluster (Identity Management), the installation of Oracle Delegated Administration Services and OracleAS Single Sign-On fails on the second node.

Solution

Perform the following steps to correct the problem:

1. Start Oracle Directory Manager.

```
prompt> cd ORACLE_HOME/bin
prompt> ./oidadmin
```

2. Navigate to the entry:

```
orclApplicationCommonName=ORASSO_SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
```

3. Remove the instance name of the failed middle tier from the values of the attribute `labeledURI`.
4. If there are no more instance names listed in the values of the attribute `labeledURI`, then remove the entry:

```
orclApplicationCommonName=ORASSO_SSOSERVER,cn=SSO,cn=Products,cn=OracleContext
```

F.4 Deinstallation Problems and Solutions

This section describes common problems related to deinstallation:

- Section F.4.1, "Obsolete Partner URLs Still Remain on the OracleAS Single Sign-On Administration Screen"
- Section F.4.2, "Unable to Reuse Instance Name of a Deleted Instance"
- Section F.4.3, "Unable to Reuse Database Name"
- Section F.4.4, "Deconfiguration Failed on Distributed OracleAS Cluster (Identity Management)"

F.4.1 Obsolete Partner URLs Still Remain on the OracleAS Single Sign-On Administration Screen

Problem

After deinstallation, some partner application entries that are obsolete remain on the OracleAS Single Sign-On Administration screen.

Solution

Run the command to de-register the entries for the obsolete partner applications. The command is similar to the command for registration, except that the `-update_mode` parameter is set to `DELETE`.

Make sure your LD_LIBRARY_PATH environment variable contains `$ORACLE_HOME/lib32`, and that your LD_LIBRARY_PATH_64 environment variable contains `$ORACLE_HOME/lib`. Then run the command (all on one line):

```
prompt> $ORACLE_HOME/jdk/bin/java
 -jar $ORACLE_HOME/sso/lib/ossoreg.jar
 -oracle_home_path $ORACLE_HOME
 -site_name hostname.domain
 -config_mod_osso TRUE
 -mod_osso_url http://hostname.domain:port
 -u userid
 -update_mode DELETE
```

For `-site_name` *hostname.domain*, specify the computer where the middle tier is installed. Include also the domain name.

For `-mod_osso_url http://`*hostname.domain:port*, specify the computer where the middle tier is installed, and the port number on which Oracle HTTP Server is listening.

For `-u` *userid*, specify the operating system user who can start up the middle-tier processes.

For a detailed explanation of the parameters, see chapter 4 of the *Oracle Application Server Single Sign-On Administrator's Guide*.

F.4.2 Unable to Reuse Instance Name of a Deleted Instance

Problem

You get an error when you try to name a new Oracle Application Server instance using the name of an instance that you deleted.

Solution

The name of the deleted instance must be removed from Oracle Internet Directory before you can reuse it. To remove entries for a deleted instance from Oracle Internet Directory, perform these steps:

1. Start up Oracle Directory Manager. Oracle home refers to the home where you installed Oracle Internet Directory.

   ```
   prompt> $ORACLE_HOME/bin/oidadmin
   ```

2. In the Connect screen, enter the Oracle Internet Directory connect information. Log in as the Oracle Internet Directory superuser (`cn=orcladmin`).
3. Expand **Entry Management** > **cn=OracleContext** > **cn=Products** > **cn=IAS** > **cn=IAS Instances**.
4. Under **cn=IAS Instances**, select the instance that you want to delete.
5. From the menu, select **Edit > Delete**.
6. Expand **Entry Management** > **cn=OracleContext** > **cn=Groups**.
7. Select **cn=IASAdmins**.
8. In the Properties tab, remove the instance from the `uniquemember` field by editing the field. Do **not** select **Edit > Delete** from the menu.
9. Click **Apply**.

F.4.3 Unable to Reuse Database Name

Problem

You get an error when you try to use the same global database name or SID as the one that you deleted.

Solution

You might see this problem if you deinstall OracleAS Metadata Repository but not Oracle Internet Directory, and you want to reuse the Oracle Internet Directory and the same database name or SID when you install another OracleAS Metadata Repository. The Oracle Internet Directory still contains the name of the deleted OracleAS Metadata Repository. You need to remove this name before you can reuse it.

Note: Do **not** perform this procedure if you are deinstalling a middle tier.

1. Start up Oracle Directory Manager. Oracle home refers to the home where you installed Oracle Internet Directory.

   ```
   prompt> $ORACLE_HOME/bin/oidadmin
   ```

2. In the Connect screen, enter the Oracle Internet Directory connect information. Log in as the Oracle Internet Directory superuser (`cn=orcladmin`).

3. Expand **Entry Management** > **cn=OracleContext** > **cn=Products** > **cn=Portal** > **cn=UltraSearch** > **cn=Database Instances** > **orclApplicationCommonName=***infrastructure_database_name*.

4. Delete all the child entries under **orclApplicationCommonName=***infrastructure_database_name*, starting with the inner-most child entry. To delete an entry, right-click each child entry and select **Delete** from the pop-up menu. Click **Yes** in the Confirmation dialog. When deleting child entries, you may get some error messages. You can ignore these error messages.

5. After you have deleted all the entries under **orclApplicationCommonName=***infrastructure_database_name*, right-click this entry and delete it.

6. Expand **Entry Management**.

   Expand the Default Subscriber entry. You need to expand each term separately. For example: if your default subscriber is "dc=us,dc=oracle,dc=com", you need to expand "dc=com", then expand "dc=oracle", then expand "dc=us".

   Then expand **cn=OracleContext** > **cn=Products** > **cn=Portal** > **cn=UltraSearch** > **cn=Database Instances** > **cn=***infrastructure_database_name*.

7. Delete all the child entries under **cn=***infrastructure_database_name*, starting with the inner-most child entry. To delete an entry, right-click each child entry and select **Delete** from the pop-up menu. Click **Yes** in the Confirmation dialog. When deleting child entries, you may get some error messages. You can ignore these error messages.

8. After you have deleted all the entries under **cn=***infrastructure_database_name*, right-click this entry and delete it.

9. Click **Apply**.

F.4.4 Deconfiguration Failed on Distributed OracleAS Cluster (Identity Management)

Problem

When running deconfiguring the first OracleAS Single Sign-On node on a Distributed OracleAS Cluster (Identity Management) configured as in Section 9.4.2, "Case 2: Client ---[HTTPS]---> Load Balancer ---[HTTPS]---> Oracle HTTP Server", the Deconfig tool fails. The log file located at `$ORACLE_HOME/sso/log/ssoreg.log` has the following error:

```
Unable to open file $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf.
Please check the file path.
SSO registration tool failed.  Please check the error in this log file, correct
the problem and re-run the tool.
```

Solution

The Deconfig tool failed because it was unable to find the `$ORACLE_HOME/Apache/Apache/conf/osso/osso-https.conf` file. Perform the following steps to correct this problem:

1. Create a link from `osso-https.conf` to `osso.conf`:

```
cd $ORACLE_HOME/Apache/Apache/conf/osso
ln osso-https.conf osso.conf
```

2. Run the Deconfig tool again.

F.5 Need More Help?

If this appendix does not solve the problem you encountered, try these other sources:

- *Oracle Application Server Release Notes*, available on the Oracle Technology Network (http://www.oracle.com/technology/documentation)
- Oracle*MetaLink* (http://metalink.oracle.com)

If you do not find a solution for your problem, open a service request.

Index

Numerics

256 color requirement, 2-6
64-bit support requirement, 2-3

A

adding users to groups
  using Deployment Delegation Console, 5-14
  using Oracle Directory Manager, 5-11
additional languages, 3-3
ASM recommendations (for OracleAS Cold Failover Cluster), 8-5
Associated Middle Tiers group, 5-3

B

backup and recovery
  in OracleAS Disaster Recovery environment, 10-2
  post-installation, 11-2
browser requirement, 2-6

C

CD-ROM
  copying to hard drive, 2-26
  format of, 3-8
  mount point, 3-8
  mounting manually, 3-8
/cdrom mount point, 3-8
character sets
  NE8ISO8859P10 and CEL8ISO8859P14, 4-11
CLASSPATH environment variable, 2-23
clocks, synchronizing, for OracleAS Cluster (Identity Management), 9-3
cluster topologies
  installing distributed identity management with integrated HTTP server, 1-5
  installing distributed identity management with standalone HTTP server, 1-7
_CLUSTER_NETWORK_NAME_ environment variable, 10-5
clusterware agents (for OracleAS Cold Failover Cluster), 8-5
cn=orcladmin superuser, 5-1
  and Delegated Administration Services, 5-2
  initial password, 5-1
  unlocking, F-5
Component Owners group, 5-3
components
  configuring vs. installing, 3-5
  default port numbers, C-1
  how to assign custom port numbers, 2-14
  how to install on separate computers, 4-4
  OracleAS Infrastructure components, 4-2
  ports used by components, 4-11
configuration assistant errors
  Database configuration assistant, F-7
  database configuration assistant, F-8
  OPMN configuration assistant - Start DAS Instance, F-9
  OPMN configuration assistant - Start HTTP Server, F-8
  OPMN configuration assistant - Start OracleAS Certificate Authority, F-9
  OracleAS Randomize Password configuration assistant, F-7
configuration assistants, E-1
  dependencies, E-1
  descriptions of, E-2
  error codes, E-2
  fatal errors, E-2
  troubleshooting, E-1
configuring components, 3-5
copying CD-ROM/DVD to hard drive, 2-26
CPU requirements, 2-3
custom ports
  see static ports

D

database administrator groups, 2-20
Database configuration assistant
  errors, F-7
  harmless error messages, F-8
database name, reusing, F-12
dba group, 2-20
deconfig tool, D-1
  log files, D-3
default port numbers, 2-13, C-1
deinstallation, D-1
  deconfig tool, D-1
  of Oracle Single Sign-On instances in OracleAS

Cluster (Identity Management), D-4
of OracleAS Cluster (Identity Management), D-5
of OracleAS Cold Failover Cluster, D-4
OracleAS Infrastructure, D-5
overview, D-3
silent mode, B-12
troubleshooting, F-11
Deployment Delegation Console
adding users to groups, 5-14
df command, 2-4
directories, integration with third-party, 4-11
disk space requirements, 2-4
DISPLAY environment variable, 2-23
distributed OracleAS Cluster (Identity Management), 9-15
deconfig failed, F-13
installing Oracle Internet Directory on first node, 9-17
installing Oracle Internet Directory on subsequent nodes, 9-19
installing OracleAS Single Sign-On and Oracle Delegated Administration Services, 9-21
distributed OracleAS Cold Failover Cluster (Identity Management), 8-19
installing, 8-22
overview of installation steps, 8-21
distributed OracleAS Cold Failover Cluster (Infrastructure), 8-11
installing, 8-13
overview of installation steps, 8-13
distributing components, 4-4
DNS server for name resolution (OracleAS Disaster Recovery), 10-4
DVD
copying to hard drive, 2-26
format of, 3-8
mount point, 3-8
mounting manually, 3-8

E

environment variables, 2-22
_CLUSTER_NETWORK_NAME_, 10-5
CLASSPATH, 2-23
DISPLAY, 2-23
LD_LIBRARY_PATH, 2-23
NLS_LANG, 11-2
ORACLE_HOME, 2-23
ORACLE_SID, 2-23
PATH, 2-23
set in .profile file, 2-22
su command and, 2-22
TEMP, 2-24
TNS_ADMIN, 2-23
error codes from configuration assistants, E-2
/etc/group file, 7-5
/etc/hosts file, 2-24
/etc/resolve.conf file, 10-5
/etc/services file, 2-13
blocking ports 389 and 636, 2-13
/etc/system file, 2-9
EXTPROC key, 2-17

F

failover (OracleAS Cold Failover Cluster), 8-4
fatal errors, E-2
first-time installation of any Oracle product, 3-2
font packages for Java, 2-30
font problems, F-5

G

grid control plug-in
installing, A-1
starting the installer, A-1
grid control plug-in agent
installing, A-3
groups (operating system)
see operating system groups
groups (Oracle Internet Directory), 5-2
adding users to, 5-10
groups command, 2-22

H

high availability environments
/etc/group file, 7-5
installation order, 7-4
inventory directory, 7-6
oracle user, 7-5
OracleAS Cluster (Identity Management), 9-1
OracleAS Cold Failover Cluster, 8-1
OracleAS Disaster Recovery, 10-1
overview, 7-1
requirements, 7-5
summary of differences, 7-4
hostname requirement, 2-3
hosts file for name resolution (OracleAS Disaster Recovery), 10-6

I

IAS Admins group, 5-2
ias_admin user, 3-4
password for, 3-4
Identity Management Access
groups required for installation, 5-5
Identity Management components, 4-2
installing, 4-16
installing Oracle Delegated Administration Services, 4-6
installing Oracle Internet Directory only, 4-20
installing OracleAS Certificate Authority and Metadata Repository, 4-21
installing OracleAS Single Sign-On, 4-6
installing separately, 4-5
installing without Internet Directory, 4-18
Identity Management default realm location, 2-24
infrastructure
see OracleAS Infrastructure

installActions.log, B-11
installation documentation locations, 1-2
installation order
  for OracleAS Infrastructure, 4-3
installation types
  OracleAS Infrastructure, 4-1, 4-2
installer
  see Oracle Universal Installer
installing additional languages, 3-3
installing components, 3-5
installing from hard drive, 2-26
installing in non-empty directory, F-3
installing the grid control plug-in, A-1
installing the grid control plug-in agent, A-3
instance names, 3-3
  how they are used, 3-4
  reusing, F-12
  valid characters, 3-4
inventory directory, 3-2, 3-6
  group for, 2-20
  location of, 2-20
IP
  installing on a computer with multiple IP addresses, 2-26
  requirements, 2-2
IPC protocol, 2-17
isainfo command, 2-3

J

J2SE patch cluster, 2-7
Java font packages, 2-30

K

kernel parameters, 2-9
  /etc/system file, 2-9

L

languages, installing additional, 3-3
LD_LIBRARY_PATH environment variable, 2-23
linking failed, F-3
load balancer
  configuring for OracleAS Cluster (Identity Management), 9-3
log files, F-1
  from non-interactive installations, B-11
  location of, F-2

M

memory requirements, 2-4
  reducing, 2-7
middle tiers
  groups required for installation, 5-7
  installing against OracleAS Cluster (Identity Management), 9-26
  installing against OracleAS Cold Failover Cluster, 8-32
  installing in OracleAS Disaster Recovery, 10-9
  installing on OracleAS Cold Failover Cluster, 8-34
Mid-Tier Administrators group, 5-3
mod_osso configuration, 11-3
monitor requirement, 2-6
mount point for CD-ROM, 3-8
mount point for DVD, 3-8
mounting CD-ROM/DVD manually, 3-8
multihomed computers, installing on, 2-26

N

name resolution (OracleAS Disaster Recovery), 10-4
  using DNS servers, 10-4
  using hosts file, 10-6
names of instances
  see instance names
namespace in Oracle Internet Directory, 4-11
Network Appliance filers, 2-29
network requirements, 2-2
network topics, 2-25
  installing from hard drive, 2-26
  installing from remote CD-ROM/DVD drive, 2-27
  installing on multihomed computers, 2-26
  NFS storage, 2-29
  remote installations, 2-28
NFS installations
  configuring Oracle HTTP Server, 11-2
NFS storage, 2-29
NIS and NIS+, 2-30
NLS_LANG environment variable, 11-2
non-interactive installations, B-1, B-2
  deinstalling, B-12
  log files, B-11
  post-installation steps, B-11
  pre-installation steps, B-2
  security tips, B-11

O

oinstall group, 2-20, 3-3
operating system groups, 2-19
  creating, 2-19
  dba group, 2-20
  for database administration, 2-20
  for inventory directory, 2-20
  groups command, 2-22
  oinstall group, 2-20
  OSDBA group, 2-20
  OSOPER group, 2-20
operating system packages, 2-9
  pkginfo command, 2-9
operating system patches, 2-7
  requirements failed, 2-8
  showrev command, 2-8
  Solaris 8, 2-8
  Solaris 9, 2-8
operating system users, 2-21
  creating, 2-21

groups command, 2-22
oracle user, 2-21
operating system version, 2-2
OPMN configuration assistant - Start DAS Instance, re-running, F-9
OPMN configuration assistant - Start HTTP Server, re-running, F-8
OPMN configuration assistant - Start OracleAS Certificate Authority, re-running, F-9
Oracle Data Guard (for OracleAS Disaster Recovery), 10-2, 10-6
Oracle database
port 1521 issue, 2-16
Oracle Delegated Administration Services, 4-6
and mod_osso, 11-3
cn=orcladmin superuser, 5-2
dependency on OracleAS Single Sign-On, 4-6
deploying on a separate host, 4-12
groups required for installation, 5-4
Oracle Directory Integration Platform, 4-6
groups required for installation, 5-4
Oracle Directory Manager
adding users to groups, 5-11
Oracle E-Delivery, 3-7
Oracle Enterprise Manager Application Server Control
URL, 11-1
Oracle home directory, 3-1
Oracle HTTP Server
in NFS installations, 11-2
Oracle Internet Directory, 5-1
adding users to groups, 5-10
cn=orcladmin superuser, 5-1
connecting using SSL, 3-7
contents of new, 5-16
creating users, 5-10
default users, 5-1
groups, 5-2, 5-4
groups required for installation, 5-4
groups required to install components, 5-4
groups required to install middle tiers, 5-7
installing, 4-20
namespace, 4-11
OracleAS Metadata Repository registration, 4-7
orcladmin user, 5-2
realms, 5-16
supported versions, 4-7
using existing, 4-7
Oracle Internet Directory groups
Associated Middle Tiers, 5-3
Component Owners, 5-3
IAS Admins, 5-2
Mid-Tier Administrators, 5-3
Repository Owners, 5-3
Trusted Application Admins, 5-2
User Management Application Admins, 5-2
Oracle Internet Directory passwords (for OracleAS Cluster (Identity Management)), 9-4
Oracle Internet Directory ports
reserved in /etc/services file, 2-13
Oracle Internet Directory Replication
fan-out replication, 6-2
installing master Oracle Internet Directory, 6-4
installing replica, 6-5
multimaster replication, 6-2
overview, 6-1
requirements, 6-3
Oracle Internet Directory users
adding to groups, 5-10
cn=orcladmin, 5-1
creating, 5-10
orcladmin, 5-1
Oracle Universal Installer
database screens, 4-26
disappears after pre-installation checks, F-4
first few screens (infrastructure), 4-23
last few screens (infrastructure), 4-25
log files, F-1
OracleAS Certificate Authority screens, 4-27
prerequisite checks, 2-30
starting, 3-9
where it writes files, 3-5
oracle user, 2-21, 7-5
ORACLE_HOME environment variable, 2-23
ORACLE_SID environment variable, 2-23
OracleAS Certificate Authority
adding after installation, 4-12
groups required for installation, 5-4, 5-5
in silent and non-interactive installations, B-3
installing, 4-21
OracleAS Cluster
groups required for installation, 5-5
OracleAS Cluster (Identity Management), 9-1
cluster configuration assistant failure, F-10
configuring LDAP virtual server, 9-3
configuring load balancer, 9-3
configuring SSL and non-SSL ports, 9-5
deinstalling, D-5
deinstalling Oracle Single Sign-On Instances, D-4
installation failure, F-10
installing, 9-7
installing middle tiers, 9-26
installing on first node, 9-9
installing on subsequent nodes, 9-12
introduction, 9-1
Oracle Internet Directory passwords, 9-4
post-installation steps, 9-24
pre-installation steps, 9-2
OracleAS Cold Failover Cluster, 8-1
ASM recommendations, 8-5
clusterware agents, 8-5
deinstalling, D-4
failover, 8-4
in OracleAS Disaster Recovery environment, 10-8
installing middle tiers, 8-32
installing Oracle Delegated Administration Services and OracleAS Single Sign-On in cold failover cluster configuration, 8-24
installing regular middle tiers, 8-34
installing the OracleAS Metadata

Repository, 8-30
introduction, 8-1
mapping virtual hostname, 8-2
mapping virtual IP address, 8-2
post-installation steps, 8-31
pre-installation steps, 8-2
setting up mountable file system, 8-4
staticports.ini file, 8-32
URLs, 8-7, 8-15, 8-19
virtual hostname, 8-7, 8-15, 8-19
OracleAS Cold Failover Cluster (Identity Management), 8-14
installing, 8-17
overview of installation steps, 8-16
OracleAS Cold Failover Cluster (Infrastructure), 8-6, 8-8, 8-13, 8-27
installing, 8-8
overview of installation steps, 8-8
OracleAS Disaster Recovery, 10-1
data synchronization, 10-2
installation steps, 10-8
installing middle tiers, 10-9
installing OracleAS Infrastructure, 10-9
name resolution, 10-4
Oracle Data Guard, 10-6
setting up, 10-3
setting up identical hostnames, 10-4
staticports.ini file, 10-3
with OracleAS Cold Failover Cluster, 10-8
OracleAS Forms Services
groups required for installation, 5-6
OracleAS Infrastructure, 4-1
components, 4-2
deinstalling, D-5
Identity Management components, 4-2
installation order, 4-3
installation types, 4-1, 4-2
installing, 4-12
installing against existing Internet Directory, 4-14
installing Identity Management components, 4-16
installing Identity Management components (against existing Internet Directory), 4-18
installing in OracleAS Cold Failover Cluster, 8-8, 8-13, 8-27
installing in OracleAS Disaster Recovery, 10-9
installing Oracle Internet Directory only, 4-20
installing OracleAS Certificate Authority, 4-21
installing OracleAS Metadata Repository only, 4-15
OracleAS Metadata Repository component, 4-2
OracleAS Metadata Repository, 4-2
contents of, 4-8
groups required to install, 5-8
incorrect name shown, F-6
installing in existing database, 4-6
installing in new database, 4-15
kernel parameters required for, 2-10
port 1521, 2-15
registering with Oracle Internet Directory, 4-7
used by OracleAS Single Sign-On, 5-6
using multiple, 4-9
OracleAS Metadata Repository installation type, 4-3
OracleAS Personalization
groups required for installation, 5-6
OracleAS Portal
groups required for installation, 5-5
OracleAS Randomize Password configuration assistant, rerunning, F-7
OracleAS Reports Services
groups required for installation, 5-6
OracleAS Single Sign-On
dependency for Oracle Delegated Administration Services, 4-6
groups required for installation, 5-4
obsolete URLs on Administration screen, F-11
OracleAS Metadata Repository used by, 5-6
specifying hostname on command-line, 2-25
OracleAS Web Cache
kernel parameters required for, 2-10
OracleAS Wireless
groups required for installation, 5-6
OracleASCluster (Identity Management)
DCM warning, F-9
OracleBI Discoverer
groups required for installation, 5-6
oraInst.loc file, 2-20
creation (non-interactive installations), B-2
oraInventory directory, 2-20, 3-2
orcladmin user, 5-2
password, 5-2
OSDBA group, 2-20
OSOPER group, 2-20

P

packages
see operating system packages
parameters, kernel, 2-9
passwords
for cn=orcladmin superuser, 5-1
for ias_admin user, 3-4
for orcladmin user, 5-2
for SYS/SYSTEM users, 4-10
randomization of schema passwords, 4-7
patches
see operating system patches
PATH environment variable, 2-23
pkginfo command, 2-9
port 1521, 2-15, 2-19
already in use, 2-16
portlist.ini file, 2-15
ports, 2-12
choosing port numbers, 2-15
/etc/services file, 2-13
how to determine, 4-11
list of default port numbers, C-1
static ports, 2-14
using default port numbers, 2-13
ports 389 and 636, 2-13

post-installation steps, 11-1
for silent or non-interactive installations, B-11
OracleAS Cluster (Identity Management), 9-24
OracleAS Cold Failover Cluster, 8-31
pre-installation steps (for silent and non-interactive installations), B-2
prerequisite checks, 2-30
failures, F-3
processor speed, 2-3
processor type, 2-3
Product Languages button, 3-3
.profile file, 2-22
prtconf command, 2-4
psrinfo command, 2-3

R

RAM requirements, 2-4
realms, 5-16
record mode in the installer, B-4
registering OracleAS Metadata Repository, 4-7
remote installations, 2-27, 2-28
Repository Owners group, 5-3
requirements
64-bit support, 2-3
browser, 2-6
disk space, 2-4
environment variables, 2-22
for multihomed computers, 2-26
hostname, 2-3
IP, 2-2
kernel parameters, 2-9
memory, 2-4
monitor, 2-6
network, 2-2
operating system packages, 2-9
operating system patches, 2-7
operating system version, 2-2
processor speed, 2-3
processor type, 2-3
space in /tmp, 2-5
swap space, 2-6
response files, B-1
creating, B-3
creating using the record mode, B-4
examples, B-4
specifying on command-line, B-11
templates, B-3
reusing database name, F-12
root user, 3-6
root.sh, 3-6
runInstaller command
-executeSysPrereqs parameter, 2-2
on CD-ROM, 3-9
on DVD, 3-9
OUI_HOSTNAME parameter, 2-25

S

screens
database, 4-26
first few (infrastructure), 4-23
last few (infrastructure), 4-25
OracleAS Certificate Authority, 4-27
security tips for silent and non-interactive installations, B-11
SEMMSL errors, F-4
SHMMAX errors, F-4
showrev command, 2-8
silent installations, B-1
deinstalling, B-12
post-installation steps, B-11
pre-installation steps, B-2
security tips, B-11
silentInstall.log, B-11
Solaris 8, patches required for, 2-8
Solaris 9, patches required for, 2-8
Solaris Management Console
creating groups using, 2-19
creating users using, 2-21
Specify Login for Oracle Internet Directory screen, 5-16
Specify Namespace in Internet Directory screen, 2-24, 4-11
SSL
connecting to Oracle Internet Directory using, 3-7
post-installation configuration, 11-2
starting grid control plug-in installer, A-1
starting Oracle Universal Installer, 3-9
static ports, 2-14
examples, 2-16
not working, 2-16
staticports.ini file, 2-14
creating, 2-14
for OracleAS Cold Failover Cluster, 8-32
format, 2-14
in OracleAS Disaster Recovery, 10-3
su command, 2-22
swap command, 2-6
swap space requirement, 2-6
symbolic links
using, 3-2
synchronize clocks for OracleAS Cluster (Identity Management), 9-3
SYS/SYSTEM user passwords, 4-10
system requirements, 2-2

T

TEMP environment variable, 2-24
/tmp directory, 2-24, 3-6
space required, 2-5
TNS_ADMIN environment variable, 2-23, F-8
tnsnames.ora file, 2-23
topologies
10.1.4.0.1 identity federation, 1-3
10.1.4.0.1 infrastructure, 1-3
distributed identity management with integrated HTTP server, 1-5
distributed identity management with

standalone HTTP server, 1-7
high availability, 1-3
identity management in a single oracle home, 1-5
with 10.1.2 middle tiers, 1-4
with 10.1.3 middle tiers, 1-4
supported, 1-3 to 1-9
troubleshooting, F-1
configuration assistants, E-1
deinstallation, F-11
general tips, F-1
Trusted Application Admins group, 5-2

U

Use Only SSL Connections With This Oracle Internet Directory button, 3-7
user interface problems, F-5
User Management Application Admins group, 5-2
users (operating system)
see operating system users
users (Oracle Internet Directory)
see Oracle Internet Directory users

V

/var/opt/oracle directory, 3-6
oraInst.loc file, 2-20
virtual hostname
OracleAS Cold Failover Cluster, 8-7, 8-15, 8-19
virtual IP, 7-2
virtual server
configuring HTTP for OracleAS Cluster (Identity Management), 9-3
configuring LDAP virtual server for OracleAS Cluster (Identity Management), 9-3
pointing to node 1 initially for OracleAS Cluster (Identity Management), 9-3

W

Welcome page, URL for, 11-1