Oracle® Application Server

Enterprise Deployment Guide

10*g* Release 3 (10.1.3.1.0)

B28939-03

January 2008

ORACLE®

Oracle Application Server Enterprise Deployment Guide 10*g* Release 3 (10.1.3.1.0)

B28939-03

Copyright © 2004, 2008, Oracle. All rights reserved.

Primary Author: Julia Pond

Contributing Authors: Janga Aliminati, Fermin Castro, Dheeraj Goswami, Mark Kennedy, Peter LaQuerre, Peter Lubbers, Greg Sowa, Tim Willard

Contributors: Senthil Arunagirinathan, Theresa Bandy, Rachel Chan, Somendu Chakraborty, Orlando Cordero, Eileen He, Pavana Jain, Pushkar Kapasi, Rajiv Maheshwari, Rahul Menezes, Mark Nelson, Lei Oh, Ted Regan, Dhaval Shah, Malai Stalin, Yaqing Wang

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 vii

Intended Audience vii
Documentation Accessibility vii
Related Documents viii
Conventions viii

1 What is an Enterprise Deployment?

1.1 Description 1-1
1.2 Benefits 1-2
1.2.1 Built-in Security 1-2
1.2.2 High Availability 1-2
1.3 In This Guide 1-2
1.4 How to Use This Guide 1-8
1.5 Hardware Requirements 1-8
1.6 Variants 1-9
1.6.1 Multi master Replication with Oracle Internet Directory 1-9
1.6.2 OracleAS Cold Failover Cluster (Identity Management) 1-10
1.6.3 Forward and Reverse Proxies for Oracle HTTP Server 1-10

2 Configuring the Data Tier

2.1 Installing the Oracle Application Server Metadata Repository for the Security Infrastructure 2-1
2.1.1 Configuring the Time out Value in the sqlnet.ora File 2-2
2.2 Configuring Fast Connection Failover for the RAC Database on INFRADBHOST1 and INFRADBHOST2 2-2
2.3 Installing the Oracle Internet Directory Instances in the Data Tier 2-2
2.3.1 Installing the First Oracle Internet Directory Instance 2-2
2.3.2 Installing the Second Oracle Internet Directory Instance 2-5
2.4 Configuring the Virtual Server to Use the Load Balancing Router 2-7
2.5 Testing the Oracle Internet Directory Instances 2-8
2.6 Installing the ORABPEL, ORAESB and ORAWSM Schemas 2-9

3 Installing and Configuring the mySOACompany Web and Application Tiers

3.1 Installing and Configuring the Web and Application Tiers 3-1
3.1.1 Installing the Oracle HTTP Servers on WEBHOST1 and WEBHOST2 3-1

3.1.2 Renaming Apache 2.0 Web Server Instances ... 3-3
3.1.3 Configuring the Cluster Gateway ... 3-3
3.1.4 Configuring the Firewall to Prevent Access to Application Server Control Console 3-4
3.1.5 Installing the Application Server Instances on APPHOST1 and APPHOST2 ... 3-4
3.1.6 Disabling Application Server Control Console on APPHOST2-4 (Optional) ... 3-6
3.1.7 Listing Occupied Ports ... 3-7
3.1.8 Creating OC4J Instances on APPHOST1 and APPHOST2 ... 3-7
3.1.9 Configuring the Oracle HTTP Server with the Load Balancing Router ... 3-8
3.1.10 Configuring the esbd.myco.com URL for Internal Use ... 3-10
3.1.11 Installing the Oracle BPEL Process Manager Instances on APPHOST1 and APPHOST2 from the Oracle BPEL Process Manager (10.1.3.1.0) CD ... 3-11
3.1.12 Configuring the Cluster of BPEL Instances ... 3-12
3.1.12.1 Necessary Steps for Cluster-based BPEL Deployments ... 3-13
3.1.13 Installing the ESB Runtime Instances on APPHOST1 and APPHOST2 from the Oracle Enterprise Bus (10.1.3.1.0) CD ... 3-14
3.1.14 Resolving Out-of-Memory Errors in the BPEL Runtime Console ... 3-15
3.1.15 Installing the ESB Repository Instance on APPHOST1 and APPHOST2 ... 3-15
3.1.16 Configuring Service Failover for the OC4J_ESBDT Instances ... 3-16
3.1.17 Configuring ESB for Singleton Adapters ... 3-16
3.1.18 Configuring the Cluster of ESB Runtime Instances on APPHOST1 and APPHOST2 ... 3-16
3.1.19 Updating the ESB Metadata ... 3-17
3.1.20 Configuring the Slide Repository to use the Database as the Repository ... 3-17
3.1.21 Configuring JNDIs for the Topic and Topic Connection Factory ... 3-18
3.1.22 Installing the OWSM Instances on APPHOST1 and APPHOST2 from the Oracle Web Services Manager (10.1.3.1.0) CD ... 3-19
3.1.23 Disabling Applications on APPHOST1 and APPHOST2 ... 3-20
3.1.24 Configuring the OWSM Cluster ... 3-20
3.1.25 Configuring the Firewall for the Application Tier ... 3-22
3.1.26 Deploying J2EE Applications ... 3-23
3.1.27 Configuring Static Discovery to Eliminate Multicast Traffic ... 3-25
3.2 Configuring Fast Connection Failover for the RAC Database on APPHOST1 and APPHOST2 ... 3-26
3.3 Managing Oracle Application Server Component Connections ... 3-27
3.4 Configuring Network Communication ... 3-27
3.5 Configuring Application Authentication and Authorization ... 3-28
3.5.1 Configuring the Cluster of BPEL Instances on APPHOST1 and APPHOST2 to use Oracle Internet Directory ... 3-28
3.5.2 Configuring Java SSO ... 3-29
3.5.3 Disabling the Worklist Application ... 3-31

4 Installing and Configuring Oracle Access Manager

4.1 Understanding Oracle Access Manager Components ... 4-2
4.2 The mySOACompany Oracle Access Manager Authentication and Authorization Process ... 4-3
4.3 Preparing to Install Oracle Access Manager Components ... 4-3
4.4 Installing the First Identity Server on IDMHOST1 ... 4-4
4.5 Installing WebPass on WEBHOST1 ... 4-6

4.6 Configuring the First Identity Server 4-8
4.7 Installing the Second Identity Server on IDMHOST2 4-10
4.8 Installing WebPass on WEBHOST2 4-12
4.9 Configuring the Second Identity Server 4-12
4.10 Installing the Access System 4-14
4.10.1 Installing the Web Server for the Policy Manager 4-14
4.10.2 Installing WebPass for the Policy Manager 4-14
4.10.3 Installing the Policy Manager on ADMINHOST 4-15
4.10.4 Configuring the Policy Manager 4-16
4.10.5 Installing the Access Server on IDMHOST1 and IDMHOST2 4-18
4.10.6 Installing the WebGate 4-21
4.11 Configuring the Access Server with the Load Balancing Router 4-25
4.12 Installing the Access Server SDK 4-25
4.12.1 Installing the Access SDK on APPHOST1 and APPHOST2 (Windows) 4-25
4.12.2 Installing the Access SDK on APPHOST1 and APPHOST2 (Solaris and Linux) 4-26
4.12.3 Configuring the AccessGate on APPHOST1 and APPHOST2 4-27
4.13 Configuring Oracle Access Manager Single Sign-On for OC4J Applications 4-29
4.13.1 Configuring Access to SOA Components 4-29
4.13.2 Configuring the Login Protected by Oracle Access Manager 4-30
4.13.3 Configuring the Logout 4-33
4.14 Configuring the Second Identity Server as a Failover Server 4-33
4.14.1 Configuring Failover Between the Secondary Identity Server on IDMHOST2 and the WebPass 4-34
4.15 Configuring the Second Access Server as a Failover Server 4-34
4.15.1 Configuring Failover Between the Access Server and WebGate 4-35
4.16 Mitigating Identity Server Product Installation Failures on Linux 4-35
4.17 Configuring Directory Server Failover 4-36
4.17.1 Configuring Directory Failover for User Data 4-37
4.17.2 Configuring Directory Failover for Oracle and Policy Data 4-38
4.17.2.1 Configuring Identity Server Failover for Oracle Data 4-38
4.17.2.1.1 Creating the failover.xml File 4-38
4.17.2.1.2 Configuring Identity Server Directory Failover for Oracle Data 4-39
4.17.2.1.3 Creating the Encrypted Password for the Bind DN 4-39
4.18 Configuring Access Server Directory Failover for Oracle and Policy Data 4-40
4.18.1 Adding a Failover Directory Server Using the ConfigureAAAServer Tool 4-40
4.19 Configuring Policy Manager Failover 4-41
4.20 Creating Failover LDAP Directory Server Profiles for the Identity and Access Servers 4-41
4.20.1 Creating a Directory Server Profile for the Identity Servers 4-41
4.20.2 Creating a Directory Server Profile for the Access Servers 4-43
4.21 Verifying the Status of the Identity Servers 4-45

5 Installing and Configuring Oracle Single Sign-On and Oracle Delegated Administration Services

5.1 Setting up the Load Balancing Router 5-1
5.2 Installing the Oracle HTTP Servers on WEBHOST3 and WEBHOST4 5-1
5.2.1 Renaming Apache 2.0 Web Server Instances 5-3

5.2.2 Configuring the Oracle HTTP Server with the Load Balancing Router 5-3
5.2.3 Configuring the esbd.myco.com URL for Internal Use 5-5
5.3 Installing and Configuring Oracle Single Sign-On 5-6
5.3.1 Installing the First Identity Management Configuration 5-6
5.3.2 Testing the Identity Management Components With Oracle Internet Directory 5-9
5.3.3 Installing the Second Identity Management Configuration 5-9
5.4 Reconfiguring Oracle Single Sign-On and Oracle Delegated Administration Services with the Oracle HTTP Servers 5-11
5.5 Testing the Identity Management Tier Components 5-14
5.6 Configuring Session State Replication for the OC4J_SECURITY Instance 5-15
5.7 Disabling the Oracle HTTP Server on the Identity Management Tier 5-15

6 Maintaining the SOA Suite

6.1 Managing the SOA Suite 6-1
6.2 Enabling Disaster Recovery 6-1

Index

Preface

This preface describes the audience, contents and conventions used in the *Oracle Application Server Enterprise Deployment Guide*.

Intended Audience

This guide is intended for system administrators who are responsible for installing and configuring Oracle Application Server.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

The following manuals in the Oracle Application Server documentation library provide additional information on the process of installing and configuring the Enterprise Deployment architectures:

- *Oracle Application Server Concepts*
- *Oracle Application Server Installation Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Application Server Single Sign-On Administrator's Guide*
- *Oracle Application Server Administrator's 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.
/	A forward slash is used as a directory separator in paths, regardless of platform.

1 What is an Enterprise Deployment?

Description

Benefits

In This Guide

Hardware Requirements

Variants

1.1 Description

An enterprise deployment of Oracle SOA Suite is a reference configuration that is designed to support large-scale, mission-critical business software applications using SOA components. The hardware and software in an Enterprise Deployment configuration delivers:

High quality service

- The system workload is managed and balanced effectively
- Applications continue to operate when resources are added or removed
- System maintenance and unexpected failures cause minimal downtime

Built-in Security

- All incoming network traffic is received by the Load Balancing Router on a single, secure port and directed to internal IP addresses within the firewall; inside the firewall, functional components are grouped within DMZs
- User accounts are provisioned and managed centrally
- Security systems are integrated
- Administrative access is isolated

Efficient software provisioning and management

- Application distribution is simple
- Systems are managed and monitored as one logical unit in a central console
- Death detection and restart mechanisms ensure availability

1.2 Benefits

The Oracle Application Server configurations discussed in this guide are designed to ensure security of all transactions, maximize hardware resources, and provide a reliable, standards-compliant system for enterprise computing with a variety of applications. The security and high availability benefits of the Oracle Application Server configurations are realized through isolation in firewall zones and replication of software components.

1.2.1 Built-in Security

The Enterprise Deployment architectures are secure because every functional group of software components is isolated in its own DMZ, and all traffic is restricted by protocol and port. The following characteristics ensure security at all needed levels, as well as a high level of standards compliance:

- All external communication received on port 80 is redirected to port 443.
- Communication from external clients does not go beyond the Load Balancing Router level.
- No direct communication from the Load Balancing Router to the Data tier DMZ is allowed.
- Components are separated between DMZs on the Web Tier, Application Tier, and the Data Tier.
- Direct communication between two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- Oracle Internet Directory is isolated in the Data tier DMZ.
- Identity Management components are in the DMZ.
- All communication between components across DMZs is restricted by port and protocol, according to firewall rules.

1.2.2 High Availability

The Enterprise Deployment architectures are highly available, because each component or functional group of software components is replicated on a different computer, and configured for component-level high availability.

1.3 In This Guide

Enterprise Deployments with the Oracle SOA Suite provide highly available, scalable and secure deployments of Oracle Enterprise Service Bus (ESB), Oracle BPEL Process Manager (BPEL), and Oracle Web Services Manager (OWSM).

This guide provides configuration instructions for these Enterprise Deployments of the Oracle SOA Suite, with different security options:

- mySOACompany with JSSO and Oracle Internet Directory (shown in Figure 1–1)
- mySOACompany with Oracle Access Manager (shown in Figure 1–2)
- mySOACompany with Oracle Single Sign-On (shown in Figure 1–3).

Table 1–1 lists the security configurations and the identity and policy stores used with them.

The policy store is the repository for OracleAS JAAS Provider authorization permissions and grants. Oracle Internet Directory and XML (the *ORACLE_HOME*/j2ee/home/system-jazn-data.xml file) are supported as policy store repositories.

User accounts and roles are always seeded in an enterprise identity store (typically an LDAP server), and are not replicated in the policy store. The policy store only has grants and references to groups and roles in the enterprise identity store. The same repository (Oracle Internet Directory or an XML file) can be used as both the identity and policy store.

In the Oracle SOA Suite, the Oracle BPEL Process Manager console uses OracleAS JAAS Provider permissions to secure and enforce user access to the Oracle BPEL Process Manager console functions. The policy store contains grants to users and roles to provide access to Oracle BPEL Process Manager server functions.

Table 1–1 Supported Security Configurations

Deployment Configuration	Policy Store	Identity Store
mySOACompany with Java SSO	OracleAS JAAS Provider and Oracle Internet Directory	OracleAS JAAS Provider and Oracle Internet Directory
mySOACompany with Oracle Single Sign-On	OracleAS JAAS Provider and Oracle Internet Directory	OracleAS JAAS Provider-Oracle Internet Directory
mySOACompany with Oracle Access Manager[1]	OracleAS JAAS Provider and XML	OracleAS JAAS Provider and Oracle Internet Directory[2]

[1] See Chapter 11 of the *Oracle Containers for J2EE Security Guide* for information on adding permissions in Oracle Access Manager environments.

[2] When Oracle Access Manager is used with OracleAS JAAS Provider and XML as the policy store and Oracle Internet Directory as the identity store, you must ensure that all user accounts and roles are in the identity store (Oracle Internet Directory), and that the policy grants are in the policy store (the system-jazn-data.xml file). Grants in this file must refer to users in the identity store (Oracle Internet Directory).

The servers in the mySOACompany system are grouped into tiers as follows:

- **Web Tier** — WEBHOST1 and WEBHOST2, with Oracle HTTP Server installed.
- **Application Tier** — APPHOST1 and APPHOST2, with Oracle Containers for J2EE installed, and multiple OC4J instances with applications deployed.

  In mySOACompany with Oracle Access Manager, this tier also includes WebGate, WebPass, and Oracle Access Manager Identity Server, Access Server, Access Manager, and ADMINHOST, for administrator use.

  In mySOACompany with Oracle Single Sign-On, this tier includes IDMHOST1 and IDMHOST2, with Oracle Single Sign-On and Oracle Delegated Administration Services.
- **Data Tier** — OIDHOST1 and OIDHOST2, with 10*g* Release 3 (10.1.4.0.1) Oracle Internet Directory installed, and INFRADBHOST1 and INFRADBHOST2, the two-node Real Application Clusters database.

Figure 1–1 mySOACompany with JSSO and Oracle Internet Directory

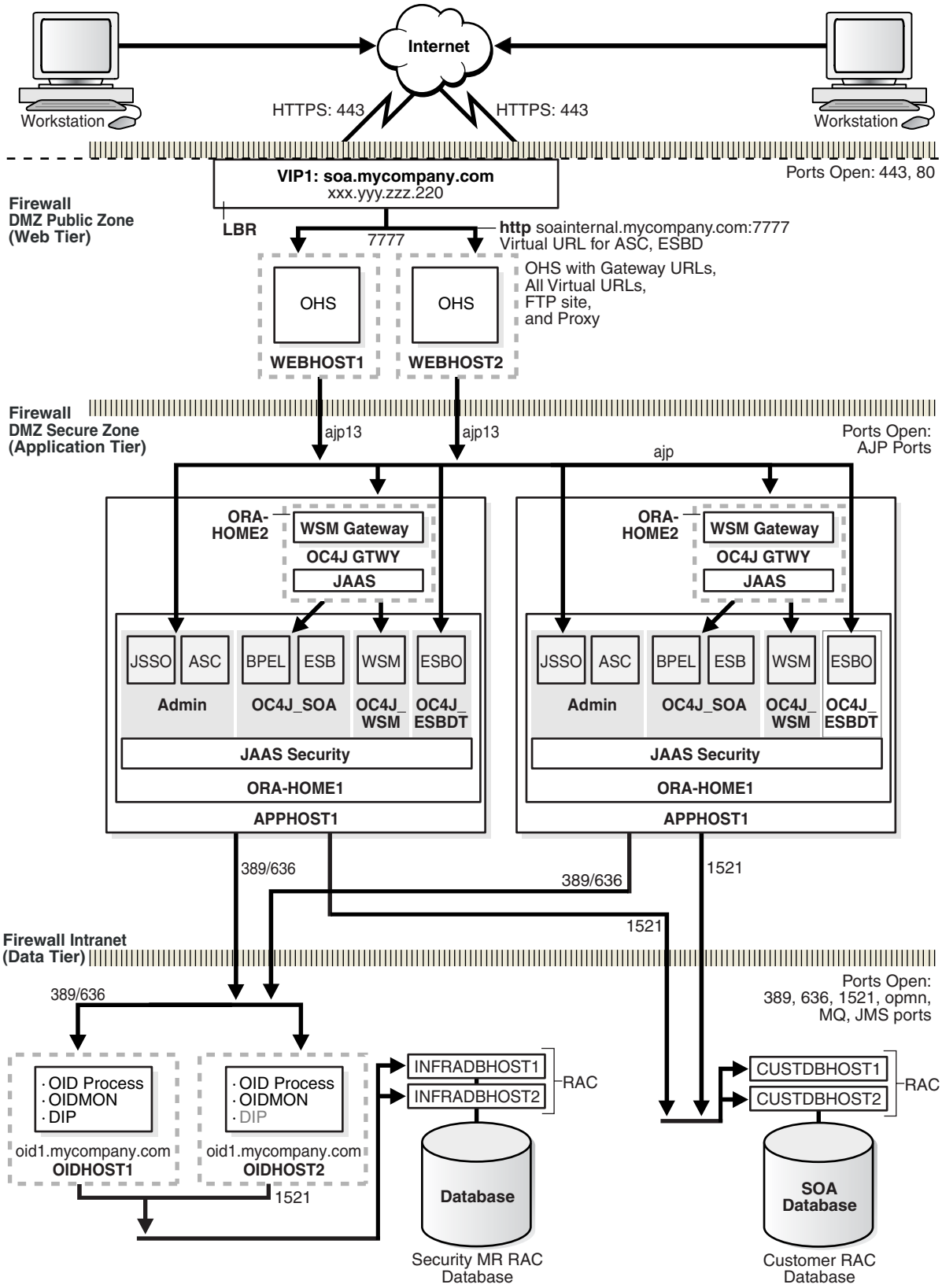


Figure 1–2 mySOACompany with JSSO and Oracle Access Manager

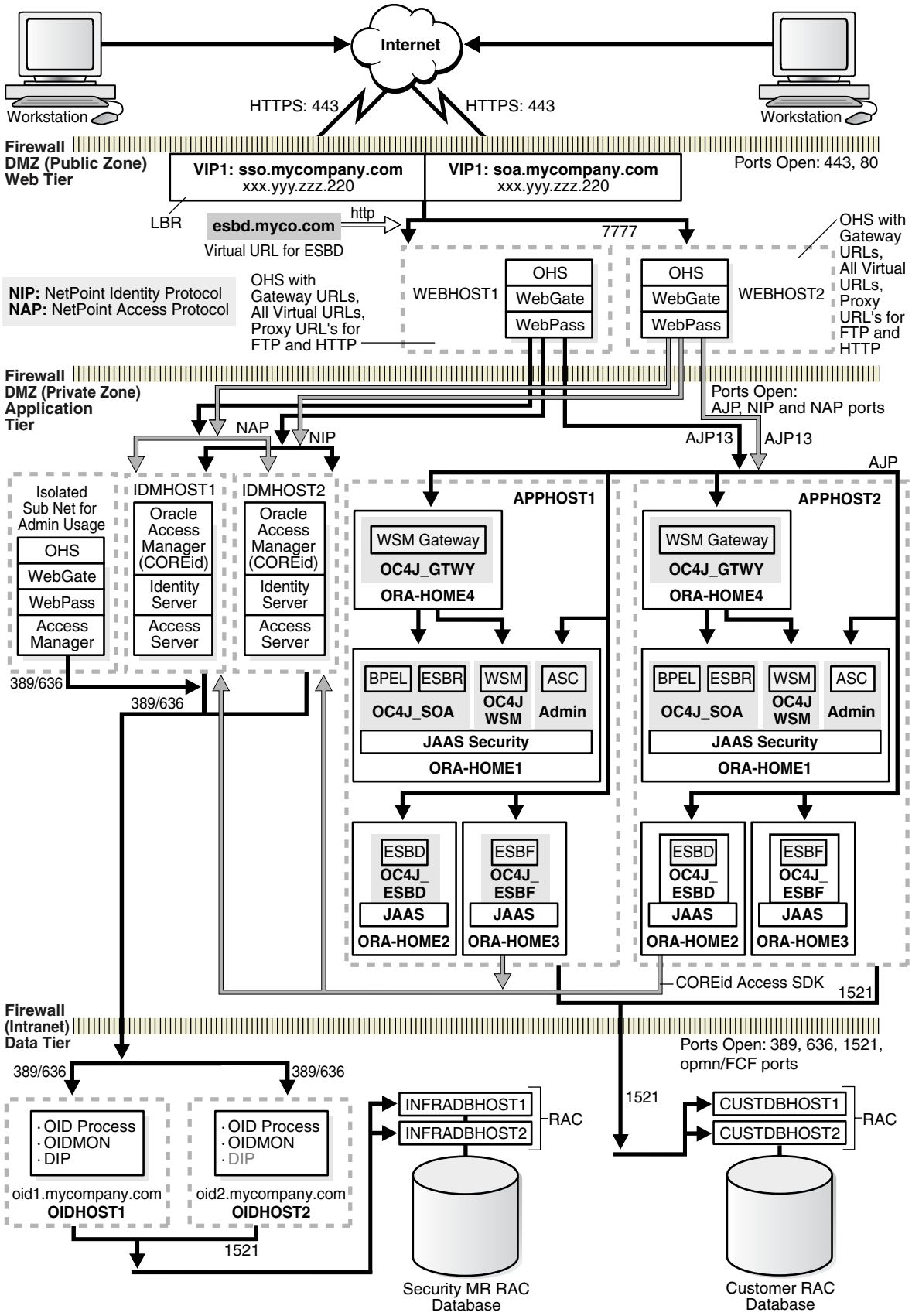
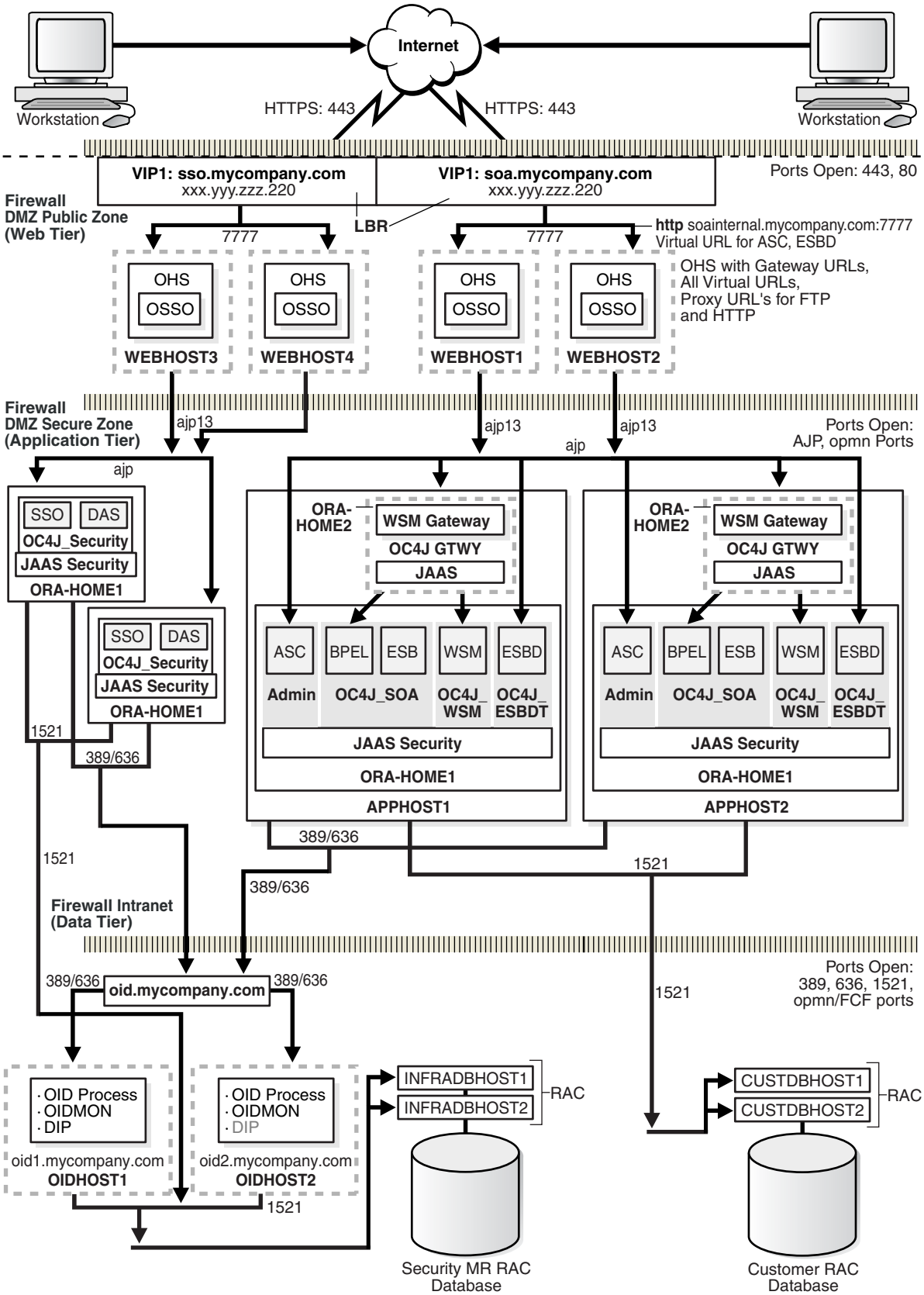


Figure 1–3 mySOAcompany with Oracle Single Sign-On


Internet
Workstation
HTTPS: 443
HTTPS: 443
Workstation
VIP1: sso.mycompany.com
xxx.yyy.zzz.220
VIP1: soa.mycompany.com
xxx.yyy.zzz.220
Ports Open: 443, 80
Firewall
DMZ Public Zone
(Web Tier)
LBR
7777
7777
http soainternal.mycompany.com:7777
Virtual URL for ASC, ESBD
OHS with Gateway URLs,
All Virtual URLs,
Proxy URL's for FTP
and HTTP
OHS
OSSO
WEBHOST3
WEBHOST4
WEBHOST1
WEBHOST2
Firewall
DMZ Secure Zone
(Application Tier)
ajp13
ajp13
ajp13
ajp
Ports Open:
AJP, opmn Ports
ajp
SSO
DAS
OC4J_Security
JAAS Security
ORA-HOME1
ORA-
HOME2
WSM Gateway
OC4J GTWY
JAAS
ASC
BPEL
ESB
WSM
ESBD
Admin
OC4J_SOA
OC4J_
WSM
OC4J_
ESBDT
JAAS Security
ORA-HOME1
APPHOST1
APPHOST2
1521
389/636
389/636
1521
389/636
1521
Firewall Intranet
(Data Tier)
Ports Open:
389, 636, 1521,
opmn/FCF ports
389/636
oid.mycompany.com
389/636
1521
· OID Process
· OIDMON
· DIP
oid1.mycompany.com
OIDHOST1
· OID Process
· OIDMON
· DIP
oid2.mycompany.com
OIDHOST2
1521
INFRADBHOST1
INFRADBHOST2
RAC
CUSTDBHOST1
CUSTDBHOST2
RAC
Security MR RAC
Database
Customer RAC
Database

1.4 How to Use This Guide

Table 1–2 summarizes the process by which you install and configure mySOACompany with each of the user authentication methods. Follow the procedures indicated in the first column, in the order shown, for the chosen configuration.

Table 1–2 Enterprise Deployment Configuration Procedures

Perform the steps in...	To configure mySOACompany with JSSO and Oracle Internet Directory	To configure mySOACompany with Oracle Access Manager	To configure mySOACompany with Oracle Single Sign-On
Chapter 2, "Configuring the Data Tier"	Yes	Yes	Yes
Section 3.1, "Installing and Configuring the Web and Application Tiers"	Yes	Yes	Yes
Section 3.2, "Configuring Fast Connection Failover for the RAC Database on APPHOST1 and APPHOST2"	Yes	Yes	Yes
Section 3.3, "Managing Oracle Application Server Component Connections"	Yes	Yes	Yes
Section 3.4, "Configuring Network Communication"	Yes	Yes	Yes
Section 3.5.1, "Configuring the Cluster of BPEL Instances on APPHOST1 and APPHOST2 to use Oracle Internet Directory"	Yes	Yes	Yes
Section 3.5.2, "Configuring Java SSO"	Yes	No	No
Chapter 4, "Installing and Configuring Oracle Access Manager"	No	Yes	No
Chapter 5, "Installing and Configuring Oracle Single Sign-On and Oracle Delegated Administration Services"	No	No	Yes

1.5 Hardware Requirements

Table 1–3 and Table 1–4 list minimum hardware requirements for the Enterprise Deployment on Windows and Linux operating systems, respectively. The memory figures represent the memory required to install and run Oracle Application Server; however, for most production sites, you should configure at least 1 GB of physical memory.

For detailed requirements, or for requirements for a platform other than these, see the *Oracle Application Server Installation Guide for Microsoft Windows* for the platform in use.

Table 1–3 mySOACompany Hardware Requirements (Windows)

Server	Processor	Disk	Memory	TMP Directory	Swap
WEBHOST	300 MHz or higher Intel Pentium processor recommended	400 MB	512 MB	55 MB to run the installer; 256 MB needed for some installation types	512 MB
APPHOST	300 MHz or higher Intel Pentium processor recommended	2 GB	1 GB	400	1 GB
OIDHOST and INFRADBHOST	300 MHz or higher Intel Pentium processor recommended	2.5 GB	1 GB	55 MB to run the installer; 256 MB needed for some installation types	1 GB
ADMINHOST	300 MHz or higher Intel Pentium processor recommended	400 MB	512 MB	n/a	512 MB

Table 1–4 mySOACompany Hardware Requirements (Linux)

Server	Processor	Disk	Memory	TMP Directory	Swap
WEBHOST	Pentium (32-bit), 450 MHz or greater	520 MB	512 MB	400 MB	1.5 GB
APPHOST	Pentium (32-bit), 450 MHz or greater	2 GB	1 GB	400	1.5 GB
OIDHOST and INFRADBHOST	Pentium (32-bit), 450 MHz or greater	2.5 GB	1 GB	400 MB	1.5 GB
ADMINHOST	Pentium (32-bit), 450 MHz or greater	520 MB	512 MB	400 MB	1.5 GB

Production requirements vary depending on applications and the number of users. All Enterprise Deployment configurations described in this guide use two servers for each tier to provide failover capability; however, this does not presume adequate computing resources for any application or user population. If the system workload increases such that performance is degraded, you can add servers to the configuration by repeating the instructions for the installation and configuration of the second server on the tier (WEBHOST2, APPHOST2, INFRADBHOST2) to add a third server where it is needed.

1.6 Variants

The variants described in this section enable you to achieve deployment goals using fewer servers, different software, or alternative configurations.

1.6.1 Multi master Replication with Oracle Internet Directory

Multi master replication is an Oracle Internet Directory software solution that ensures read and write access to Oracle Internet Directory at all times, if at least one of the directory servers in the system remains available. When an Oracle Directory server resumes functioning after being unavailable, replication from the surviving directory server resumes automatically and synchronizes the contents between the directory servers forming the directory replication group. In addition, any changes made on one directory server instance are reflected on the second directory server instance.

To implement multi master replication in Oracle Internet Directory, follow the instructions in the *Oracle Internet Directory Administrator's Guide*, Oracle Internet Directory Replication Administration chapter, section titled "Installing and Configuring Multi master Replication".

1.6.2 OracleAS Cold Failover Cluster (Identity Management)

The OracleAS Cold Failover Cluster (Identity Management) solution is a hardware cluster comprising two computers. The computer that is actively executing an Infrastructure installation at any given time is called the primary (hot) node. If this node fails, the hardware cluster automatically diverts Infrastructure operations to the secondary (cold) node.

Each hardware cluster node is a standalone server that runs its own set of processes, but accesses a shared storage subsystem. The cluster can access the same storage, usually disks, from both nodes, but only the primary node has active access to the storage at any given time. If the primary node fails, the hardware cluster's software grants the secondary node access to the storage.

Note: For a detailed discussion of the OracleAS Cold Failover Cluster (Identity Management) solution, see the *Oracle Application Server High Availability Guide*.

The OracleAS Cold Failover Cluster (Identity Management) solution differs from the standard configuration in the following ways:

- The Oracle Internet Directory server and the database are on the same computer, whereas in the standard configuration the first Oracle Internet Directory instance and a database instance occupy OIDHOST1 and INFRADBHOST1, while the second Oracle Internet Directory instance and a database instance occupy OIDHOST2 and INFRADBHOST2. Thus, the OracleAS Cold Failover Cluster (Identity Management) solution operates two fewer servers than the RAC configuration.
- In the event of node failure, clients will experience a brief interruption of service while the workload is diverted to the cold node.

To implement the OracleAS Cold Failover Cluster (Identity Management) solution:

1. Obtain and configure a hardware cluster.
2. Install and configure the Oracle Application Server instances on the cluster computers to use the OracleAS Cold Failover Cluster (Identity Management) solution. Follow the instructions in the *Oracle Application Server Installation Guide for Microsoft Windows*, "Installing an OracleAS Cold Failover Cluster (Identity Management) Configuration".
3. Manage the OracleAS Cold Failover Cluster (Identity Management) solution, following the instructions from the *Oracle Application Server High Availability Guide*, "Managing Oracle Application Server Cold Failover Cluster (Identity Management)".

1.6.3 Forward and Reverse Proxies for Oracle HTTP Server

Proxies change the way the Oracle HTTP Server processes client requests.

A forward proxy is an intermediary server between a client and the origin server containing the content. Forward proxies are usually used to provide Internet access to internal clients that are otherwise restricted by a firewall. To get content from the origin server, the client sends a request to the proxy, naming the origin server as the target. The proxy requests the content from the origin server and returns it to the client. The client must be configured to use the forward proxy to access other sites.

A reverse proxy is a server that appears to outside clients to be the content server. It relays requests from outside the firewall to servers behind the firewall, and delivers retrieved content back to the client. A firewall rule allows access only to the proxy server, so that the content servers are protected. The proxy server changes URLs listed in the headers of any messages generated by the content servers, so that external clients are given no information about the servers behind the firewall. No configuration of clients is necessary with a reverse proxy (the client makes requests for content in the name-space of the reverse proxy). The reverse proxy decides where to send the requests, and returns the content as if it was the origin server.

2

Configuring the Data Tier

Installing the Oracle Application Server Metadata Repository for the Security Infrastructure

Configuring Fast Connection Failover for the RAC Database on INFRADBHOST1 and INFRADBHOST2

Installing the Oracle Internet Directory Instances in the Data Tier

Configuring the Virtual Server to Use the Load Balancing Router

Testing the Oracle Internet Directory Instances

Installing the ORABPEL, ORAESB and ORAWSM Schemas

2.1 Installing the Oracle Application Server Metadata Repository for the Security Infrastructure

You must install the 10*g*(10.1.4.0.1) OracleAS Metadata Repository into the Real Application Clusters database before you install components into the Security DMZ. Oracle Application Server provides a tool, the Oracle Application Server Repository Creation Assistant, to create the OracleAS Metadata Repository in an existing database.

The 10*g* (10.1.4.0.1) OracleAS RepCA is available on the OracleAS RepCA CD-ROM or the Oracle Application Server DVD-ROM. You install the OracleAS RepCA in its own, separate Oracle home.

To install and execute the OracleAS Metadata Repository, you must perform these steps:

1. Install the OracleAS RepCA into the Real Application Clusters database, following the steps in the *Oracle Application Server Metadata Repository Creation Assistant User's Guide for Microsoft Windows* for the platform you are using. You can find this guide in the Oracle Application Server documentation library (Getting Started tab).
2. Ensure that the database meets the requirements specified in the "Database Requirements" section of the *Oracle Application Server Metadata Repository Creation Assistant User's Guide for Microsoft Windows*. In addition, ensure that the database computer has at least 512 MB of swap space available for execution of the OracleAS RepCA
3. Execute the OracleAS RepCA.

   The RepCA creates the schemas listed in the *Oracle Application Server Metadata Repository Creation Assistant User's Guide for Microsoft Windows.*

4. Perform the post-installation step described in Section 2.1.1.

2.1.1 Configuring the Time out Value in the sqlnet.ora File

You must configure the `SQLNET.EXPIRE_TIME` parameter in the `sqlnet.ora` file on the application infrastructure database.

1. Open the file *ORACLE_HOME*`/network/admin/sqlnet.ora` file (UNIX) or the *ORACLE_BASE*`/` *ORACLE_HOME*`/network/admin/sqlnet.ora` file (Windows).
2. Set the `SQLNET.EXPIRE_TIME` parameter to a value lower than the TCP session time out value for the Load Balancing Router and firewall.
3. Restart the listener by issuing these commands in *ORACLE_HOME*`/bin`:

```
lsnrctl stop

lsnrctl start
```

2.2 Configuring Fast Connection Failover for the RAC Database on INFRADBHOST1 and INFRADBHOST2

Fast Connection Failover provides failover for a JDBC connection to a 10*g* R1 or 10*g* R2 RAC database. Upon failure of a RAC node, Oracle Notification Service (ONS) detects the failure and an SQL exception is thrown to application code. To enable Fast Connection Failover on INFRADBHOST1 and INFRADBHOST2:

1. Open the *ORACLE_HOME*`/opmn/conf/ons.conf` file .
2. Add the following:

```
localport=6100
remoteport=6200
nodes=infradbhost1.mycompany.com:6200,infradbhost2.mycompany.com:6200
```

3. Save and close the file.

Note: Additional configuration is required on the application tier (see Section 3.2, "Configuring Fast Connection Failover for the RAC Database on APPHOST1 and APPHOST2").

2.3 Installing the Oracle Internet Directory Instances in the Data Tier

Follow these steps to install the Oracle Internet Directory components (OIDHOST1 and OIDHOST2) on the Data Tier with the Metadata Repository. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

Note: Ensure that the clocks are synchronized between the two computers on which you intend to install the Oracle Internet Directory instances. Errors will occur if this is not done.

2.3.1 Installing the First Oracle Internet Directory Instance

The OracleAS Metadata Repository must be running before you perform this task. Follow these steps to install the 10*g* (10.1.4.0.1)Oracle Internet Directory on OIDHOST1:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Ensure that ports 389 and 636 are not in use by any service on the computer by issuing these commands for the operating system you are using. (If the port is not in use, no output is returned from the command.)

   On UNIX:

   `netstat -an | grep "389"`

   `netstat -an | grep "636"`

   On Windows:

   `netstat -an | findstr :389`

   `netstat -an | findstr :636`

   If the port is in use (if the command returns output identifying the port), you must free the port.

   In UNIX:

   Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, or restart the computer.

   In Windows:

   Stop the component that is using the port.
3. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.
4. Edit the `staticport.ini` file to assign the following custom ports:

   ```
   Oracle Internet Directory port = 389
   Oracle Internet Directory (SSL) port = 636
   ```

5. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.
6. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.
7. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.
8. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.
9. Open a window and run the script, following the prompts in the window.
10. Return to the Oracle Universal Installer screen and click **Next**.

    The **Specify File Locations** screen appears with default locations for:

    - The product files for the installation (Source)

- The name and path to an Oracle home (Destination)

Note: It is a good idea to make the Oracle home directory path for OIDHOST1 the same as the path to the Oracle home location of OIDHOST2. For example, if the path to the Oracle home on OIDHOST1 is:

```
/u01/app/oracle/product/AS10gOID
```

then the path to the Oracle home on OIDHOST2 should be:

```
/u01/app/oracle/product/AS10gOID
```

---

11. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

12. Select OracleAS Infrastructure 10*g* and click **Next**.

    The **Select Installation Type** screen appears.

13. Select **Identity Management** and click **Next**.

    The **Upgrade Existing Oracle Application Server (10.1.2) Infrastructure** screen appears.

14. Select **Install New Oracle Application Server Infrastructure 10*g* (10.1.4.0.1)** and click **Next**.

    The **Product-Specific Prerequisite Checks** screen appears.

15. Click **Next**.

    The **Confirm Pre-Installation Requirements** screen appears.

16. Ensure that the requirements are met, check the box for each, and click **Next**.

    The **Select Configuration Options** screen appears.

17. Select **Oracle Internet Directory**, **OracleAS Directory Integration and Provisioning**, and **High Availability and Replication** and click **Next**.

    The **Specify Port Configuration Options** screen appears.

18. Select **Manual** and click **Next**.

    The **Specify Repository** screen appears.

19. Provide the DBA login and computer information and click **Next**.

Note: The syntax for the hostname and port field for a RAC database is:

```
infradbhost1.mycompany.com:1521^infradbhost2.mycompany.com:1521^
```

    The **Select High Availability or Replication Option** screen appears.

20. Select **OracleAS Cluster (Identity Management)** and click **Next**.

    The **Specify Namespace in Internet Directory** screen appears.

21. Click **Next** to specify the default **Suggested Namespace**, or enter values for the **Custom Namespace** and click **Next**.

The **Specify Instance Name and ias_admin Password** screen appears.

22. Specify the instance name and password and click **Next**.

    The **Summary** screen appears.

23. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.

24. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.

25. Click **Exit**, and then confirm your choice to exit.

2.3.2 Installing the Second Oracle Internet Directory Instance

The OracleAS Metadata Repository and the first Oracle Internet Directory instance must be running before you perform this task. Follow these steps to install the 10*g* Release 2 (10.1.2) Oracle Internet Directory on OIDHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Ensure that ports 389 and 636 are not in use by any service on the computer by issuing these commands for the operating system you are using. (If the port is not in use, no output is returned from the command.)

    On UNIX:

    ```
    netstat -an | grep "389"
    ```

    ```
    netstat -an | grep "636"
    ```

    On Windows:

    ```
    netstat -an | findstr :389
    ```

    ```
    netstat -an | findstr :636
    ```

    If the port is in use (if the command returns output identifying the port), you must free the port.

    In UNIX:

    Remove the entries for ports 389 and 636 in the `/etc/services` file and restart the services, or restart the computer.

    In Windows:

    Stop the component that is using the port.

3. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.
4. Edit the `staticport.ini` file and uncomment, and update these entries:

    ```
    Oracle Internet Directory port = 389
    Oracle Internet Directory (SSL) port = 636
    ```

5. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.

6. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.

7. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.

8. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.

9. Open a window and run the script, following the prompts in the window.

10. Return to the Oracle Universal Installer screen and click **Next**.

    The **Specify File Locations** screen appears with default locations for:

    - The product files for the installation (Source)
    - The name and path to an Oracle home (Destination)

    Note: It is a good idea to make the Oracle home directory path for OIDHOST1 the same as the path to the Oracle home location of OIDHOST2. For example, if the path to the Oracle home on OIDHOST1 is:

    `/u01/app/oracle/product/AS10gOID`

    then the path to the Oracle home on OIDHOST2 should be:

    `/u01/app/oracle/product/AS10gOID`

    ---

11. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

12. Select OracleAS Infrastructure 10*g* and click **Next**.

    The **Select Installation Type** screen appears.

13. Select **Identity Management** and click **Next**.

    The **Upgrade Existing Oracle Application Server (10.1.2) Infrastructure** screen appears.

14. Select **Install New Oracle Application Server Infrastructure 10*g* (10.1.4.0.1)** and click **Next**.

    The **Product-Specific Prerequisite Checks** screen appears.

15. Click **Next**.

    The **Confirm Pre-Installation Requirements** screen appears.

16. Ensure that the requirements are met, check the box for each, and click **Next**.

The **Select Configuration Options** screen appears.

17. Select **Oracle Internet Directory**, **OracleAS Directory Integration and Provisioning**, and **High Availability and Replication** and click **Next**.

    The **Specify Port Configuration Options** screen appears.

18. Select **Manual** and click **Next**.

    The **Specify Repository** screen appears.

19. Provide the DBA login and computer information and click **Next**.

    Note: The syntax for the hostname and port field for a RAC database is:

    ```
    infradbhost1.mycompany.com:1521^infradbhost2.mycompany.com:1521^
    ```

    A dialog opens, prompting you to synchronize the system time of the primary Oracle Internet Directory computer and the system time on the computer on which you are installing.

20. Synchronize the system time on the computers and click **OK**.

    The **Specify ODS Password** screen appears.

21. Specify the ODS password (by default, the ias_admin password) and click **Next**.

22. Specify the user name and password and click **Next**.

    The **Specify OID Login** screen appears.

    The **Specify Instance Name and ias_admin Password** screen appears.

23. Specify the instance name and password and click **Next**.

    The **Summary** screen appears.

24. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.

25. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.

26. Click **Exit**, and then confirm your choice to exit.

2.4 Configuring the Virtual Server to Use the Load Balancing Router

If you plan to use the Enterprise Deployment Architecture for mySOAcompany.com with JAZN-SSO/DAS, you must configure the Load Balancing Router to perform these functions:

- Listen on oid.mycompany.com.
- Balance the requests received on ports 389 and 636 to oidhost1.mycompany.com and oidhost2.mycompany.com on ports 389 and 636.

- Monitor the heartbeat of the Oracle Internet Directory processes on both computers. If an Oracle Internet Directory process stops on one of the computers, the Load Balancing Router must route the LDAP traffic to the surviving computer.

  Note: Some tuning of the Load Balancing Router's monitoring interval and time out values may be required to ensure system availability. If the interval or time out value is too long, the Load Balancing Router will not detect service failures in time; if it is too short, the Load Balancing Router may erroneously detect that a server is down.

  For example, suppose the Load Balancing Router maps the virtual IP address oid.mycompany.com to the two Oracle Internet Directory servers for round robin load balancing, and the monitoring scheme attempts an ldapbind at 10-second intervals.

  If the Oracle Internet Directory on APPHOST1 is down, then the Load Balancing Router directs all traffic to the Oracle Internet Directory on APPHOST2 only.

  However, there is a10-second interval during which the Load Balancing Router is unaware that the Oracle Internet Directory on APPHOST1 is down. There is also a 30-second time out period. During this period, the Load Balancing Router continues to direct traffic to both Oracle Internet Directory servers in round robin mode, and ldapbind failures will occur when it attempts connections to the Oracle Internet Directory on APPHOST1.

2.5 Testing the Oracle Internet Directory Instances

1. Ensure that you can connect to each Oracle Internet Directory instance and the Load Balancing Router, using this command:

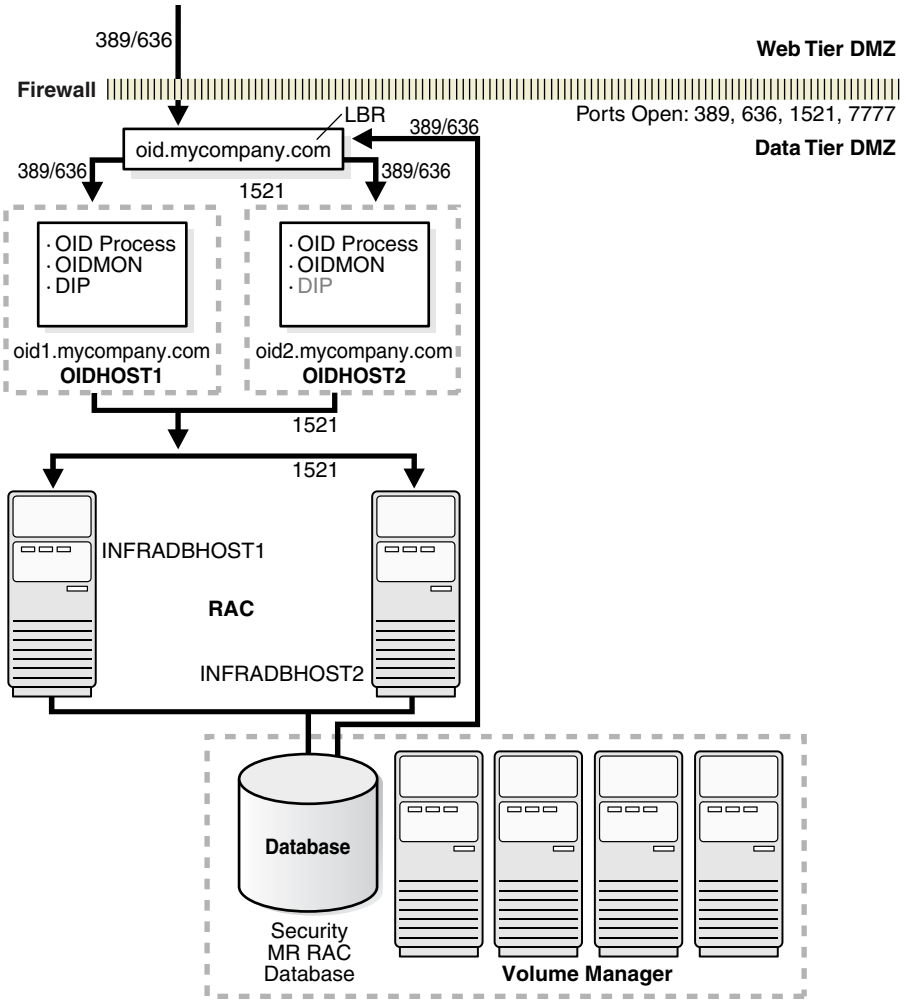
   ```
   ldapbind -p 389 -h OIDHOST1
   ldapbind -p 389 -h OIDHOST2
   ldapbind -p 389 -h oid.mycompany.com
   ```

2. Start the `oidadmin` tool on each Oracle Internet Directory instance in *ORACLE_HOME*`/bin` with this command:

   ```
   oidadmin
   ```

The Data Tier configuration is now as shown in Figure 2–1.

Figure 2–1 Data Tier Configuration



2.6 Installing the ORABPEL, ORAESB and ORAWSM Schemas

The database for the SOA Suite must be of one of the versions listed in Table 2–1:

Table 2–1 Database versions supported for SOA Suite

Database Series	Version
Oracle9i Release 2 (9.2.x)	9.2.0.7 or later
Oracle Database 10g Release 1 (10.1.x)	10.1.0.5 or later
Oracle Database Express Edition 10g Release 2 (10.2.x)	10.2.0.1
Oracle Database 10g Release 2 (10.2.x)	10.2.0.2 or later

Use these commands to determine the database version:

```
sqlplus "sys/password as sysdba"
```

```
SQL> select version from product_component_version where product
like 'Oracle%9i%' or product like 'Oracle%Database%';
```

Before you install the SOA Suite, you must install the ORABPEL, ORAESB, and ORAWSM schemas into the Oracle database (CUSTDBHOST1 and CUSTDBHOST2), according to these database requirements:

1. Navigate to the Oracle Application Server `Disk1/install/soa_schemas/irca` directory.
2. Execute the `irca.bat` or `irca.sh` script.

3

Installing and Configuring the mySOACompany Web and Application Tiers

Installing and Configuring the Web and Application Tiers

Configuring Fast Connection Failover for the RAC Database on APPHOST1 and APPHOST2

Managing Oracle Application Server Component Connections

Configuring Network Communication

Configuring Application Authentication and Authorization

3.1 Installing and Configuring the Web and Application Tiers

The Application Tier consists of multiple computers hosting middle tier Oracle Application Server instances. Each Oracle home contains multiple Oracle Containers for J2EE instances on which you deploy applications. In the complete configuration, requests are balanced among the OC4J instances on the application tier computers to create a performant and fault tolerant application environment.

The Web Tier(WEBHOST1 and WEBHOST2) consists of Oracle HTTP Servers. Figure 1–1, Figure 1–2 and Figure 1–3 show the Application and Web tiers.

3.1.1 Installing the Oracle HTTP Servers on WEBHOST1 and WEBHOST2

Use the Advanced option of the Oracle Universal Installer to install the Oracle HTTP Server instances.

1. Ensure that the system, patch, kernel and other requirements are met as specified in the *Oracle Application Server Installation Guide* for the platform you are using. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a local directory, such as TMP. You will provide the path to this file during installation.
3. Edit the `staticport.ini` file to assign the following custom ports:

```
Oracle HTTP Server port = 7777
```

> **Note:** Ensure that these ports are not already in use by any other service on the computer. Using the Static Ports feature to install the the Application Server Tier ensures that the port assignments will be consistent, if the ports are correctly specified in the file and the port is not already in use. If a port is incorrectly specified, the Oracle Universal Installer will assign the default port. If a port is already in use, the Oracle Universal Installer will select the next available port.

4. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Oracle Application Server 10.1.3.1.0 Installation** screen appears.
5. Specify an installation directory for the instance.
6. Select **Advanced Installation Mode**.
7. Click **Install**.

   The **Select Installation Type** screen appears.
8. Select **Web Server** and click **Next**.

   The **Specify Port Configuration Options** screen appears.
9. Select **Manual**, specify the location of the `staticports.ini` file, and click **Next**.

   The **Specify Instance Name** screen appears.
10. Specify the instance name and click **Next**.

    The **Cluster Topology Configuration** screen appears.
11. Check the box to configure the instance to be part of an Oracle Application Server cluster.
12. Specify the multicast address and port.

> **Note:** An example of a multicast address is `225.0.0.20`, with port `8001`. The address and port should be the same for each computer in a farm.

13. Click **Next**.

    The **Summary** Screen apears.
14. click **install**.
15. The **Configuration Assistants** screen appears. When the configuration process completes, the **End of Installation** screen appears.
16. Click **Exit**, and then confirm your choice to exit.
17. Verify that the installation was successful by viewing the Oracle HTTP Server instance. Start a browser and access:

    `http://`*`hostname`*`:7777`

Note: The *ORACLE_HOME*/install/readme.txt file contains the URLs for the installation and a command to verify the status of processes.

3.1.2 Renaming Apache 2.0 Web Server Instances

If you installed the Oracle HTTP Server based on Apache 2.0 from the Companion CD on WEBHOST1 and WEBHOST2, the instance name on both computers will be the default name assigned by the installer. In a cluster, you will want the instance names to be unique when you view the instances with the opmnctl @cluster status command. Follow these steps to rename an instance:

1. Stop the instance by issuing this command:

   opmnctl stopall

2. Modify the *ORACLE_HOME*/opmn/conf/opmn.xml file to change the instance id and name as shown:

   ```
   <ias-instance id="IAS-1
    name="IAS-1">
   ```

   Replace both occurrences of the existing instance name (IAS-1 in the example) with a unique instance name.

3. Save and close the file.

4. Restart the instance by issuing this command:

   opmnctl startall

3.1.3 Configuring the Cluster Gateway

Because there is a firewall between the instances clustered on the Web tier and the1 instances clustered on the Application tier, you must configure a cross-topology gateway to enable communication between the clusters. In the gateway configuration, one server on each side of the firewall is an entry point into the cluster. These instructions designate APPHOST1 and WEBHOST1 as the gateway servers, but any server may be designated the gateway server. The remote port is used for communication with the gateway server; it is designated in the <gateway> subelement in opmn.xml as shown in bold.

Follow these steps to specify gateway servers on the Application Tier and the Web Tier:

1. Open the *APPHOST1_ORACLE_HOME*/opmn/conf/opmn.xml file.

2. Create the <gateway> subelement as shown in the example:

```
<notification-server>
  <port local="6101" remote="6201" request="6004"/>
  <ssl enabled="true" wallet-file="$ORACLE_HOME\opmn\conf\ssl.wlt\default"/>
   <topology>
   <discover list="*225.0.0.20:8001"/>
    <gateway
list="apphost1.mycompany.com:6200&amp;apphost2.mycompany.com:6200&amp;webhost1.
mycompany.com:6200&amp;webhost2.mycompany.com:6200/"/>
   </topology>
</notification-server>
...
```

> **Note:** 6201 is the OPMN remote port onAPPHOST1, and 6202 is the OPMN remote port on WEBHOST1. You must view the `opmn.xml` file on each server to determine the port values needed for the configuration.

3. Issue this command in *`APPHOST1_ORACLE_HOME`*`/opmn/bin`:

   `opmnctl reload`

4. Copy the `<gateway>` subelement to the *`WEBHOST1_ORACLE_HOME`*`/opmn/conf/opmn.xml` file.

5. Issue this command in *`WEBHOST1_ORACLE_HOME`*`/opmn/bin`:

   `opmnctl reload`

> **Note:** For more information, see "Configuring Cross-Topology Gateways" in the *Oracle Containers for J2EE Configuration and Administration Guide*.

3.1.4 Configuring the Firewall to Prevent Access to Application Server Control Console

Application Server Control Console should be accessible from inside the firewall only. Consult the documentation for your firewall to configure it to prevent such access from outside.

3.1.5 Installing the Application Server Instances on APPHOST1 and APPHOST2

You can install an Oracle Application Server instance consisting only of one OC4J instance, using the Advanced installation option of the Oracle Universal Installer. Follow these steps to install application servers to create ORA-HOME1, ORA-HOME2, ORA-HOME3 and ORA-HOME4 on APPHOST1 and APPHOST2.

1. Ensure that the system, patch, kernel and other requirements are met as specified in the *Oracle Application Server Installation Guide*. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.

2. Start the Oracle Universal Installer using one of these commands:

   - On UNIX, issue this command: **`runInstaller`**
   - On Windows, double-click **`setup.exe`**

   The **Oracle Application Server 10.1.3.1.0 Installation** screen appears with the Basic Installation Mode and the Integrated Web Server, J2EE Web Server and Process Management installation type selected.

3. Specify an installation directory for the instance, or leave the default.

4. Select **Advanced Install** and click **Next**.

   A confirmation dialog appears.

5. Click **Yes**.

   A progress dialog appears, then the **Select Installation Type** screen appears.

6. Select **J2EE Server** and click **Next**.

   The Specify **Port Configuration Options** screen appears.

7. Select **Automatic** and click **Next**.

   The **Administration Settings** screen appears.

8. Specify an instance name for the application server instance.

   > **Note:** The instance name you specify will be prepended to the host name. For example, if you specify `J2EE` as the instance name and the host name is `server1.mycompany.com`, the instance name will be `J2EE.server1.mycompany.com`.

9. Specify and confirm the administrator password for the default OC4J instance.

10. Specify a name for the default OC4J instance created by the installer (the default is `home`), such as `Admin`, or a similar name that designates it as the instance dedicated to Application Server Control.

    > **Note:** You will not deploy applications to this instance; it will not be clustered with the user-created OC4J instances on which applications are deployed.

11. Check the box to designate the instance installed as an administration OC4J instance (the instance on which the Application Server Control Console will operate).

12. Click Next.

    The **Cluster Topology Configuration** screen appears.

13. Specify the multicast address and port.

    > **Note:** An example of a multicast address is `225.0.0.20`, with port `8001`. The address and port should be the same for each computer in a farm.

14. Select the checkbox for the option **Access this OC4J instance from a separate Oracle HTTP Server**.

15. Click **Next**.

    The **Summary** screen appears.

16. Click **Install**.

    The **Preparing to Install** dialog appears, then the **Install** screen appears.

17. The **Configuration Assistants** screen appears. When the configuration process completes, the **End of Installation** screen appears.

18. Click **Exit**, and then confirm your choice to exit.

    The first Oracle home, labeled ORA-HOME1 in the diagrams in Section 1.3, now exists on APPHOST1, with the Admin OC4J instance created.

19. Repeat steps 1 through 18 to create the second Oracle home, labeled ORA-HOME2 in the diagrams in Section 1.3, with these exceptions:

    a. In step 3, specify a different installation directory to create the second Oracle home.

b. Do not designate the default OC4J instance as the administration instance.

c. Name the default OC4J instance OC4J_ESBDT.

20. Verify that the installation was successful by viewing the instance in Oracle Enterprise Manager 10*g* (from inside the firewall only; see Section 3.1.4). Start a browser, log in to the Application Server Control Console, and view the application server instance at:

`http://WEBHOST1.mycompany.com:7777/em`

> **Note:** On Windows, you can use the Start menu to select the instance, and then select the **Oracle Application Server Control** option.

21. Verify that the installation was successful by viewing the instance in Oracle Enterprise Manager 10*g* (from inside the firewall only; see Section 3.1.4). Start a browser, log in to the Application Server Control Console, and view the application server instance at:

`http://WEBHOST2.mycompany.com:7777/em`

> **Note:** The *ORACLE_HOME*`/install/readme.txt` file contains the URLs for the installation and a command to verify the status of processes.

3.1.6 Disabling Application Server Control Console on APPHOST2-4 (Optional)

Application Server Control Console stores certain local state information that does not get replicated to another active Application Server Control Console. This includes things such as JMX Notification Subscriptions and Received Notifications. If you use JMX notifications, you may wish to disable Application Server Control Consoles other than that on APPHOST1 so that Oracle HTTP Server does not route requests to them. This will ensure that notifications subscriptions are not changed or deleted on the instance receiving requests (causing the two instances to be out of synchronization). You can disable routing to Application Server Control Consoles by setting the `ohs-routing` tag in the `default-web-site.xml` file for the Application Server Control Console to `false` as shown:

```
<web-app application="ascontrol" load-on-startup="true" name="ascontrol"
ohs-routing="false" root="/em"/>
```

You can set `ohs-routing` to `true` if you need to use the secondary Application Server Control Consoles for failover. You will need to use some backup and recovery procedure in order to restore the state of notification subscriptions and received notifications from the primary Application Server Control Consoles to the secondary.

If you have multiple Application Server Control Consoles active, be aware of the following:

- If you change the administrator password on the managed OC4J instances, you will have to make the same change to the stored administrator password on all Application Server Control Console instances. When Oracle HTTP Server directs requests to an Application Server Control Console that does not have the correct password, attempts to connect to the managed instance will fail and Application Server Control Console will prompt for the new administrator password.

On login, Application Server Control Console displays a warning on the Cluster Topology page that there are multiple instances running.

3.1.7 Listing Occupied Ports

Use the `netstat` command to identify occupied ports:

```
netstat -an
```

The AJP port range is 12501-12600. Note the port numbers in this range that do not appear in the output of the `netstat` command; these are the ports you can assign to OC4J instances.

3.1.8 Creating OC4J Instances on APPHOST1 and APPHOST2

There are three Oracle homes (application server instances) on APPHOST1 and APPHOST2. You must create the OC4J instances shown in the diagrams in Section 1.3. The single OC4J instance on APPHOST2, OC4J_ESBDT, was created during installation, so you need to create these instances:

- OC4J_SOA
- OC4J_GTWY
- OC4J_WSM

1. Log in to the Application Server Control Console with the password set during installation.

   The **Cluster Topology** page appears.

2. Click the link in the **Members** list for the application server instance on APPHOST1.

   The Application Server page for the instance appears, listing the Admin OC4J instance in the System Components list.

3. Click Create OC4J Instance.

   The **Create OC4J Instance** page appears.

4. Enter `OC4J_SOA` in the **OC4J Instance Name** field. Leave the defaults for the group and check the box to start the instance.

5. Click **Create**.

   The Processing: screen appears with a message, then the **Application Server** page appears with the new instance and a confirmation message that the instance was created and added to the group.

6. Click the OC4J_SOA instance.

   The **OC4J** page appears.

7. Click **Administration**.

   The Administration Tasks table appears.

8. Click the **Go to Task** icon for Server Properties in the Properties list.

   The **Server Properties** page appears.

9. Specify an unused AJP port (determined in Section 3.1.7) for the default-web-site and click **Apply**.

The **Processing** screen appears with a status message, then a confirmation message appears.

10. Repeat steps 1 through 9 for the OC4J_GTWY and OC4J_WM instances, assigning a different unique port from the range to each.
11. Issue these commands in *ORACLE_HOME*/opmn/bin:

    ```
    opmnctl stopall
    ```

    ```
    opmnctl startall
    ```

12. Repeat Steps 1 through 11 on APPHOST2.

3.1.9 Configuring the Oracle HTTP Server with the Load Balancing Router

The Load Balancing Router (soa.mycompany.com, shown in Figure 1–1, "mySOACompany with JSSO and Oracle Internet Directory") must be configured to receive client requests and balance them to the two Oracle HTTP Server instances on the Web tier. See the load balancing router documentation for instructions on configuring the load balancer, and follow the instructions in this section configure the Oracle HTTP Server.

Incoming requests must be associated with the Load Balancing Router hostname and port in the mySOACompany configuration. To configure this, perform these steps on WEBHOST1 and WEBHOST2:

1. Open the Oracle HTTP Server configuration file:

   Apache 1.3:

   ORACLE_HOME/Apache/Apache/conf/httpd.conf

   Apache 2.0:

   ORACLE_HOME/ohs/conf/httpd.conf

2. Perform the following steps:

   a. Add the `LoadModule certheaders_module` directive for the appropriate platform.

      UNIX Apache 1.3:

      ```
      LoadModule certheaders_module libexec/mod_certheaders.so
      ```

      UNIX Apache 2.0; use this directive if you plan to use Apache 2.0 on UNIX:

      ```
      LoadModule certheaders_module modules/mod_certheaders.so
      ```

      Windows:

      ```
      LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll
      ```

   b. Add the lines shown for the Apache version you are using to create a `NameVirtualHost` directive and a `VirtualHost` container for soa.mycompany.com and port 443.

      Apache 1.3:

      ```
      NameVirtualHost *:7777
      <VirtualHost *:7777>
        ServerName soa.mycompany.com
        Port 7777
        ServerAdmin you@your.address
      ```

```
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>

NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soa.mycompany.com:443
  Port 443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Apache 2.0 (UNIX):

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soa.mycompany.com:7777
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>

NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soa.mycompany.com:443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Notes: The `LoadModule` directives (in particular, the `LoadModule rewrite_module` directive) must appear in the `httpd.conf` file at a location preceding the `VirtualHost` directives. The server must load all modules before it can execute the directives in the `VirtualHost` container.

It is a good idea to create the `VirtualHost` directives at the end of the `httpd.conf` file.

The `LoadModule rewrite_module` directive must appear before the `LoadModule certheaders_module` directive.

---

3. Save the `httpd.conf` file.
4. Restart the components using these commands in *ORACLE_HOME*`/opmn/bin`:

   `opmnctl stopall`

   `opmnctl startall`

5. Verify that you can access these URLs:

   `http://soa.mycompany.com:7777/j2ee`

   `https://soa.mycompany.com/j2ee`

3.1.10 Configuring the esbd.myco.com URL for Internal Use

The Load Balancing Router must be configured to provide internal access to the ESBD instances on the Web tier. See the load balancing router documentation for instructions on configuring the load balancer, and follow the instructions in this section configure the Oracle HTTP Server for this URL.

Incoming requests must be associated with the Load Balancing Router hostname and port in the mySOACompany configuration. To configure this, perform these steps on WEBHOST1 and WEBHOST2:

1. Open the Oracle HTTP Server configuration file:

   Apache 1.3:

   ORACLE_HOME/Apache/Apache/conf/httpd.conf

   Apache 2.0:

   ORACLE_HOME/ohs/conf/httpd.conf

2. Perform the following steps:

   a. Add the `LoadModule certheaders_module` directive for the appropriate platform.

      UNIX Apache 1.3:

      ```
      LoadModule certheaders_module libexec/mod_certheaders.so
      ```

      UNIX Apache 2.0; use this directive if you plan to use Apache 2.0 on UNIX:

      ```
      LoadModule certheaders_module modules/mod_certheaders.so
      ```

      Windows:

      ```
      LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll
      ```

   b. Add the lines shown for the Apache version you are using to create a `NameVirtualHost` directive and a `VirtualHost` container for esb.mycompany.com.

      Apache 1.3:

      ```
      NameVirtualHost *:7777
      <VirtualHost *:7777>
        ServerName esbd.myco.com
        Port 7777
        ServerAdmin you@your.address
        RewriteEngine On
        RewriteOptions inherit
      </VirtualHost>
      ```

      Apache 2.0 (UNIX):

      ```
      NameVirtualHost *:7777
      <VirtualHost *:7777>
        ServerName esbd.myco.com:7777
        ServerAdmin you@your.address
        RewriteEngine On
        RewriteOptions inherit
      </VirtualHost>
      ```

> **Notes:** The `LoadModule` directives (in particular, the `LoadModule rewrite_module` directive) must appear in the `httpd.conf` file at a location preceding the `VirtualHost` directives. The server must load all modules before it can execute the directives in the `VirtualHost` container.
>
> It is a good idea to create the `VirtualHost` directives at the end of the `httpd.conf` file.
>
> The `LoadModule rewrite_module` directive must appear before the `LoadModule certheaders_module` directive.

3. Save the `httpd.conf` file.
4. Restart the components using these commands in *`ORACLE_HOME`*`/opmn/bin`:

   `opmnctl stopall`

   `opmnctl startall`

5. Verify that you can access these URLs:

   `http://esbd.myco.com:7777/j2ee`

   `https://esbd.myco.com/j2ee`

3.1.11 Installing the Oracle BPEL Process Manager Instances on APPHOST1 and APPHOST2 from the Oracle BPEL Process Manager (10.1.3.1.0) CD

The Oracle BPEL Process Manager instances must be installed in the `OC4J_SOA` instances on `APPHOST1` and `APPHOST2`.

> **Note:** You use the component CD-ROMs (for example, the Oracle BPEL Process Manager CD-ROM or the Oracle Enterprise Service Bus CD-ROM) to install individual components, and you install the individual components into the same Oracle home as the J2EE Server installation (performed in Section 3.1.5, "Installing the Application Server Instances on APPHOST1 and APPHOST2").

1. Ensure that the system, patch, kernel and other requirements are met as specified in the *Oracle Application Server Installation Guide* for the platform you are using. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Insert the Oracle BPEL Process Manager (10.1.3.1.0) CD.
3. Start the Oracle Universal Installer using one of these commands:
   - On UNIX, issue this command: **`runInstaller`**
   - On Windows, double-click **`setup.exe`**

     The **Welcome** screen appears.
4. Click **Next**.

   The **Specify File Locations** screen appears.

   Specify the installation directory into which you installed the J2EE Server Oracle Application Server instance.

5. Click **Next**.

   The **Select Installation Type** screen appears.

6. Select the **BPEL Process Manager for OracleAS Middle Tier** option and click **Next**.

   The **Specify Outgoing HTTP Proxy Information** screen appears.

7. Specify the host, port and bypass proxy and click **Next**.

   The **Specify Database** screen appears.

8. Specify database information:

   Database Type: `Oracle Database`

   Hostname and Port: *`INFRADBHOST1`*`.mycompany.com:1521^`*`INFRADBHOST2`*`.mycompany.com:1521`

   Service Name: `orcldb.mycompany.com`

   ORABPEL Schema Password: BPEL Process Manager Schema password

9. Click **Next**.

   The **Administration Settings** screen appears.

10. Specify administration settings:

    AS Administrator Password: The Oracle Application Server administrator password set during installation

    OC4J Instance Name: `OC4J_SOA`

    HTTP Host:Port: `soa.mycompany.com:7777`

11. Click **Next**.

    The **Summary** screen appears.

12. Click **Install**.

    The installation proceeds, and then completes.

13. Click Exit, and confirm your choice to exit.

14. Verify that the installation was performed correctly by accessing these URLs:

    `http://soa.mycompany.com:7777/BPELConsole`

    `https://soa.mycompany.com/BPELConsole`

3.1.12 Configuring the Cluster of BPEL Instances

This section briefly explains how to configure the cluster for the enterprise deployment. For more information, see the *Oracle BPEL Process Manager Installation Guide*, section titled "Creating an Oracle BPEL Process Manager Cluster".

1. Configure these server side properties on both J2EE instances (where host computers are in the same subnet):

   Set `enableCluster` to true and assign the same name to the `ClusterName` property in:

   `ORACLE_HOME``/bpel/system/config/collaxa-config.xml`

   Set `mcast-addr` and `mcast-port` to the same address in:

ORACLE_HOME/bpel/system/config/jgroup-protocol.xml (these values must be the same on all of the computers in the cluster)

2. Configure these properties on the client side of all computers in the cluster:

   In the *ORACLE_HOME*/bpel/utilities/ant-orabpel.properties file:

   Set cluster to true.

   Set oc4jinstancename to the name of the OC4J group (for example, "default_group").

3. Set the soapServerURL and the soapCallbackUrl to the same value as the load balancer URL:

   a. Open the *ORACLE_HOME*/bpel/system/config/collaxa-config.xml file.

   b. Set the soapServerUrl and soapCallbackUrl to the HTTPS URL, so that the entries resemble the following:

```
...
    <property id="soapServerUrl">
        <name>BPEL soap server URL</name>
           <value>https://soa.mycompany.com</value>
...
    </property>
...
    <property id="soapCallbackUrl">
        <name>BPEL soap callback URL</name>
           <value>https://soa.mycompany.com</value>
...
    </property>
```

4. Restart the OC4J_SOA instances on both computers.

3.1.12.1 Necessary Steps for Cluster-based BPEL Deployments

When deploying applications in a BPEL cluster, ensure that you:

- Always deploy the BPEL process and all other artifacts to each computer in the cluster. This is necessary because custom jars may be needed on each computer (for example, a local EJB).
- Execute obant.sh on each computer in the cluster.
- Start the computers one at a time, and wait until one computer is completely started before starting the next one.
- Copy the client interfaces for EJB bindings to each computer's system/classes directory and then restart the BPEL Process Manager so that the classes are loaded.
- In applications that you build and deploy, define wsdlLocation in the bpel.xml file to point to the wsdl file on the local file system and wsdlRuntimeLocation points to the wsdl file at run time. An example is provided in *ORACLE_HOME*/bpel/samples/demos/LoanFlow/LoanDemo/bpel/bpel.xml.
- Confirm that the BPEL process works after deployment using the sample application, LoanFlow, located in the *ORACLE_HOME*/bpel/samples/demos/LoanDemo directory.

3.1.13 Installing the ESB Runtime Instances on APPHOST1 and APPHOST2 from the Oracle Enterprise Bus (10.1.3.1.0) CD

The ESB Runtime instances must be installed in the `OC4J_SOA` instances on `APPHOST1` and `APPHOST2`.

> **Note:** You use the component CD-ROMs (for example, the Oracle BPEL Process Manager CD-ROM or the Oracle Enterprise Service Bus CD-ROM) to install individual components, and you install the individual components into the same Oracle home as the J2EE Server installation (performed in Section 3.1.5, "Installing the Application Server Instances on APPHOST1 and APPHOST2").

1. Ensure that the system, patch, kernel and other requirements are met as specified in the *Oracle Application Server Installation Guide* for the platform you are using. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Insert the Oracle Enterprise Bus (10.1.3.1.0) CD.
3. Start the Oracle Universal Installer using one of these commands:
   - On UNIX, issue this command: **`runInstaller`**
   - On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.
4. Click **Next**.

   The **Specify File Locations** screen appears.

   Specify the installation directory into which you installed the first J2EE Server Oracle Application Server instance (the instance in which the Admin instance resides).
5. Click **Next**.

   The **Select Installation Type** screen appears.
6. Select the **Enterprise Service Bus for OracleAS Middle Tier** option and click **Next**.

   The **Specify Outgoing HTTP Proxy Information** screen appears.
7. Specify the host, port and bypass proxy and click **Next**.

   The **Specify Database** screen appears.
8. Specify database information:

   Database Type: `Oracle Database`

   Hostname and Port:
   `INFRADBHOST1``.mycompany.com:1521^`*`INFRADBHOST2`*`.mycompany.com:1521`

   Service Name: `orcldb.mycompany.com`

   ORAESB Schema Password: ESB Schema password
9. Click **Next**.

   The **Administration Settings** screen appears.

10. Provide the administrator password set at installation time, select the OC4J_SOA instance, provide the HTTP host and port values (soa.mycompany.com:7777) and click **Next**.

    The **Select ESB Type** screen appears.

11. Select Runtime and click **Next**.

    The **Summary** screen appears.

12. Click **Install**.

    When the installation process completes, the **End of Installation** screen appears.

13. Click **Exit**, and then confirm your choice to exit.

3.1.14 Resolving Out-of-Memory Errors in the BPEL Runtime Console

When you work with tasks in the BPEL Console, this error may occur:

```
500 Internal Server Error

java.lang.OutOfMemoryError: PermGen space
```

To resolve the error, you increase the memory allocated to the PermGen space (used for loading static classes) with the `MaxPermSize` parameter. Follow these instructions to set the `MaxPermSize` parameter in the Oracle Application Server instances on APPHOST1 and APPHOST2:

1. Open the *ORACLE_HOME*`/opmn/conf/opmn.xml` file and locate the `MaxPermSize` parameter (shown in bold in Example 3–1.

Example 3–1 MaxPermSize Parameter

```
...
<category id="start-parameters">
                    <data id="java-options" value="-Xrs -server
-XX:MaxPermSize=128M -ms512M -mx1024M -XX:AppendRatio=3
 -Djava.security.policy=$ORACLE_HOME/j2ee/Admin/config/java2.policy
 -Djava.awt.headless=true -Dhttp.webdir.enable=false"/>
                  </category>
                  <category id="stop-parameters">
                     <data id="java-options"
 value="-Djava.security.policy=$ORACLE_HOME/j2ee/Admin/config/java2.policy
 -Djava.awt.headless=true -Dhttp.webdir.enable=false"/>
...
```

2. Increase the value, for example:

   `-XX:MaxPermSize=256M`

3. Save and close the file, and restart the OPMN instance.

3.1.15 Installing the ESB Repository Instance on APPHOST1 and APPHOST2

1. Perform the steps in Section 3.1.13, "Installing the ESB Runtime Instances on APPHOST1 and APPHOST2 from the Oracle Enterprise Bus (10.1.3.1.0) CD", with these exceptions:

   a. Select the applicable Oracle home (ORA-HOME2) in the Specify File Locations screen.

   b. Select the OC4J_ESBDT instance in the **Administration Settings** screen.

c. Select **Repository** in the **ESB Type** screen.

3.1.16 Configuring Service Failover for the OC4J_ESBDT Instances

The failover scheme for the OC4J_ESBDT instances dictates that only one instance is up at any given time. If the single active instance fails, OPMN will start the other instance. Follow these steps on both OC4J_ESBDT instances to configure the failover:

1. Open the *ORACLE_HOME*\opmn\conf\opmn.xml file.
2. Modify the OC4J_ESBDT process as shown:

```
<process-type id="OC4J_ESBDT" module-id="OC4J" service-failover="1"
status="enabled">
```

3. Remove the numprocs entry:

```
<process-set id="default_group" numprocs="1"/>
```

4. Restart the instance by issuing these commands in *ORACLE_HOME*\opmn\bin:

```
opmnctl reload

opmnctl restartproc process-type=OC4J_ESBDT
```

3.1.17 Configuring ESB for Singleton Adapters

In order to support a system with a singleton adapter such as an inbound file adapter or FTP adapter, you need an additional ESB runtime instance (one that is not a member of the cluster of ESB instances) to host the file adapter. Follow the instructions in Section 3.1.13, "Installing the ESB Runtime Instances on APPHOST1 and APPHOST2 from the Oracle Enterprise Bus (10.1.3.1.0) CD" to install the additional ESB runtime instance.

An inbound file adapter is only supported on a single ESB runtime server. If you are using an inbound FileAdapter, the name for the cluster of ESB instances (the cluster_name property in the *ORACLE_HOME*/integration/esb/config/esb_config.ini file) must be set to the ESB file adapter system on only one ESB runtime server.

3.1.18 Configuring the Cluster of ESB Runtime Instances on APPHOST1 and APPHOST2

> **Note:** The cluster of ESB Instances must include instances of the Runtime Server type only. The cluster must not include instances of the Repository Server type.

1. In the ESB Runtime instance installation, open the *ORACLE_HOME*/integration/esb/config/esb_config.ini file.
2. Comment out the primary_oc4j parameter:

```
# Central OC4J or not
# primary_oc4j=true
```

3. Restart the server using these opmn commands:

```
opmnctl stopall
```

```
opmnctl startall
```

3.1.19 Updating the ESB Metadata

1. Navigate to the *ORACLE_HOME*/integration/esb/bin directory and issue this command:

   Windows: **esbsetenv.bat**

   UNIX: **esbsetenv.sh**

2. Create a file called esbparam.properties with the key=value pairs shown in Example 3–2.

Example 3–2 esbparam.properties file

```
DT_OC4J_HTTP_PORT=7777
DT_OC4J_HOST=soa.mycompany.com
PROP_NAME_DEFERRED_TOPIC_JNDI=ESBTopics/Topics/ESB_JAVA_DEFERRED
PROP_NAME_DEFERRED_TCF_JNDI=OracleOJMS/TCF
PROP_NAME_DEFERRED_XATCF_JNDI=OracleOJMS/XATCF
PROP_NAME_CONTROL_TOPIC_JNDI=ESBTopics/Topics/ESB_CONTROL
PROP_NAME_CONTROL_TCF_JNDI=OracleOJMS/XATCF
PROP_NAME_ERROR_TOPIC_JNDI=ESBTopics/Topics/ESB_ERROR
PROP_NAME_ERROR_TCF_JNDI=OracleOJMS/TCF
PROP_NAME_ERROR_XATCF_JNDI=OracleOJMS/XATCF
PROP_NAME_ERROR_RETRY_JNDI=ESBTopics/Topics/ESB_ERROR_RETRY
PROP_NAME_ERROR_RETRY_TCF_JNDI=OracleOJMS/XATCF
PROP_NAME_MONITOR_TOPIC_JNDI=ESBTopics/Topics/ESB_MONITOR
PROP_NAME_MONITOR_TCF_JNDI=OracleOJMS/TCF
PROP_NAME_INITIAL_CONTEXT_FACTORY=com.evermind.server.rmi.RMIInitialContextFactory
ACT_ID_RANGE=400
```

3. Issue this command to populate the esb.parameter table:

   ant import-params -Dparamfile=esbparam.properties

Example 3–3 import command

```
ant import-params -Dparamfile=esbparam.properties -DDB_
URL=jdbc:oracle:thin:@//localhost:1521/ORCL -DDB_USER=oraesb -DDB_PASSWORD=oraesb
```

Example 3–4 export command

```
ant export-params -DDB_URL=jdbc:oracle:thin:@//localhost:1521/ORCL -DDB_
USER=oraesb -DDB_PASSWORD=oraesb
```

4. On the ESB Console System screen, for each installation, update the topic and topic connection factory for asynchronous topics with these values:

   Topic: ESBTopics/Topics/ESB_JAVA_DEFERRED

   Topic Connection Factory: OracleOJMS/XATCF

3.1.20 Configuring the Slide Repository to use the Database as the Repository

1. Navigate to the *ORACLE_HOME*/integration/esb/config directory.
2. Make a copy of the Domain_DB.xml file, naming the copy Domain.xml.
3. Restart the server.

3.1.21 Configuring JNDIs for the Topic and Topic Connection Factory

Using Oracle Enterprise Manager 10*g*, follow these steps to configure JNDIs in the Design Time and both ESB repository instances.

1. In the Administration tab, click Expand All, Services, Enterprise Messaging Service, then Database Persistence.

   The **Database Persistence** configuration page appears.

2. On the Database Persistence configuration page, click **Deploy**.
3. In Oracle Enterprise Manager 10*g*, navigate to the OC4J Admin instance's Administration tab.
4. Click **Expand All**.
5. Navigate to **Administration Tasks**, **Services**, **Enterprise Messaging Service**, **Database Persistence**.
6. Click **Deploy**.

   The **Deploy Database Persistence Provider** screen appears.

7. Make the following entries and selections:

   Resource Adapter Module Name: `OracleOJMS`

   Select **Add a new resource provider to be used by this connector**

   Resource Provider Name: `esbRP`

   Datasource JNDI Location: `jdbc/esbaqdatasource`

8. Click **OK**.

   A confirmation page appears.

9. Click **Restart** and confirm your choice to restart when prompted. If errors occur, use the `opmnctl shutdown` and `opmnctl startall` command to restart the `default` application.

   A confirmation message appears.

10. On the **Resource Adapter** page for the OracleOJMS RA, in the **Connection Factories** tab, click **Create** to create a connection factory.

    The **Create Connection Factory: Select Interface** screen appears.

11. Select `javax.jms.XATopicConnectionFactory` from the **Connection Factory Interface** drop-down list and click **Continue**.

    The **Create Connection Factory** screen appears.

12. In the JNDI Location field, enter `OracleOJMS/XATCF`. Click **Finish**.

    A confirmation message appears.

13. Create another connection factory by repeating steps 10-12, but substitute these values:

    Select `javax.jms.TopicConnectionFactory` from the **Connection Factory Interface** drop-down list.

    In the **JNDI Location** field, enter `OracleOJMS/TCF` and click **Finish**.

14. Click the **Administered Objects** tab and click **Create**.

    The **Create Administered Object** screen appears.

15. Select `oracle.j2ee.ra.jms.generic.AdminObjectTopicImpl` from the **Object Class** drop-down list and click **Continue**.
16. In the **JNDI Location** field, enter `ESBTopics`. Click **Finish**. In the **JNDI Location** field, enter `ESBTopics`. In the **resourceProviderName** field, enter `esbRP`.
17. Click **Finish**.

    A confirmation message appears.

3.1.22 Installing the OWSM Instances on APPHOST1 and APPHOST2 from the Oracle Web Services Manager (10.1.3.1.0) CD

The OWSM instances must be installed in these OC4J instances as follows:

APPHOST1, Oracle home 1: OC4J_WSM

APPHOST2, Oracle home 4: OC4J_GTWY

APPHOST2, Oracle home 1: OC4J_WSM

APPHOST2, Oracle home 4: OC4J_GTWY

> **Note:** You use the component CD-ROMs (for example, the Oracle BPEL Process Manager CD-ROM or the Oracle Enterprise Service Bus CD-ROM) to install individual components, and you install the individual components into the same Oracle home as the J2EE Server installation (performed in Section 3.1.5, "Installing the Application Server Instances on APPHOST1 and APPHOST2").

1. Ensure that the system, patch, kernel and other requirements are met as specified in the *Oracle Application Server Installation Guide* for the platform you are using. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Insert the Oracle Web Services Manager (10.1.3.1.0) CD.
3. Start the Oracle Universal Installer using one of these commands:
   - On UNIX, issue this command: **`runInstaller`**
   - On Windows, double-click **`setup.exe`**

   The Oracle Web Services Manager 10*g* (10.1.3.1.0) Installation screen appears.
4. Specify the installation directory into which you installed J2EE Server Oracle Application Server instance.
5. Specify the **Application Server Details**:

   HTTP host:port: `soa.mycompany.com:7777`

   OC4J Instance: OC4J_WSM or OC4J_GTWY (each in its own Oracle home on APPHOST1 and APPHOST2)

   Administrator Username: `oc4jadmin`

   Administrator Password: The password set during installation
6. Specify the Database Details:

   Database Type: Oracle (default)

   Driver Type: Thin (default)

Name: Service name of the SOA database

Database Connect String: hostname and port of the SOA database listener, in the format *host*:*port*

User ID: `ORAWSM`

Password: Oracle Web Services Manager schema password

7. Click **Next**.

   The **Summary** screen appears.

8. Click **Install**.

   The **Install**, the **Oracle WSM Configuration Assistant**, and then the **End of Installation** screens appear.

9. Click **Exit**, and then confirm your choice to exit.

3.1.23 Disabling Applications on APPHOST1 and APPHOST2

1. Navigate to the *ORACLE_HOME*`/j2ee/OC4J_GTWY/config` directory.
2. Open the `default-web-site.xml` file.
3. Remove the `load-on-startup` parameter.
4. Navigate to the *ORACLE_HOME*`/j2ee/OC4J_WSM/config` directory.
5. Open the `default-web-site.xml` file.
6. Remove the `load-on-startup` parameter.
7. Issue these commands in *ORACLE_HOME_1*`/opmn/bin`:

   ```
   opmnctl stopall
   opmnctl startall
   ```

8. Issue these commands in *ORACLE_HOME_4*`/opmn/bin`:

   ```
   opmnctl stopall
   opmnctl startall
   ```

Table 3–1 OC4J Applications disabled

Disable this application...	on these OC4J instances
`ccore`	Both OC4J_GTWY instances
`coreman`	Both OC4J_GTWY instances and one of the OC4J_WSM instances
`policymanager`	Both OC4J_GTWY instances
`gateway`	Both OC4J_WSM instances

3.1.24 Configuring the OWSM Cluster

1. Connect each gateway host to the OWSM policy manager:

   a. Edit the *ORACLE_HOME*`/owsm/config/gateway/gateway-config-installer.properties` file to set the `gateway.policymanagerURL` property to the Policy Manager's URL, for example: http://soa.mycompany.com/policymanager

b. Redploy the application by issuing this command in *ORACLE_HOME*/owsm/bin:

Windows: **wsmadmin.bat deploy *password* gateway**

Linux: **wsmadmin.sh deploy *password* gateway**

In the preceding command, *password* is the OC4J_GTWY administrator password set when you created the OC4J_GTWY instance.

2. Access the OWSM console (user name admin, password oracle) at:

http://soa.mycompany.com/ccore

Note: The passwordgiven in the step is the default password. You should change this password to ensure security.

3. Click **Add New Component** to add a new gateway.
4. Use these values to register the clustered gateways:

Component Name: Gateway_Cluster

Component Type: gateway

Container Type: Oracle Web Services Manager

Component URL: http://soa.mycompany.com/gateway

Leave the defaults for all other values.

5. Connect the single logical gateway to the OWSM monitor:
   a. Start the Oracle WSM Control application by accessing http://soa.mycompany.com/ccore

      The Enforcement Points page appears.

   b. Locate the Gateway to configure and click its Edit icon.
   c. Set the cfluent.monitor.rmi.host property to the Monitor's host name, for example, *APPHOST1*.mycompany.com. (Assume coreman is up on apphost1, down on apphost2.)
   d. Set the cfluent.monitor.rmi.port property to the Monitor's RMI port, for example, 3118. (The port number is the value of dataload.monitor.rmi.port in the *ORACLE_HOME*/owsm/bin/coresv.properties file.)
6. Click **Save**.
7. Connect the Oracle WSM Control to the Oracle WSM Monitor by performing these steps on each OC4J_WSM instance:
   a. Open the *ORACLE_HOME*/owsm/config/ccore/ui-config-installer.properties file.
   b. Set the ui.om.server.rmiHost property to the Monitor's host name.
   c. Set the ui.om.server.rmiPort property to the Monitor's RMI port.
   d. Save and close the ui-config-installer.properties file.
   e. Redploy the application using one of these commands:

      (Windows) **wsmadmin.bat deploy *password* control**

(Linux) **`wsmadmin.sh deploy`** ***`password`*** **`control`**

In the preceding commands, *password* is the OC4J administrator password.

3.1.25 Configuring the Firewall for the Application Tier

After you have installed all of the components on the Application Tier, you will be able to identify the port numbers that need to be opened on the firewall. This depends on the number of application server instances and types of components installed. In general, the process of configuring the firewall involves these steps:

1. For each installed instance, determine the component types and their designated port ranges (for example, the OC4J home instance and any instances you create) by examining the `opmn.xml` file. Example 3–5 shows components and default ports in the `opmn.xml` file. In the example, the OC4J `Admin` instance is listening on port 8888. Another instance, `Apps`, occupies port 12501.
2. Determine the ports in use with the `netstat` command:

   `netstat -an`

3. Configure the firewall to open only the ports in use.

Example 3–5 Oracle Application Server components and port ranges in opmn.xml

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<opmn xmlns="http://www.mycompany.com/ias-instance">
   <log path="$ORACLE_HOME/opmn/logs/opmn.log" comp="internal;ons;pm"
rotation-size="1500000"/>
   <debug path="$ORACLE_HOME/opmn/logs/opmn.dbg" comp="" rotation-size="1500000"/>
   <notification-server interface="ipv4">
      <port local="6104" remote="6204" request="6007"/>
      <ssl enabled="true" wallet-file="$ORACLE_HOME/opmn/conf/ssl.wlt/default"/>
   </notification-server>
   <process-manager>
      <process-modules>
...
      </process-modules>
      <ias-instance id="ohcoreidoid.stana17.mycompany.com"
 name="ohcoreidoid.stana17.mycompany.com">
...
            <process-type id="IASPT" module-id="IASPT"
 working-dir="/scratch/aime6/coreidoid/oh/iaspt/bin">
               <port id="ajp" range="7501-7600"/>
               <process-set id="IASPT" numprocs="1"/>
            </process-type>
         </ias-component>
         <ias-component id="ASG" status="enabled" id-matching="true">
...
               </module-data>
               <start timeout="600" retry="2"/>
               <stop timeout="120"/>
               <restart timeout="720" retry="2"/>
               <port id="default-web-site" range="8895" protocol="ajp"/>
               <port id="rmi" range="12401-12500"/>
               <port id="rmis" range="12701-12800"/>
               <port id="jms" range="12601-12700"/>
               <process-set id="default_group" numprocs="1"/>
            </process-type>
            <process-type id="admin" module-id="OC4J" status="enabled">
               <module-data>
```

```
...
               <port id="default-web-site" range="12501-12600" protocol="ajp"/>
               <port id="rmi" range="12401-12500"/>
               <port id="rmis" range="12701-12800"/>
               <port id="jms" range="12601-12700"/>
               <process-set id="default_group" numprocs="1"/>
            </process-type>
         </ias-component>
         <ias-component id="soa_group" status="enabled">
            <process-type id="oc4j_soa" module-id="OC4J" status="enabled">
...
               <start timeout="600" retry="2"/>
               <stop timeout="120"/>
               <restart timeout="720" retry="2"/>
               <port id="default-web-site" range="12501-12600" protocol="ajp"/>
               <port id="rmi" range="12401-12500"/>
               <port id="rmis" range="12701-12800"/>
               <port id="jms" range="12601-12700"/>
               <process-set id="default_group" numprocs="1"/>
            </process-type>
         </ias-component>
      </ias-instance>
   </process-manager>
</opmn>
```

Note that the AJP ports used by applications fall within the range 12501-12600. Ensure that all of the AJP ports used by OC4J applications are open on the firewall between the Web server and the application. If a port is not open, the following error occurs when access to the application from the Web tier is attempted (that is, when the URL ***web host:port/application*** is requested):

```
mod_oc4j: request to OC4J apphost1.mycompany.com:12501 failed:
Connect failed (errno=110)
```

This error creates an entry in a log file in the `ohs/logs` directory.

3.1.26 Deploying J2EE Applications

Follow the steps in this section to deploy applications. You can perform this step before or after configuring clusters.

Deploying Applications with the Oracle Enterprise Manager 10*g* Application Server Control Console

You can use Application Server Control Console to deploy applications. Follow these steps:

1. Access the Application Server Control Console at:

   `http://soa.mycompany.com:7777/em`

   The **Login** page appears.

2. Provide the password that was set during installation and click **Login**.

   The **OC4J:home** page appears.

3. Click the **Cluster Topology** link.

   The **Cluster Topology** page appears.

4. Identify in the **Members** list the OC4J instance in which you will deploy applications. Ensure that a green upward arrow appears in its Status column, indicating that it is running.

   Note: You can deploy an application into multiple instances that belong to the same group. Instances in a group have the same name and password. For instructions on creating a group, see the *Oracle Application Server Administrator's Guide*, section titled "Using Application Server Control to Create and Manage Groups".

   If a group exists, you can scroll down to the Groups section to see the list of instances in the group. To deploy to the group, click the Group name and continue with Step 8.

5. If necessary, start the OC4J instance by clicking the **Select** checkbox at the beginning of the row and then clicking the **Start** button preceding the **Members** list.

   The **Processing: Starting** screen appears with this message:

   `The selected topology members are being started.`

   The Cluster Topology screen appears with a message that the topology member was started.

6. Click the link for the OC4J instance for application deployment.

   The OC4J screen for the instance appears.

7. Click the **Applications** link.

   The Applications page for the instance appears.

8. Click **Deploy**.

   The Deploy: Select Archive screen appears.

9. Provide the location of the archive and click **Next**.

   The Deploy: Application Attributes screen appears.

   Provide the application name and click **Next**.

   The Deploy: Deployment Settings screen appears.

10. (Optional) Perform deployment tasks or deployment plan editing, or save the current settings as a deployment plan.

11. Click **Deploy**.

    The Processing: Deploy screen appears with progress messages.

Deploying Applications on the Command Line

To deploy applications into OC4J instances using the command line, follow these steps:

1. Issue this command in *APPHOST1_ORACLE_HOME*`\jdk\bin\java` (the parameters are shown on separate lines for readability only):

   `java -jar admin_client.jar` ***`uri admin ID admin password`***

   `-deploy -file` ***`full path`*** **`-deploymentName`** ***`app name`***

   `[-bindAllWebApps [`* ***`Web site name`*** **`]]`**

```
[-targetPath full path] [-parent app name]
[-deploymentDirectory full path]

[-iiopClientJar full path]
```

> **Note:** Ideally, you should include the `-bindAllWebApps` subswitch to bind all Web modules within the EAR to the Web site through which they will be accessed. If no Web site is specified, modules will be bound to the default Web site.

The EAR file is deployed to the *ORACLE_HOME*/j2ee/instance name/applications/ directory by default. The deployed EAR file is also copied to this directory. Each successive deployment causes this EAR file to be overwritten.

3.1.27 Configuring Static Discovery to Eliminate Multicast Traffic

If multicast traffic is a problem, you can configure the Web and Application Tier cluster for static discovery by modifying the *ORACLE_HOME*\opmn\conf\opmn.xml file after installation.

1. Locate the multicast entry:

```
<topology>
  <discover list="*225.0.0.1:8001"/>
</topology>
```

2. Replace the entry with a nodes list to specify static discovery instead:

```
<topology>
  <nodes
list="apphost1:6200,apphost1:6200,apphost2:6200,apphost2:6200,webhost1:6200,web
host1:6200"/>
</topology>
```

3. Issue this command in *ORACLE_HOME*\opmn\bin:

```
opmnctl reload
```

4. Verify that all nodes are present in the cluster by issuing this command in *ORACLE_HOME*\opmn\bin:

```
opmnctl @cluster status
```

> **Note:** When APPHOST1 and APPHOST2 and WEBHOST1 and WEBHOST2 are in different subnets, you also need a gateway entry (shown in bold in the example). The gateway list can consist of only one host and port from each subnet. However, for failover, you need to include multiple hosts from each subnet.

```
<notification-server>
  ...
   <gateway
list="apphost1.mycompany.com:6200&amp;apphost2.mycompany.com:6200&a
mp;webhost1.mycompany.com:6200&amp;webhost2.mycompany.com:6200/"/>
   </topology>
</notification-server>
```

Note: Oracle Notification Service (ONS) and BPEL must use different multicast addresses, if multicast is used for instance discovery.

3.2 Configuring Fast Connection Failover for the RAC Database on APPHOST1 and APPHOST2

Fast Connection Failover provides failover for a JDBC connection to a 10*g* R1 or 10*g* R2 RAC database. Upon failure of a RAC node, Oracle Notification Service (ONS) detects the failure and an SQL exception is thrown to application code. To enable Fast Connection Failover on APPHOST1 and APPHOST2:

1. Open the *ORACLE_HOME*/opmn/conf/opmn.xml file.
2. Add the RAC database hostname and remote port identifiers:

```
<notification-server>
  <port local="6100" remote="6200" request="6003"/>
  <ssl enabled="false" wallet-file="$ORACLE_HOME\opmn\conf\ssl.wlt\default"/>
  <topology>
  <nodeslist="apphost1:6200,apphost2:6200,webhost1:6200,webhost2:6200,infradbho
st1:6200,infradbhost2:6200"/>
  </topology>
</notification-server>
```

3. Save and close the file.
4. Open the *ORACLE_HOME*/j2ee/OC4J_SOA/config/data-sources.xml file.
5. Add the RAC node information and enable Fast Connection Failover:

```
<managed-data-source
 jndi-name="jdbc/TestDemoDS"
 description="Managed DataSource for TestDemoDS"
 connection-pool-name="TestDemoDS Connection Pool"
 name="TestDemoDS"/>
<connection-pool
 name="TestDemoDS Connection Pool"
 min-connections="10"
 max-connections="30"
 inactivity-timeout="30">
 <connection-factory
   factory-class="oracle.jdbc.pool.OracleDataSource"
   user="system"
   password="welcome1"
   url="jdbc:oracle:oci:@(DESCRIPTION=(LOAD_BALANCE=off)
     (ADDRESS=(PROTOCOL=TCP)(HOST=infradbhost1.mycompany.com)(PORT=1521))
     (ADDRESS=(PROTOCOL=TCP)(HOST=infradbhost2.mycompany.com)(PORT=1521))
     (CONNECT_DATA=(SERVICE_NAME=loon)))"/>
   <property name="loginTimeout" value="30"/>
   <property name="connectionCachingEnabled" value="true"/>
   <property name="fastConnectionFailoverEnabled" value="true"/>
 </connection-factory>
</connection-pool>
```

6. Save and close the file.
7. Issue this command in *ORACLE_HOME*/opmn/bin:

```
opmnctl reload
```

Note: Additional configuration is required on the data tier (see Section 2.2, "Configuring Fast Connection Failover for the RAC Database on INFRADBHOST1 and INFRADBHOST2").

3.3 Managing Oracle Application Server Component Connections

In order to ensure consistent availability of all services, ensure that the connection time out values for all Oracle Application Server components are set to a lower time out value than that on the firewall and Load Balancing Router. If the firewall or Load Balancing Router drops a connection without sending a TCP close notification message, then Oracle Application Server components will continue to try to use the connection when it is no longer available.

3.4 Configuring Network Communication

After the installation and configuration is complete, configure the network communication as described in this section. Table 3–2 lists the ports open on each firewall.

Configure the Load Balancing Router to:

- Receive requests on http://soa.mycompany.com, port 443
- Balance requests with SSL acceleration to WEBHOST1, WEBHOST2 on port 7777

Configure the firewall for communication into DMZ1:

- http://WEBHOST1:7777
- http://WEBHOST2:7777
- ONS remote port 6200 on WEBHOST1 and WEBHOST2

Configure the firewall for communication into and out of DMZ2:

- http://APPHOST1 (J2EE with SOA components) AJP ports 12501-12510
- http://APPHOST2 (J2EE with SOA components) AJP ports 12501-12510
- ONS remote port 6200 on APPHOST1 and APPHOST2

Configure the firewall for communication into DMZ3:

- INFRADBHOST1 INFRADBHOST2 database with listener on port 1521

Table 3–2 Open ports between firewall zones

Firewall Zones	Ports	Purpose
DMZ1 to DMZ2	12510-12510	WEBHOST1 and WEBHOST2, to access APPHOST1 and APPHOST2 AJP ports
DMZ1 to DMZ2	6200, 6201	OPMN cluster gateway
DMZ2 to DMZ1	7777	APPHOST1 and APPHOST2 loopback access to mysoacompany.com:7777
DMZ2 to DMZ3	1521	Database access

Table 3–2 (Cont.) Open ports between firewall zones

Firewall Zones	Ports	Purpose
DMZ2 to DMZ3	389, 636	Oracle Internet Directory server access
DMZ2 to DMZ3	6200	ONS remote port for Fast Connection Failover for RAC database
DMZ3 to DMZ2	6200	ONS remote port for Fast Connection Failover for RAC database

3.5 Configuring Application Authentication and Authorization

The tasks you have to perform depend on the authentication method you will use for mySOACompany. If you want user login sessions to persist after a failover event, you will need to use single sign-on.

mySOACompany with JSSO and Oracle Internet Directory

Perform these tasks:

1. Section 3.5.1, "Configuring the Cluster of BPEL Instances on APPHOST1 and APPHOST2 to use Oracle Internet Directory"
2. Section 3.5.2, "Configuring Java SSO"

mySOACompany with Oracle Access Manager

Perform these tasks:

1. Section 3.5.1, "Configuring the Cluster of BPEL Instances on APPHOST1 and APPHOST2 to use Oracle Internet Directory"
2. Chapter 4, "Installing and Configuring Oracle Access Manager"

mySOACompany with Oracle Single Sign-On

Perform these tasks:

1. "Steps to Use the Oracle Identity Management Security Provider" and "Settings for Authentication Method with Oracle Identity Management" in the *Oracle Containers for J2EE Security Guide*, Chapter 8.
2. Section 3.5.1, "Configuring the Cluster of BPEL Instances on APPHOST1 and APPHOST2 to use Oracle Internet Directory"
3. Chapter 5, "Installing and Configuring Oracle Single Sign-On and Oracle Delegated Administration Services"

3.5.1 Configuring the Cluster of BPEL Instances on APPHOST1 and APPHOST2 to use Oracle Internet Directory

You will need to manually replicate certain OracleAS JAAS Provider settings from the Admin OC4J instance (created during installation) in the OC4J instances that use Oracle Internet Directory, created as described in this section.

For more information on pre- and post-installation requirements, see the *Oracle BPEL Process Manager Administrator's Guide*, Chapter 2, section titled "Configuring Identity Service 10.1.3.1.0 with 10.1.2 Oracle Internet Directory".

1. To configure Oracle Internet Directory for BPEL:

a. Navigate to *ORACLE_HOME*/bpel/system/services/install/ant-tasks:

b. Issue this command:

(Windows) **configure_oid.bat**

(Linux) **configure_oid.sh**

The syntax for Linux is:

```
sh ./configure_oid.sh oid_admin_user oid_admin_passwd oid_nonssl_port ssl_
enabled oid_realm_name seedRequiredUsers | seedRequiredUsers oc4j_admin_
user oc4j_admin_passwd oc4j_container_name
```

For example:

```
sh ./configure_oid.sh orcladmin welcome 389 false us seedRequiredUsers
oc4jadmin
welcome1 oc4j_soa
```

2. If you deployed BPEL or ESB in OC4J instances other the default (home) instance, copy the *ORACLE_HOME*/j2ee/home/config/jazn.xml file to the *ORACLE_HOME*/j2ee/*oc4j instance name*/config/jazn.xml file.

Note: The policies for an OC4J instance are specified by the provider in the <jazn> element in the jazn.xml file.

When you deploy an application that uses a different provider than the instance-level provider for the instance to which the application is deployed (<jazn> config in the orion-application.xml file differs from <jazn> config in the jazn.xml file, in that one is XML and the other is LDAP), the provider specified in the orion-application.xml file is used for identity store and authentication, while the provider specified in the jazn.xml file would be used for policies and authorization. This is not a recommended usage.

Note: The hw_services application should not be JSSO-enabled. If this application has been inadvertently SSO enabled, deploying a process using ant through the command line will say "Successfully deployed the process..." although the deployment did not actually occur.

3.5.2 Configuring Java SSO

You will need to follow these steps on both Oracle Application Server instances (APPHOST1 and APPHOST2), to configure Java SSO for these applications in the OC4J_Admin and OC4J_SOA instances:

- orabpel (for Oracle BPEL Process Manager)
- esb-dt (for Oracle Enterprise Service Bus)
- ccore (for Oracle Web Services Manager)
- ascontrol (for Application Server Control Console)

Access the Oracle Enterprise Manager 10*g* Application Server Control Console and perform these steps:

1. Click the link for the OC4J instance.

   The **OC4J:** page appears.

2. Click **Applications**.

   The applications are listed.

3. Click **Expand All**.

4. Select the `javasso` application and click **Start**.

   This warning message appears:

   ```
   Java SSO is not properly configured. This is often caused
   when you are running multiple Java SSO applications in the
   cluster that use different shared symmetric keys. Please
   configure all Java SSO applications in the cluster to use the
   same shared symmetric key. You can do this from Java SSO
   Configuration page.
   ```

5. Click **Configure Java SSO**.

   A confirmation message appears that the SSO configuration was completed and will take effect after the instances are restarted.

6. Click **Restart**.

   A confirmation message appears.

7. Click **Yes**.

   The instance is restarted. (If you are configuring the OC4J _Admin instance, the system terminates your login session and you must log back in to continue the setup.)

8. Scroll to the Administration section and click **Java SSO Configuration**.

   The Java SSO Configuration page appears.

9. Click **Participating Applications**.

   The applications are listed.

10. Click the check box for the applications to be Java SSO enabled.

11. Click **Apply**.

12. To configure SSO for OWSM:

    a. Navigate to *ORACLE_HOME*`/owsm/bin`.

    b. Edit the *ORACLE_HOME*`/owsm/bin/install.properties` file to set the `install.sso.support` property to `true`.

       Issue this command:

       (Windows) **`wsmadmin.bat deploy` *`password`* `console`**

       (Linux) **`wsmadmin.sh deploy` *`password`* `console`**

       In the preceding commands, *password* is the OC4J administrator password.

13. Reconfigure the `owsm` console application with the Oracle Internet Directory security provider as described in "Steps to Use the Oracle Identity Management

Security Provider" and "Settings for Authentication Method with Oracle Identity Management" in the *Oracle Containers for J2EE Security Guide*.

3.5.3 Disabling the Worklist Application

The worklist application is a sample application that does not support Oracle Single Sign-On or Java SSO. If you do not want any applications that do not support single sign-on to be enabled in a production environment, follow these steps to disable the worklist application:

1. Open the *ORACLE_HOME*`/j2ee/home/config/default-web-site.xml` file.
2. Modify the file to comment out or delete this line:

```
<web-app application="hw_services" name="worklistapp" load-on-startup="true"
root="/integration/worklistapp" />
```

3. Restart the server.

4

Installing and Configuring Oracle Access Manager

Understanding Oracle Access Manager Components

The mySOACompany Oracle Access Manager Authentication and Authorization Process

Preparing to Install Oracle Access Manager Components

Installing the First Identity Server on IDMHOST1

Installing WebPass on WEBHOST1

Configuring the First Identity Server

Installing the Second Identity Server on IDMHOST2

Installing WebPass on WEBHOST2

Configuring the Second Identity Server

Installing the Access System

Configuring the Access Server with the Load Balancing Router

Installing the Access Server SDK

Configuring Oracle Access Manager Single Sign-On for OC4J Applications

Configuring the Second Identity Server as a Failover Server

Configuring the Second Access Server as a Failover Server

Mitigating Identity Server Product Installation Failures on Linux

Configuring Directory Server Failover

Configuring Access Server Directory Failover for Oracle and Policy Data

Configuring Policy Manager Failover

Creating Failover LDAP Directory Server Profiles for the Identity and Access Servers

Verifying the Status of the Identity Servers

4.1 Understanding Oracle Access Manager Components

The Oracle Access Manager authentication and authorization services are provided by the components described in this section. The components are shown in Figure 1–2, "mySOACompany with JSSO and Oracle Access Manager".

> **Note:** The WebPass and AccessManager components are not available on Windows at the time of publication. Therefore, WEBHOST1, WEBHOST2 and ADMINHOST in the mySOAOracle Access Manager configuration must be servers with operating systems other than Microsoft Windows.

WebGate and WebPass on the Web tier with Oracle HTTP Server

WebGate is a web server plug-in access client that intercepts HTTP requests and forwards them to the Access Server for authentication and authorization.

WebPass is a web server plug-in that passes information between a web server and a Oracle Access Manager server. Every web server instance that communicates with a Oracle Access Manager server must be configured with WebPass. WebPass is also required on each computer hosting an Access Manager.

Oracle Access Manager, Identity Server and Access Server on the Application Tier

The Access Manager is a software component that writes policy data to Oracle Internet Directory, and updates the Access Server with policy modifications. It includes an Access System Console that enables administrators to manage policies and the system configuration.

The Oracle Access Manager Identity Server is a software component that processes all user identity, group, organization, and credentials management requests.

The Access Server is a software component that receives requests, responds to the access client, and manages the login session. The Access Server receives requests from WebGate and queries the authentication, authorization, and auditing rules in Oracle Internet Directory to:

- Determine whether and how a requested resource is protected
- Whether a user is already authenticated
- Challenge unauthenticated users for credentials
- Determine validity of credentials
- Determine whether, and under what conditions, the user is authorized for the requested resource (and communicates the authentication scheme to WebGate, authorizing the user)

The Access Server also manages the login session by helping WebGate to terminate sessions, setting user session time-outs, re-authenticating when time-outs occur, and tracking session activity.

Isolated Subnet for Administration

An isolated subnet on ADMINHOST hosts the Oracle HTTP Server, WebGate, WebPass, and the Access Manager for administrator use.

Access SDK

The Access SDK provides API libraries that protect non-HTTP resources (the AJP protocol is used for communication to OC4J instances) and implement single sign-on for the OC4J applications.

4.2 The mySOACompany Oracle Access Manager Authentication and Authorization Process

This section describes the sequence for authentication and authorization for J2EE applications using Oracle Access Manager single sign-on:

1. The user requests an application URL.
2. A login page is presented.
3. The user provides a user name and password.
4. WebGate captures the name and password and communicates with Access Server.
5. The Access Server communicates with Oracle Internet Directory.
6. The Access Server authenticates the user and returns the `ObSSOCookie` to WebGate.
7. WebGate transmits the cookie and other HTTP headers to mod_oc4j, which routes the request to the appropriate OC4J instance.

8.OC4J validates the cookie and fetches extra roles from the Access Server.

4.3 Preparing to Install Oracle Access Manager Components

Before you install the Oracle Access Manager software:

- Synchronize the clocks on WEBHOST1, WEBHOST2, IDMHOST1 and IDMHOST2 within 60 seconds. In addition, ensure that:

  WEBHOST1 and WEBHOST2 (WebGate, WebPass) are not running ahead of IDMHOST1 and IDMHOST2 (Access and Oracle Access Manager Servers).

  The clocks must be synchronized in this manner so that an incoming request is not stamped with a time that has not yet occurred on the receiving server. See `http://www.ntp.org` for information about time synchronization.
- Obtain the DNS host names of all the servers on which you will install Oracle Access Manager components.
- Define the Master Identity Administrator user account (this user has access to all Oracle Access Manager functionality).
- Have a user account with administrator privileges on all computers.
- On Windows, ensure that the user account used to install the Oracle Access Manager server and Access Server has the privilege to log on as a service. The Oracle Access Manager Administrator must have the "Log on as a service" privilege. (Select Control Panel, Administrative Tools, Local Security Policy, Local Policies, User Rights Assignments, Log on as a service.)
- Ensure that the directory server you plan to use is installed and configured. If you use Oracle Internet Directory, follow the instructions in Chapter 2, "Configuring the Data Tier".

4.4 Installing the First Identity Server on IDMHOST1

1. Log in to IDMHOST1 as an administrator.
2. Issue one of these commands to start the installation (according to platform and installation option):

   Windows console installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe
   -console
   ```

   Windows GUI installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe
   ```

   Linux console installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server
   ```

   Linux GUI installation:

   ```
   ./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server -gui
   ```

   Note: If a password error occurs with the `-gui` installation option, use the console option instead. You may safely ignore any warnings about fonts or scroll bars that occur when using the (default) GUI installation on Solaris.

   The Welcome screen appears.
3. Click **Next**.

   The license agreement appears.
4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.
5. Specify credentials as appropriate to the platform:

   Windows:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX:

   Specify the user name and group that the Oracle Access Manager server will use and click **Next**.

   You are prompted for the installation directory.
6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 4.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:
   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.
8. Click **Next**.

   A progress message appears, then you are prompted for the transport security mode.
9. Specify **Open** and click **Next**.

   You are prompted for the Identity Server configuration details.
10. Specify the server name. This name must:
    - Be unique among all server names in the Oracle Access Manager System Console
    - Be unique among all server names accessing the same Oracle Internet Directory
    - Not contain any spaces
11. Specify the host name on which the Identity Server will reside.
12. Specify the port on which the Identity server will communicate with WebPass.

    You are asked if this is the first Identity server to be installed for the directory server.
13. Select **Yes**.

    The Identity Server Configuration screen appears with these options:
    - Directory Server hosting user data is in SSL
    - Directory Server hosting Oracle data is in SSL
14. Leave the checkboxes clear (do not select an option) and click **Next**.

    You are prompted to select the directory server type from the drop-down list.
15. Select **Oracle Internet Directory** and click **Next**.
16. Select the option that indicates where data is stored.
17. Select the schema update option and click **Next**.
18. Specify the Oracle Internet Directory host name, port, bind DN and password and click **Next**.

    Note: The distinguished name you enter for the bind DN must have full permissions for the user and Oracle Access Manager branches of the directory information tree (DIT). Oracle Access Manager will access the directory server as this account.

    Documentation references and contact information appears.
19. Click **Next**.

An installation summary appears.

20. Note any details about the installation and click **Finish**.
21. Start the Identity server by doing one of the following:

    Windows:

    Select **Start**, **All Programs, Administrative Tools**, **Services** and start the Identity server service.

    Linux:

    Issue this command in *`Oracle Access Manager installation directory`*`/identity/oblix/apps/common/bin`:

    `start_ois_server`

4.5 Installing WebPass on WEBHOST1

1. Log in to the computer as an administrator.
2. Issue one of these commands to start the installation (according to platform and installation option):

    Linux console installation:

    `./Oracle_Access_Manager10_1_4_0_1_linux_OHS_WebPass`

    or

    `./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebPass`[1]

    Linux GUI installation:

    `./Oracle_Access_Manager10_1_4_linux_OHS2_WebPass -gui`

    The Welcome screen appears.
3. Click **Next**.

    The license agreement appears.
4. Read and accept the terms and click **Next**.

    You are prompted to specify your credentials.
5. Specify credentials as appropriate to the platform:

    Windows:

    Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

    UNIX:

    Specify the user name and group that the WebPass web server will use and click **Next**.

    You are prompted for the installation directory.
6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice (other than the Identity server directory), and click **Next**.

[1] OHS2 is the Oracle HTTP Server based on the Apache HTTP Server version 2.0

Note: (Linux only) If the installation stops after you specify the directory, see Section 4.16.

On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:
   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.
8. Click **Next**.

   A progress message appears, then you are prompted for the transport security mode.
9. Specify `Open` and click **Next**.

   You are prompted for WebPass configuration details.
10. Specify the WebPass name. This name must:
    - Be unique among all server names in the Oracle Access Manager System Console
    - Be unique among all server names accessing the same Oracle Internet Directory
    - Not contain any spaces
11. Specify the host name of IDMHOST1, on which the Identity server resides.
12. Specify the port number of the Identity server with which the WebPass will communicate, and click **Next**.

    A progress message appears, then you are prompted to update the WebPass web server configuration.
13. Click **Yes**, then click **Next**.
14. Specify the full path of the directory containing the `httpd.conf` file (*`ORACLE_HOME`*`/Apache/Apache/conf/httpd.conf`).
15. Click **Yes** to automatically update the web server.
16. Stop the WebPass web server instance.

17. If you are using Linux RedHat Advanced Server 3.0:

    Update the *ORACLE_HOME*/opmn/conf/opmn.xml file to set the environment variable LD_ASSUME_KERNEL for the HTTP_Server component, as shown in this example:

```
...
<ias-component id="HTTP_Server">
        <process-type id="HTTP_Server" module-id="OHS2">
          <environment>
            <variable id="LD_ASSUME_KERNEL" value="2.4.19"/>
          </environment>
          <module-data>
...
```

18. Stop the Identity server service by issuing the following command in the *Oracle Access Manager installation directory*/oblix/apps/common/bin directory:

    stop_ois_server

19. Start the Identity server service by issuing the following command in the *Oracle Access Manager installation directory*/oblix/apps/common/bin directory:

    start_ois_server

20. Start the WebPass web server instance.

21. Click **Next**.

    The Read Me file appears.

22. Review the file and click **Next**.

23. Confirm that the WebPass is installed correctly by performing the following steps:

    a. Ensure that the Identity server and the WebPass web server are running.

    b. Access the Oracle Access Manager system console at this URL:

       http://*WEBHOST1*:*port*/identity/oblix

       The Oracle Access Manager system main page appears.

4.6 Configuring the First Identity Server

After the Identity server and the WebPass instance are installed, you must specify the associations between them to make the system functional. Follow these steps to configure the first Identity server:

1. Access the Oracle Access Manager system console at this URL:

   http://*WEBHOST1*:*port*/identity/oblix

2. Click the Identity System Console link.

   The System Console setup page appears.

3. Click **Setup**.

   The Product Setup page appears.

4. Select **Directory Server Type** and click **Next**.

   The **Schema Change** page appears.

5. Click **Next**. (You do not need to do anything because the schema was updated during installation.)
6. Specify the following server details:

   In the **Host** field, specify the DNS host name of the user data directory server.

   In the **Port Number** field, specify the port of the user data directory server.

   In the **Root DN** field, specify the bind distinguished name of the user data directory server.

   In the **Root Password** field, specify the password for the bind distinguished name.

   In the **Directory Server Security Mode** field, specify **Open**.

   In the **Is Oracle data stored in this directory also?** field, specify **Yes**.
7. Click **Next**.

   A page containing fields for location of user and configuration data appears.

   Note: For detailed information on completing these fields, see "Specifying Object Class Details" on page 140 of the *Oracle Access Manager Access and Identity Installation Guide*.
8. Provide the **Searchbase** and **Configuration DN** and click **Next**.

   For example, the bind distinguished name and location and location of user and configuration data would be an entry resembling the following:
   `dc=us,dc=oracle,dc=com`
9. Provide the Person object class and click the **Auto configure objectclass** text box, and click **Next**.

   For example, the Person object class would be an entry resembling the following:
   `inetorgPerson`

   The Group object class screen appears.
10. Provide the Group object class and click the **Auto Configure objectclass** box, then click **Next**.

    For example, the Group object class would be an entry resembling the following:
    `groupOfUniqueNames`

    A message appears instructing you to restart the Oracle Access Manager system.
11. Stop the Web Pass web server instance.
12. Stop, then start the Identity server service.
13. Start the WebPass web server instance.
14. Return to the Oracle Access Manager system setup window and click **Next**.

    A screen appears summarizing the object class changes that were made automatically.
15. Click **Yes** to accept the changes.
16. Review the Group object class attributes, then click **Yes**.

    The Configure Administrators page appears.
17. Click **Select User**.

The Selector page appears.

18. Complete the fields with the search criteria for the user you want to select as an administrator and click **Go**.

    Search results matching the specified criteria appear.

19. Click **Add** next to the person you want to select as an administrator.

    The name of the person appears under the Selected column on the right.

20. Add other names as needed.

21. Click **Done**.

    The Configure Administrators page appears with the selected users listed as administrators.

22. Click **Next**.

    The Securing Data Directories page appears.

23. Verify the configuration by performing these steps:

    a. Access the Oracle Access Manager system console at this URL:

       http://*WEBHOST1*:*port*/identity/oblix

    b. Click User Manager, Group Manager, or Org. Manager and log in with the newly created administrator user's credentials.

4.7 Installing the Second Identity Server on IDMHOST2

1. Log in to IDMHOST2 as an administrator.

2. Issue one of these commands to start the installation (according to platform and installation option):

   Windows console installation:

   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe -console

   Windows GUI installation:

   Oracle_Access_Manager10_1_4_0_1_Win32_Identity_Server.exe

   Linux console installation:

   ./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server

   Linux GUI installation:

   ./Oracle_Access_Manager10_1_4_0_1_linux_Identity_Server -gui

   > **Note:** If a password error occurs with the `-gui` installation option, use the console option instead. You may safely ignore any warnings about fonts or scroll bars that occur when using the (default) GUI installation on Solaris.

   The Welcome screen appears.

3. Click **Next**.

   The license agreement appears.

4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

5. Specify credentials as appropriate to the platform:

   Windows:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX:

   Specify the user name and group that the Identity Server will use and click **Next**.

   You are prompted for the installation directory.

6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 4.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

   On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:

   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

8. Click **Next**.

   A progress message appears, then you are prompted for the transport security mode.

9. Specify **Open** and click **Next**.

   You are prompted for Identity Server configuration details.

10. Specify the Identity Server name. This name must:

    - Be unique among all server names in the System Console
    - Be unique among all server names accessing the same Oracle Internet Directory
    - Not contain any spaces

11. Specify the host name on which the Identity Server will reside.

12. Specify the port on which the Identity Server will communicate with WebPass.

    You are asked if this is the first Identity Server to be installed for the directory server.

13. Select **No** and click **Next**.

    The documentation references and contact information appear.

14. Click **Next**.

    An installation summary appears.

15. Note any details about the installation and click **Finish**.

16. Start the Identity Server by doing one of the following:

    Windows:

    Select **Start**, **All Programs, Administrative Tools**, **Services** and start the Identity Server service.

    Linux:

    Issue this command:

    ***Identity Server installation directory*/identity/oblix/apps/common/bin/start_ois_server**

4.8 Installing WebPass on WEBHOST2

Follow the steps in Section 4.5, "Installing WebPass on WEBHOST1" on page 4-6 to install WebPass on WEBHOST2, specifying the host name and port for the Identity Server on IDMHOST2. After the installation is complete, confirm that the WebPass is installed correctly by performing the following steps:

1. Ensure that the Identity Server and the WebPass web server are running.

2. Access the Identity Server system console at this URL:

   http://*WEBHOST2*:*port*/identity/oblix

   The Identity Server system main page appears.

4.9 Configuring the Second Identity Server

1. Access the Identity Server system console at this URL:

   http://*WEBHOST2*:*port*/identity/oblix

   The Identity Server System screen appears.

2. Click **Identity Server System Console**.

   A dialog appears with the message "Application is not set up."

3. Click **Setup**.

4. The **Directory Server Type containing User Data** screen appears.

5. Select **Oracle Internet Directory** from the drop-down list and click **Next**.

   The **Location of Directory Server with User Data** screen appears.

6. Complete the fields and selections as follows:

   Host - Type the OIDHOST2 host name.

   Port Number - `389`

   Root DN - `cn=orcladmin`

   Root Password - Type the root password.

   Directory Server Security Mode - `Open`

   Is the Configuration Data stored in this directory also? - `Yes`

7. Click **Next**.

   The **Location of Configuration Data and the Identity Server Searchbase** screen appears.

8. Complete the fields as follows:

   Configuration DN - `dc=us,dc=oracle,dc=com`

   Searchbase - `dc=us,dc=oracle,dc=com`

9. Click **Next**.

   The **Securing Data Directories** screen appears.

10. Click **Done**.

11. Restart the identity server and the web server.

12. Access this URL:

    `http://`*`WEBHOST2`*`:`*`port`*`/identity/oblix`

13. Click any of the links (User Manager, Group Manager, Org. Manager or Identity Server System Console) and log as the administrator user specified in Section 4.6.

14. Access this URL:

    `http://`*`WEBHOST2`*`:`*`port`*`/identity/oblix`

15. Click **Identity Server System Console**.

    A login dialog appears.

16. Provide the orcladmin user name and password and click **Login**.

    The **System Configuration** screen appears.

17. Scroll down, and then click **Identity System Console**. Click **System Configuration**, then click **WebPass**.

    The two WebPass instances are listed.

18. Click the WebPass instance for WEBHOST1.

    The **Details for WebPass** screen appears.

19. Select the WebPass that is installed on WEBHOST1 and click **List Identity Servers**.

    The Identity Servers associated with the WebPass are listed.

20. Click **Add**.

    The **Add a new Identity Server to the WebPass:** screen appears.

21. Select the identity server installed on APPHOST2, select **Primary Server** and specify 2 connections, then click **Add**.

22. Repeat Steps 18 through 21 for the WEBHOST2 WebPass instance.

4.10 Installing the Access System

The Access System consists of three components: The Policy Manager, the Access Server, and the WebGate. The Access System must also have a web server instance installed.

Policy Manager

The Policy Manager is the login interface for the Access System. Administrators use the Access Manager to define the resources to be protected, and to group resources into policy domains.

Access Server

The Access Server is a software component that provides dynamic policy evaluation services for resources and applications. The Access Server receives a request from the web server, queries the LDAP directory to authenticate users, and manages user sessions.

WebGate

The WebGate is a web server plug-in access client that intercepts HTTP requests for Web resources and forwards them to the Access Server for authentication and authorization.

The primary function of the Access System is to provide an access system console for administrators. It is installed on an isolated subnet to provide secure system administrator access to the Identity Server system.

In mySOACompany with Oracle Access Manager, these components are installed on the following servers:

- Policy Manager on ADMINHOST
- Access Server on IDMHOST1 and IDMHOST2
- WebGate on ADMINHOST and WEBHOST1 and WEBHOST2
- WebPass on ADMINHOST and WEBHOST1 and WEBHOST2

4.10.1 Installing the Web Server for the Policy Manager

A web server instance is needed to host the Policy Manager components. Follow the steps in Section 3.1.1, "Installing the Oracle HTTP Servers on WEBHOST1 and WEBHOST2" on page 3-1 to install a Web Server on ADMINHOST for use with the Policy Manager.

4.10.2 Installing WebPass for the Policy Manager

A WebPass instance must be installed on ADMINHOST, at the same directory level on which the Policy Manager will be installed. Follow the steps in Section 4.5, "Installing WebPass on WEBHOST1" on page 4-6 to install WebPass for the Policy Manager.

During the installation:

- You will be prompted to configure the WebPass against the Identity Server on IDMHOST1:6022; follow the prompts to configure the WebPass.
- Note the installation path for the WebPass, since this is the path you will specify in the Policy Manager installation.

After the installation, access the system console at **http://*ADMINHOST*:*port*/identity/oblix** and add a second Identity Server instance, IDMHOST2 on port 6022, for the WebPass.

4.10.3 Installing the Policy Manager on ADMINHOST

The Policy Manager must be installed in the same directory as the WebPass on ADMINHOST. Follow these steps to install the Policy Manager:

1. Log in to ADMINHOST as an administrator.
2. Issue one of these commands to start the installation (according to platform and installation option):

   Windows:

   Oracle_Access_Manager10_1_4_0_1_Win32_NSAPI_Policy_Manager.exe

   or

   Linux console installation:

   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_Policy_Manager

   Linux GUI installation:

   ./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_Policy_Manager -gui

   The Welcome screen appears.
3. Click **Next**.

   The license agreement appears.
4. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.
5. Specify credentials as appropriate to the platform:

   Windows: Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX: Specify the user name and group that the web server will use and click **Next**.

   You are prompted for the installation directory.
6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 4.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

   On non-Linux platforms, you are prompted to select the locale (language).
7. Do one of the following:
   - On Linux, install the GCC runtime libraries and proceed with the installation.

- On other platforms, select the default locale and any other locales and click **Next**.

The installation directory and required disk space is displayed.

8. Click **Next**.

   A progress message appears, then the Configure Directory Server for Policy Data screen appears with the **Directory Server Type** drop down list.

9. Select **Oracle Internet Directory**.

   You are prompted for the communication method for Oracle Internet Directory.

10. Select the **Open** option.

    A progress message appears, then the Configure Directory Server for Policy Data screen appears with the **Directory Server Type** drop down list.

11. Select **Oracle Internet Directory**, then click **Next**.

    You are prompted to specify whether policy data is in a separate directory server than the directory containing Oracle configuration data or user data, and if so, whether you would like the installer to automatically configure the directory server containing policy data.

12. Select **No** and click **Next**.

13. Specify the full path of the directory containing the `httpd.conf` file (*`ORACLE_HOME`*`/Apache/Apache/conf`).

14. Click **Next**.

    A message informs you that the web server configuration has been updated.

15. Stop the Policy Manager web server instance.

16. Stop and then start the Identity Server instance.

17. Start the Policy Manager web server instance.

18. Click **Next**.

    Read Me information appears.

19. Review the information and click **Next**.

    A message appears informing you that the installation was successful.

20. Click **Finish**.

4.10.4 Configuring the Policy Manager

The Policy Manager must be configured to communicate with Oracle Internet Directory. Follow these steps to configure the communication:

1. Ensure that the web server is running.

2. Access the Access System Console at the URL for the WebPass instance that connects to the Policy Manager:

   `http://`*`ADMINHOST`*`:`*`port`*`/access/oblix`

   The Access System main page appears.

3. Click the Access System Console link.

   A message informs you that the application is not yet set up.

4. Click **Setup**.

   You are prompted for the directory server type.

5. Select the user data directory server type.

6. Specify the following server details:

   In the **Machine** field, specify the DNS host name of the user data directory server.

   In the **Port Number** field, specify the port of the user data directory server.

   In the **Root DN** field, specify the bind distinguished name of the user data directory server.

   In the **Root Password** field, specify the password for the bind distinguished name.

   You are prompted for the type of directory server containing Oracle configuration data.

7. Select the configuration data directory server type and click **Next**.

   A message informs you that you can store user data and Oracle data in the same or different directories.

8. Select **Store Oracle data in the User Directory Server**.

   You are prompted for the location of policy data.

9. Select **Store Policy and Oracle data in the same directory server**.

10. Specify the following:

    Searchbase `dc=us,dc=oracle,dc=com` (the same searchbase specified during Identity Server installation)

    Configuration DN `dc=us,dc=oracle,dc=com` (the same configuration distinguished name specified during Identity Server installation)

    Policy Base `dc=us,dc=oracle,dc=com`

    You are prompted to specify the Person object class.

11. Specify the Person object class that was specified during Identity Server system configuration, and click **Next**.

    You are prompted to restart the web server.

12. Stop and then start the WebPass and Access Manager web server instance and the related Identity Server instance.

13. Click **Next**.

    You are prompted for the root directory for policy domains.

14. Accept the default root directory for policy domains, or specify a root directory, then click **Next**.

    You are prompted for information about configuring authentication schemes.

15. Select **Yes** to start the automatic configuration.

16. Select **Basic Over LDAP** and **Client Certificate** and click **Next**.

    The Define a new authentication scheme screen appears with the Basic over LDAP parameters.

17. Change the parameters, if needed, and click **Next**.

The Define a new authentication scheme screen appears with the Client Certificate parameters.

18. Change the parameters, if needed, and click **Next**.

    You are prompted to configure policies to protect NetPoint URLs.

19. Select **Yes** and click **Next**.

    Instructions for completing the Policy Manager setup appear.

20. Read the information.

21. Stop the WebPass/Access Manager web server instance.

22. Stop and then start the Identity Server service for the WebPass.

23. Restart the WebPass/Policy Manager web server instance.

24. After the Web server reastarts, click **Done**.

    The Policy Manager home page appears.

25. Confirm that the Policy Manager is installed correctly by performing the following steps:

    a. Access the Access System Console at this URL:

       http://*ADMINHOST*:*port*/access/oblix

    b. Click the Access System Console link.

    c. Log in as an administrator.

    d. Click the Access System Configuration tab.

    e. Click Authentication Management.

       A list of the authentication schemes configured appears.

4.10.5 Installing the Access Server on IDMHOST1 and IDMHOST2

Before you begin installing the Access Server:

- On Windows, ensure that the user account used to install the Access Server has the privilege to log on as a service. The Access Server Administrator must have the "Log on as a service" privilege. (Select Control Panel, Administrative Tools, Local Security Policy, Local Policies, User Rights Assignments, Log on as a service.)
- Note that the Access Server cannot be installed in the same directory as the Access Manager.

Follow these instructions to install the Access Server:

1. Create an instance for the Access Server in the Access System Console:

    a. Access the Access System Console at this URL:

       http://*ADMINHOST*:*port*/access/oblix

    b. Click the Access System Console link.

    c. Log in as an administrator.

    d. Click the Access System Configuration tab.

    e. Click Access Server Configuration.

    f. Click **Add**.

The Add Access Server page appears.

g. In the **Name** field, provide a name for the Access Server that is different from all others already specified for this directory server.

In the **Hostname** field, specify IDMHOST1.

In the **Port** field, specify the port on which the Access Server will listen.

In the **Transport Security** field, specify `Open` (the transport security mode must be the same between all Access Servers and WebGates).

h. Click **Save**.

The List All Access Servers page appears with a link to the newly created instance.

i. Click the link for the instance, print the Details page for reference, and then click **Back**.

j. Click **Logout** and close the browser window.

2. Issue one of these commands to start the installation (according to platform and installation option):

Windows console installation:

```
Oracle_Access_Manager10_1_4_0_1_Win32_Access_Server.exe
-console
```

Windows GUI installation:

```
Oracle_Access_Manager10_1_4_0_1_Win32_Access_Server.exe
```

Solaris console installation:

```
./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Access_Server
```

Solaris GUI installation:

```
./Oracle_Access_Manager10_1_4_0_1_sparc-s2_Access_Server -gui
```

Linux GUI installation:

```
./Oracle_Access_Manager10_1_4_0_1_linux_Access_Server
```

The Welcome screen appears.

3. Click **Next**.

The license agreement appears.

4. Read and accept the terms and click **Next**.

You are prompted to specify your credentials.

5. Specify credentials as appropriate to the platform:

Windows:

Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

UNIX:

Specify the user name and group that the web server will use and click **Next**.

You are prompted for the installation directory.

6. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 4.16.

   On Linux systems, you are prompted to install and provide the location of `libgcc_s.so.1` and `libstdc++.so.5` that is compatible with GCC 3.3.2.

   On non-Linux platforms, you are prompted to select the locale (language).

7. Do one of the following:
   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

8. Click **Next**.

   A progress message appears, then you are prompted for the transport security mode.

9. Specify `Open` for the transport security mode.

   You are prompted for mode in which the Directory Server containing Oracle configuration data is running.

10. Specify `Open`.

    You are prompted for directory server details.

11. Specify the following server details:

    In the **Host** field, specify the DNS host name of the Oracle configuration data directory server.

    In the **Port Number** field, specify the port of the Oracle configuration data directory server.

    In the **Root DN** field, specify the bind distinguished name of the Oracle configuration data directory server.

    In the **Root Password** field, specify the password for the bind distinguished name.

    In the **Oblix Directory** field, specify the type of directory server for the Oracle configuration data.

12. Choose `Oracle Directory` to specify the location of the policy data.

    You are prompted for the Access Server instance ID specified in the Access System Console, and the configuration DN and policy base.

13. Specify the following:

    Access Server ID the name specified when installing the Access Server (step 1.g. in Section 4.10.5, "Installing the Access Server on IDMHOST1 and IDMHOST2").

    Configuration DN `dc=us,dc=oracle,dc=com` (the same configuration distinguished name specified during Identity Server installation)

    Policy Base `dc=us,dc=oracle,dc=com`

14. Click **Next**.

Read Me information appears.

15. Review the information and click **Next**.

    A message appears informing you that the installation was successful.

16. Click **Finish**.

17. Start the Access Server by doing one of the following:

    Windows: Locate and start the Windows service for this Access Server. The service name will be the Access Server ID you specified in the Access System Console prepended with `NetPoint AAA Server`.

    Solaris: In the *`Access Server installation directory`*`/access/oblix/apps/common/bin` directory, issue this command:

    `start_access_server`

    Note: If you used a password file, you must start the Access Server locally.

18. Repeat the preceding steps on IDMHOST2, substituting the hostname where appropriate.

4.10.6 Installing the WebGate

Before you begin installing the WebGate:

- Ensure that the user account used to install the WebGate has administration privileges.
- Note that the WebGate may be installed in the same directory as the Access Manager and WebPass. Separate `_jvmWebGate` and `_uninstWebGate` subdirectories are included and WebGate information is added to the `/oracle` directory. If you install WebGate into the same directory as the Access Manager and WebPass, a prompt will appear asking you if you want to replace files. Select **No to All**.
- The WebGate may be installed at the root level or the site level. However, if you have multiple virtual sites, you still only have one instance of WebGate.
- You must install WebGate on a computer that hosts a web server. You can configure the WebGate at the computer level or the virtual web server level. However, do not install at both the computer level and the virtual server level.

Follow these instructions to install the WebGate:

1. Create an instance for the WebGate in the Access System Console:

   a. Access the Access System Console at one of these URLs (depending on where you are installing):

      `http://`*`ADMINHOST`*`:`*`port`*`/access/oblix`

   b. Click the Access System Console link.

   c. Log in as an administrator.

   d. Click the Access System Configuration tab.

   e. Click **Add New Access Gate**.

f. In the **AccessGate Name** field, provide a name for the WebGate that is different from all others already specified for this directory server.

   In the **Description** field (optional), supply additional descriptive information about the WebGate.

   In the **Hostname** field, specify WEBHOST1 or WEBHOST2 or ADMINHOST.

   (Optional) In the **Port** field, specify the port on which the web server will listen.

   In the **AccessGate Password** and **Re-type AccessGate Password** fields, provide and confirm a unique password for the instance.

   In the **Transport Security** field, specify `Open` (the transport security mode must be the same between all Access Servers and WebGates).

   In the **Preferred HTTP Host** field, specify the host on which the web server is running.

   The **Primary HTTP Cookie Domain** is used to designate a single-sign on domain between WebGates on different hosts. You may leave this field blank.

g. Click **Save**.

   Details for the WebGate instance appear, and you are prompted to associate an Access Server or Access Server cluster with the WebGate.

h. Print the page for reference, and then click **Back**.

2. Assign an Access Server to the WebGate by performing the following steps:

   a. Navigate to the Details for NetPoint AccessGate page, if necessary. (From the Access System Console, select Access System Configuration, then AccessGate Configuration, then the link for the WebGate.)

      The Details for NetPoint AccessGate page appears.

   b. Click **List Access Servers**.

      A page appears with a message that there are no primary or secondary Access Servers currently configured for this WebGate.

   c. Click **Add**.

      The Add a new Access Server page appears.

   d. Select an Access Server from the Select Server list, specify primary server, and define 2 Access Servers (connections) for the WebGate.

   e. Click **Add**.

      A page appears, showing the association of the Access Server with the WebGate.

   f. Repeat Steps c through e to add the second Access Server.

3. Issue one of these commands to start the installation (according to platform and installation option):

   Windows console installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Domino_WebGate.exe
   -console
   ```

   Windows GUI installation:

   ```
   Oracle_Access_Manager10_1_4_0_1_Win32_Domino_WebGate.exe
   ```

Linux console installation:

`./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebGate`

Linux GUI installation:

`./Oracle_Access_Manager10_1_4_0_1_linux_OHS2_WebGate -gui`

4. The Welcome screen appears.
5. Click **Next**.

   The license agreement appears.
6. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.
7. Specify credentials as appropriate to the platform:

   Windows: Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   UNIX: Specify the user name and group that the web server will use and click **Next**.

   You are prompted for the installation directory.
8. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 4.16.

   On Linux systems, this prompt appears:

```
To proceed with installation of Oracle Access Manager 7.0.4 WebGate and for
successfully  running the product, you must install additional GCC runtime
libraries, namely  libgcc_s.so.1 and libstdc++.so.5. Note that these libraries
should be  compatible with GCC 3.3.2. The libraries are available for download
from  either of the following locations - http://metalink.oracle.com (requires
login), or http://www.oracle.com/technology/products/ias/index.html. Once
these libraries are locally available, please specify the directory containing
the files and proceed with the installation.

    Location of GCC runtime libraries []:
```

   On non-Linux platforms, you are prompted to select the locale (language).
9. Do one of the following:
   - On Linux, install the GCC runtime libraries and proceed with the installation.
   - On other platforms, select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.
10. Click **Next**.

    A progress message appears, then you are prompted for the transport security mode.
11. Specify Cert for the transport security mode for the WebGate.

You are prompted for directory server details.

12. Specify the following WebGate details:

    In the **WebGate ID** field, specify the unique ID that identifies the WebGate in the Access System Console.

    In the **WebGate password** field, specify the password defined in the Access System Console. If no password was specified, leave this field blank.

    In the **Access Server ID** field, specify the Access Server associated with the WebGate.

    In the **DNS Hostname** field, specify the DNS host name of the Access Server.

    In the **Port Number** field, specify the port on which the Access Server listens for the WebGate.

    Specify the password phrase.

13. Click **Next**.

14. Click **Yes** to automatically update the web server, then click **Next**.

15. Specify the full path of the directory containing the `httpd.conf` file (*ORACLE_HOME*`/Apache/Apache/conf`).

    A message informs you that the web server configuration has been updated.

16. Stop, and then start, the web server.

17. Click **Next**.

    Read Me information appears.

18. Review the information and click **Next**.

    A message appears informing you that the installation was successful.

19. Click **Finish**.

20. Restart the computer.

21. Verify the installation by performing the following steps:

    a. Ensure that the Identity Server, WebPass, and Access Server are running.

    b. Access this URL:

       `https://`*`WEBHOST1`*`:7777/access/oblix/apps/webgate/bin/webgate.cgi?progid=1`

       The WebGate page appears as shown in Figure 4–1.

Figure 4–1 Web Gate Page

Access Server	Connection State	Created	Installation Directory	Num Of Threads	Directory Information								
					Directory	Host:Port	State	Priority	Mode	Size limit	Time limit	Login Distinguished Name	Created
idmhost1.pdx.com:6021, 1	Up	June 1 2006 11:29 pm	/home/oracleqa/edg/M7/access	200	User	oidhost1.pdx.com:389	Up	0	OPEN,REFERRAL,PRIMARY	0	0	cn=orcladmin	June 2 2006 02:55 pm

Note: If the WebGate page does not appear, the installation was not successful. In this case you must uninstall, and then reinstall, the WebGate.

4.11 Configuring the Access Server with the Load Balancing Router

If the Load Balancing Router is configured for SSL acceleration, and Oracle HTTP Server is listening on a non-SSL port, you must perform the following steps to make the Access Server function properly:

1. Access the Access System Console at this URL:

   `http://`*`ADMINHOST`*`:`*`port`*`/access/oblix`

2. Click the Access System Console link.
3. Log in as an administrator.
4. Click the Access System Configuration tab.
5. Navigate to the WebGate entries section.
6. Add the user-defined parameter `ProxySSLHeaderVar`, providing a header variable name, for example:

   Name: ProxySSLHeaderVarVal: IS_SSL

7. Modify the Load Balancing Router (reverse proxy web server) settings to insert an HTTP header string that sets the `IS_SSL` value to `ssl`. For example, in the F5 load balancer, in Advanced Proxy Settings, you add the HTTP header string `IS_SSL:ssl`.

4.12 Installing the Access Server SDK

The Access Server SDK contains Access Server API libraries that are needed to perform authentication and authorization services on the Access Server for OC4J applications, specifically to:

- Protect non-HTTP resources (the AJP protocol is used for communication to OC4J instances)
- Implement single sign-on for the OC4J applications

The Access Server SDK is not included with the Access Server installation package. The SDK is provided in a separate setup package, `Oracle_Access_Manager10_1_4_`*`platform`*`_AccessServerSDK[.ext]`.

For a comprehensive discussion of the Access SDK, see Chapter 5 of the *Oracle Identity Management Application Developer's Guide*.

4.12.1 Installing the Access SDK on APPHOST1 and APPHOST2 (Windows)

Follow these steps to install the Access SDK on the computers on which you plan to install J2EE applications:

1. Log on to the computer as an administrator.
2. Navigate to the Access Server SDK installation package directory.
3. Launch the installer by double-clicking `Oracle_Access_Manager_Win32_AccessServerSDK.exe`

The Welcome screen appears.

4. Click **Next**.
5. Click **Next**.

   The license agreement appears.
6. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.
7. Specify credentials as appropriate to the platform:

   Click **Next** to indicate that you are logged in with administrator privileges. If you are not, cancel the installation, log in with administrator privileges, and restart the installation.

   You are prompted for the installation directory.
8. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   You are prompted to select the locale (language).
9. Select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.
10. Make a note of the directory (you will be prompted to provide it later).
11. Click **Next**.
12. Respond to the successive prompts.

    A screen appears with a message that the installation was successful.

4.12.2 Installing the Access SDK on APPHOST1 and APPHOST2 (Solaris and Linux)

1. Log on to the computer as the owner of the application that the AccessGate will protect.
2. Navigate to the Access Server SDK installation package directory.
3. Launch the installer by issuing one of these commands (substituting the platform for the installation):

   Solaris GUI:

   `./Oracle_Access_Manager10_1_4_0_1_sparc-s2_AccessServerSDK`

   Solaris command line:

   `./Oracle_Access_Manager10_1_4_0_1_sparc-s2_AccessServerSDK`

   Linux:

   `./Oracle_Access_Manager10_1_4_0_1_linux_AccessServerSDK`

   The Welcome screen appears.
4. Click **Next**.

   The license agreement appears.
5. Read and accept the terms and click **Next**.

   You are prompted to specify your credentials.

6. Specify the user name and group of the owner of the application that the AccessGate will protect and click **Next**.

   You are prompted for the installation directory.

7. Leave the field unchanged to accept the default, or change the field to specify a directory of your choice, and click **Next**.

   Note: (Linux only) If the installation stops after you specify the directory, see Section 4.16.

   You are prompted to select the locale (language).

8. Select the default locale and any other locales and click **Next**.

   The installation directory and required disk space is displayed.

9. Make a note of the directory (you will be prompted to provide it later).

10. Click **Next**.

    On Linux systems, this prompt appears:

```
To proceed with installation of Oracle Access Manager 7.0.4 Access Server SDK
and for successfully  running the product, you must install additional GCC
runtime libraries, namely  libgcc_s.so.1 and libstdc++.so.5. Note that these
libraries should be  compatible with GCC 3.3.2. The libraries are available for
download from  either of the following locations - http://metalink.oracle.com
(requires login), or http://www.oracle.com/technology/products/ias/index.html.
Once these libraries are locally available, please specify the directory
containing the files and proceed with the installation.

    Location of GCC runtime libraries []:
```

11. Respond to the prompts.

    A screen appears with a message that the installation was successful.

4.12.3 Configuring the AccessGate on APPHOST1 and APPHOST2

1. Create an instance for the AccessGate in the Access System Console:

   a. Access the Access System Console at this URL:

      http://*ADMINHOST*:*port*/access/oblix

   b. Click the Access System Console link.

   c. Log in as an administrator.

   d. Click the Access System Configuration tab.

   e. Click **Add New AccessGate**.

   f. In the **AccessGate Name** field, provide a name for the AccessGate that is different from all others already specified for this directory server.

      In the **Description** field (optional), supply additional descriptive information about the AccessGate.

      In the **Hostname** field, specify IDMHOST1 or IDMHOST2 or ADMINHOST.

      (Optional) In the **Port** field, specify the port on which the web server will listen.

In the **AccessGate Password** and **Re-type AccessGate Password** fields, provide and confirm a unique password for the instance.

In the **Transport Security** field, specify `Open` (the transport security mode must be the same between all Access Servers and WebGates).

g. Click **Save**.

Details for the AccessGate instance appear, and you are prompted to associate an Access Server or Access Server cluster with the AccessGate.

h. Print the page for reference, and then click **Back**.

2. Navigate to:

   ***AccessServerSDK path*/oblix/tools/configureAccessGate**

3. Issue this command:

   ./configureAccessGate -i AccessServerSDK path **-t AccessGate**

   The following prompt appears:

   ```
   Please enter the Mode in which you want the AccessGate to
   run: 1(Open) 2(Simple) 3(Cert):
   ```

4. Enter **2**.

   The following prompt appears:

   ```
   Please enter the AccessGate ID:
   ```

5. Enter **access_gate_*APPHOST1*_sdk1**

   The following prompt appears:

   ```
   Please enter the Password for this AccessGate:
   ```

6. Enter a password.

   The following prompt appears:

   ```
   Please enter the Access Server ID:
   ```

7. Enter **access_server_*IDMHOST1***.

   The following prompt appears:

   ```
   Please enter the Access Server Host Machine Name:
   ```

8. Enter ***IDMHOST1*.mycompany.com**.

   The following prompt appears:

   ```
   Please enter the Access Server Port:
   ```

9. Enter **6021**.

   The following prompts appear:

   ```
   Preparing to connect to Access Server. Please wait.

   AccessGate installed Successfully.

   Press enter key to continue...
   ```

10. Press **Enter**.

11. Repeat the preceding steps on APPHOST2, substituting the host name where appropriate.

12. Update the `opmn.xml` file in all OC4J instances to include the AccessSDK shared library path:

```
<process-type id="app1" module-id="OC4J" status="enabled">
                <module-data>
                    <category id="start-parameters">
                       <data id="java-options" value="-server
-Djava.library.path=AccessServerSDK path/oblix/lib
-Djava.security.policy=$ORACLE_HOME/j2ee/app1/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false"/>
```

13. Restart OPMN by issuing this command in *APPHOST2_ORACLE_HOME*`/OPMN/BIN`:

```
opmnctl reload
```

14. Restart the OC4J instances in which the applications using Oracle Access Manager are deployed.

4.13 Configuring Oracle Access Manager Single Sign-On for OC4J Applications

After you have installed the Oracle Access Manager, WebGate and Access Server SDK, complete the procedures in this section to integrate SOA components with Oracle Access Manager.

4.13.1 Configuring Access to SOA Components

1. Update the `opmn.xml` file to set the `LD_ASSUME_KERNEL` environment variable to `2.4.19`, as shown in Example 4–1.

Example 4–1 opmn.xml File Updates

```
<process-type id="OC4J_SOA" module-id="OC4J" status="enabled">
               <environment>
                 <variable id="LD_ASSUME_KERNEL" value="2.4.19"/>
               </environment>
               <module-data>
                  <category id="start-parameters">
                     <data id="java-options" value="-server -XX:MaxPermSize=128M
-ms512M -mx1024M -XX:AppendRatio=3
-Djava.library.path=/product/oracle/AccessServerSDK/oblix/lib
-Djava.security.policy=$ORACLE_HOME/j2ee/home/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false
...
```

2. Copy the Access Server `/oblix/lib/jobaccess.jar` file to the *ORACLE_HOME*`/j2ee/home/lib/ext` directory. For example:

```
cp product/oracle/AccessServerSDK/oblix/lib/jobaccess.jar ORACLE_
HOME/j2ee/home/lib/ext
```

3. Restart the OC4J_SOA instance by issuing these commands:

```
opmnctl reload

opmnctl restartproc process-type=OC4J_SOA
```

4. Create the file *ORACLE_HOME*/ohs/htdocs/login/login.html. The variable names for username and password match the plug-ins defined for COREidSSOform and COREidSSONoPwd in the next step.

   Note: If you need detailed information, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Create a Login Form".

5. Create authentication schemes, resource types and action URL protection in the Access Server console, as follows:

   Create COREidSSOform, a form-based authentication scheme. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Define Form-Based Authentication in Policy Manager".

   Create COREidSSONoPwd, for authentication without password. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Define Basic Authentication in Policy Manager".

   Create myresourcetype, to be used in the login-modules section of the system-jazn-data.xml file. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Configure the Name and Operation of the Resource Type".

   Protect the action URL in the login.html file with COREidSSONoPwd. For instructions, see the *Oracle Containers for J2EE Security Guide*, Chapter 11, section titled "Protect the Action URL".

   Note: The plug-ins in COREidSSOform and COREidSSONoPwd must match the variables in the login.html file.

4.13.2 Configuring the Login Protected by Oracle Access Manager

1. Use the Access Server console and the instructions in *Oracle Access Manager Access System Administration Guide* to create policy domains to protect the URLS with COREidSSOform, for example:

   ```
   /em

   /BPELConsole

   /esb

   /ccore

   /ruleauthor
   ```

2. Visit the protected URLs created in Step 1.

   The login is not fully functional at this point; attempting to access the URLs causes a redirect to the /login/login.html page.

3. Add the entries shown in Example 4–2 to the jazn-policy section of the *ORACLE_HOME*/j2ee/OC4J_SOA/config/system-jazn-data.xml file.

   This step establishes Oracle Access Manager as the sole authentication provider for the Oracle BPEL Control and Worklist applications. Other SOA components, such as Oracle Enterprise Service Bus and Application Server Control Console, do not provide their own authentication capabilities and automatically use Oracle Access Manager.

Example 4–2 Addition to <jazn-policy> section of system-jazn-data.xml

```
<jazn-policy>
  <grant>
    <grantee>
        <principals>
           <principal>
           <class>oracle.security.jazn.realm.CoreIDPrincipal</class>
           <name>BPMSystemAdmin</name>
           </principal>
        </principals>
    </grantee>
    <permissions>
        <permission>
           <class>com.collaxa.security.ServerPermission</class>
           <name>server</name>
           <actions>all</actions>
        </permission>
    </permissions>
  </grant>
  <grant>
    <grantee>
        <principals>
           <principal>
                 <realm-name>jazn.com</realm-name>
                 <type>role</type>
                 <class>oracle.security.jazn.realm.CoreIDPrincipal</class>
                 <name>jazn.com/BPMDefaultDomainAdmin</name>
           </principal>
        </principals>
    </grantee>
    <permissions>
        <permission>
           <class>com.collaxa.security.DomainPermission</class>
           <name>default</name>
           <actions>all</actions>
        </permission>
    </permissions>
  </grant>
</jazn-policy>
```

4. Locate the `application` section in the `jazn-loginconfig` section of the *ORACLE_HOME*`/j2ee/OC4J_SOA/config/system-jazn-data.xml` file. The `application` section is shown in bold in Example 4–3.

Example 4–3 Additions to <application> section of system-jazn-data.xml

```
<!-- Login Module Data -->
<jazn-loginconfig>
...
 <application>
   <name>ccore</name>
   <login-modules>
       <login-module>
         <class>oracle.security.jazn.login.module.coreid.CoreIDLoginModule</class>
         <control-flag>required</control-flag>
             <options>
                 <option>
                     <name>coreid.password.attribute</name>
                     <value>passwordvar</value>
                 </option>
```

```
                    <option>
                        <name>coreid.name.attribute</name>
                        <value>usernamevar</value>
                    </option>
                    <option>
                        <name>addAllRoles</name>
                        <value>true</value>
                    <option>
                        <name>coreid.resource.operation</name>
                        <value>MYRESOURCEOPERATION</value>
                    </option>
                    <option>
                        <name>coreid.resource.type</name>
                        <value>myresourcetype</value>
                    </option>
                    <option>
                        <name>coreid.name.header</name>
                        <value>your http header name variable</value>
                    </option>
                    <option>
                        <name>coreid.resource.name</name>
                        <value>/myresourcetype</value>
                    </option>
                </options>
            </login-module>
        </login-modules>
    </application>
</jazn-loginconfig>
```

5. Replace the application name (`ccore` in bold text in Example 4–3) with the application name of the SOA component to authorize. For example, for Oracle BPEL Control, it is `orabpel`. For Application Server Control Console, it is `ascontrol`. For Oracle Enterprise Service Bus, it is `esb-dt`.
6. If there are additional SOA components to authorize, then create an application section for each component to authorize by copying and pasting an existing application section, and replacing the `name` value with the name of the application.
7. Add `COREIDSSO` as the authentication method to *`ORACLE_HOME`*`/j2ee/OC4J_SOA/application-deployments/ccore/orion-application.xml`. For example, replace:

   ```
   <jazn provider="XML" location"../..config/system-jazn.data.xml">
   jaas-mode="doAsPrivileged"/>
   ```

   with the following, shown in bold (note also that the slash following `doASPrivileged` must be removed):

   ```
   <jazn provider="XML" location"../..config/system-jazn.data.xml">
   jaas-mode="doAsPrivileged">
   <jazn-web-app auth-method="COREIDSSO"/>
   </jazn>
   ```

   Caution: Edit the file with care, making certain that the XML is well-formed. If it is not, restarting the application with the `opmnctl` utility can remove the `orabpel` application from the `server.xml` file. This causes the application to become undeployed.

8. Ensure that the appropriate roles and users are populated in Oracle Access Manager for use with Oracle Internet Directory.
   a. For Oracle BPEL Process Manager, follow the instructions in Section 3.5.1.
   b. For other applications, add `oc4jadmin` to the `oc4j-administrators` and `ascontrol_admin` groups in Oracle Internet Directory. For instructions on adding users to groups, see the Oracle Internet Directory documentation set. It is available in the Oracle Identity Management 10g (10.1.4.0.1) documentation library. Click **View Library, Identity and Access Management** at:

      http://www.oracle.com/technology/documentation/oim1014.html
9. Restart the OC4J instance.
10. Access a protected URL to verify that the login is working.

4.13.3 Configuring the Logout

1. Copy the `logout.html` file from the WebGate directory `access/oblix/lang/en-us/` to *ORACLE_HOME*`/ohs/htdocs`.
2. Navigate to **Access System Console, Access System Configuration, Server Settings, Configure SSO logout URL**.
3. Set the URL to `/logout.html`.
4. Restart the Oracle HTTP Server for the Policy Manager.
5. Perform one of the following steps to cause Oracle Access Manager to reread the configuration:
   - Restart the Oracle Access Manager server.
   - Clear the cache in the Identity System Console by selecting **System Configuration, Server settings, Cache**.
6. In the *ORACLE_HOME*`/j2ee/OC4J_SOA/config/jazn.xml` file, update `custom.sso.url.logout` property to:

   ```
   <property name="custom.sso.url.logout" value="/logout.html"/>
   ```
7. Restart the OC4J instance by issuing these commands:

   ```
   opmnctl reload
   ```

   ```
   opmnctl restartproc process-type=OC4J_SOA
   ```

   The logout for all components will now redirect to this logout page.

4.14 Configuring the Second Identity Server as a Failover Server

The Identity Server on IDMHOST2 must be configured to service requests routed to the Identity Server on IDMHOST1 if IDMHOST1 becomes unavailable. Before you can configure the Identity Server on IDMHOST2 as a failover server, it must:

- Communicate with the existing Oracle Internet Directory
- Be associated with the existing WebPass as a secondary server

There are two failover paths to configure:

- Identity Server and WebPass communications
- Access Server and WebGate communications

4.14.1 Configuring Failover Between the Secondary Identity Server on IDMHOST2 and the WebPass

1. Access the Identity Server system console at this URL:

   `http://ADMINHOST:port/identity/oblix`

   The Identity Server system main page appears.

2. Select System Admin, System Configuration, Configure WebPass, *WebPass name*, Modify.

3. Complete the fields as follows:

   Failover Threshold — The number of live connections from the web component to its primary NetPoint server.

   Identity Server Timeout Threshold — The number of seconds the web component waits for a non-responsive NetPoint server before it considers it unreachable and attempts to contact another.

   Sleep For (seconds) — The number of seconds after which the WebGate verifies that the number of valid connections equals the maximum number of connections configured.

4. Save the changes.

5. Click **List Identity Servers**.

6. Click **Add**.

7. Select the Identity Server from the drop-down list.

8. Set the **Priority** to **Primary Server**.

9. Set **Number of Connections** to 2 or more.

10. Click **Add**.

    Both Identity servers are listed. Ensure that the number of connections for each is 2 or more.

11. Select System Admin, System Configuration, Configure Directory Options.

    The Configure Profiles page appears with the directory server information.

12. Select the name of the Identity Server profile from under the Configure LDAP Directory Server Profiles heading.

    The Modify Directory Server Profile page appears.

13. Locate the Used by field and select All Identity Servers.

4.15 Configuring the Second Access Server as a Failover Server

The Access Server on IDMHOST2 must be configured to service requests routed to the Access Server on IDMHOST1 if IDMHOST1 becomes unavailable. Before you can configure the Access server on IDMHOST2 as a failover server, it must:

- Communicate with the existing Oracle Internet Directory
- Be associated with the existing WebPass as a secondary server

4.15.1 Configuring Failover Between the Access Server and WebGate

1. Access the Access System Console at the URL for the WebPass instance that connects to the Access Manager:

   http://*ADMINHOST*:*port*/access/oblix

   The Access system console page appears.

2. Select Access System Configuration, AccessGate Configuration, All, Go, *Name*.

   The AccessGate page appears.

3. Complete the fields as follows:

   Failover Threshold — The number of live connections from the web component to its primary NetPoint server.

   Access Server Timeout Threshold — The number of seconds the web component waits for a non-responsive NetPoint server before it considers it unreachable and attempts to contact another.

   Sleep For (seconds) — The number of seconds after which the WebGate verifies that the number of valid connections equals the maximum number of connections configured.

4. Save the changes.

5. Select System Configuration, View Server Settings.

   The View Server Settings page appears with the directory server information.

6. Select the name of the Access Server profile from under the Configure LDAP Directory Server Profiles heading.

   The Modify Directory Server Profile page appears.

7. Locate the Used by field and select All Access Servers.

8. Save the changes.

4.16 Mitigating Identity Server Product Installation Failures on Linux

At the time of publication, an unresolved defect in a third-party product, InstallShield, caused some Identity Server product installations to stop after the installation directory was specified. This occurred intermittently, and only in the Linux version.

If an installation stopped after the installation directory was specified, repeat the installation as follows:

1. Open a shell window and paste these lines into it:

```
cd /tmp
mkdir bin.$$
cd bin.$$
cat > mount <<EOF
#! /bin/sh
exec /bin/true
EOF
chmod 755 mount
export PATH=`pwd`:$PATH
```

2. Perform the installation steps for the product you want to install.
3. Issue this command to empty the temporary directory:

```
rm -r /tmp/bin.$$
```

4.17 Configuring Directory Server Failover

The instructions for configuring failover from Identity Server components to directory servers vary, depending on the component (Identity Server, Access Server, or Access Manager), and whether you are configuring failover for user data or Oracle data. Table 4–1 lists the components, data stores, and configuration methods.

Table 4–1 Supported Failover Configurations for Directory Servers

Component	Data Store	Operation	Configuration Method
Identity Server	User	Read/Write	Directory Profile See Section 4.17.1, "Configuring Directory Failover for User Data"
Identity Server	Oracle	Read/Write	Directory Profile and XML Configuration Files See Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Server	User	Read/Write[1]	Directory Profile See Section 4.17.1, "Configuring Directory Failover for User Data"
Access Server	Oracle	Read/Write[2]	`ConfigureAAAServer` command line tool Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Server	Policy	Read/Write[3]	`ConfigureAAAServer` command line tool Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Manager	User	Read	Directory Profile XML Configuration Files
Access Manager	Oracle	Read/Write[4]	Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"
Access Manager	Policy	Read/Write[5]	XML configuration files Section 4.17.2, "Configuring Directory Failover for Oracle and Policy Data"

[1] Only applicable when password policy is enabled

[2] Only applicable when the Access Management Service is On. Unless there is only one back-end RAC database, load balancing is not recommended due to cache synchronization problems.

[3] Only applicable when the Access Management Service is On. Unless there is only one back-end RAC database, load balancing is not recommended due to cache synchronization problems.

[4] Load balancing for the Access Manager Write profile is not supported unless there only one back-end RAC database, due to cache synchronization problems.

[5] Load balancing for the Access Manager Write profile is not supported unless there only one back-end RAC database, due to cache synchronization problems.

Note: Load balancing will work with Oracle Internet Directory, since the directory server instances refer to the same data. However, using load balancing with the directory server in replication mode (for example, IPlanet load balancing) is not recommended, because replication delays can occur, with resulting cache synchronization problems across access servers.

4.17.1 Configuring Directory Failover for User Data

This section explains how to configure failover of Identity Server requests to directory servers that contain user data. The failover sequence consists of the LDAP SDK detecting a failure, returning a connection or "server down" error, and directing the request to a secondary directory server.

Each installed component has a directory profile. Follow these steps to configure user data directory failover using the Identity Server System or Access System Directory Profile page:

1. Access the Directory Profile page for the server on which you are configuring failover:
   - From the Identity Server System Console, log in as the administrator, then navigate to System Configuration, Directory Profiles.
   - From the Access System Console, select System Configuration, Server Settings.
2. Under **Configure LDAP Directory Server Profiles**, select the directory profile that contains connection information for the component and data for which you want failover capability.
3. Complete the **Failover Threshold** field.

   Failover Threshold — The number of live primary directory servers required. If the number of primary directory servers drops below the failover threshold, Identity Server attempts to establish a connection to a primary server, if available, and if not, the first secondary server listed, and then the next secondary server listed, and so on.
4. Complete the **Sleep For** field with the number of seconds before the watcher thread wakes up and attempts to reestablish or create new connections when connections fail.
5. Navigate to **Database Instances**, select **Add**, and indicate the instances' status as secondary servers.

Note: To load balance requests between the two Directory Servers, specify both as primary servers here (which represents an active-active failover solution).

To configure one server as active and the other as standby (representing an active-passive solution), designate the directory server you added as the secondary server. The secondary server will not operate unless the primary server is not available.

In either case, failover is achieved; however, in this guide the active-active solution is emphasized. You may have special considerations that indicate use of an active-passive solution.

4.17.2 Configuring Directory Failover for Oracle and Policy Data

This section explains how to configure failover in the Identity Server for Oracle and Policy data.

4.17.2.1 Configuring Identity Server Failover for Oracle Data

Most of the configuration data is managed in XML configuration files. Multi-language and referential integrity data is managed on the Directory Profile page.

If there is a failure of the primary configuration data directory server, then the Identity Server cannot read any configuration entries. The `failover.xml` file provides bootstrap secondary directory server information. See Example 4–4 for an example of the `failover.xml` file.

The procedure for configuring Identity Server failover for Oracle data is:

1. Creating the failover.xml File
2. Configuring Identity Server Directory Failover for Oracle Data
3. Creating the Encrypted Password for the Bind DN

4.17.2.1.1 Creating the failover.xml File Follow these steps to create the file for each Identity Server that needs failover capability:

1. Copy and paste the existing `sample_failover.xml` file template into the *`Oracle_Access_Manager_INSTALLATION_DIRECTORY`*`/identity/oblix/config/ldap` directory.
2. Use a text editor to add failover information for secondary servers, using Example 4–4 as a guide (server information and encrypted password shown in bold).

> **Note:** Instructions for obtaining the encrypted password are provided in Section 4.17.2.1.3, "Creating the Encrypted Password for the Bind DN" on page 4-39.

3. Save the `sample_failover.xml` file as `failover.xml`.

Example 4–4 failover.xml File

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<CompoundList xmlns="http://www.oblix.com"
ListName="failover.xml">
<!-- # Max number of connections allowed to all the active ldap servers -- note
this is the same as Max Active Servers>
<SimpleList>
<NameValPair ParamName="maxConnections" Value="1">
</NameValPair>
</SimpleList>
<!-- # Number of seconds after which we switch to a secondary or
reconnect to a restarted primary ldap server -->
<SimpleList>
<NameValPair ParamName="sleepFor" Value="60">
</NameValPair>
</SimpleList>
<!-- # Max amount of time after which a connection to the ldap
server will expire -->
<SimpleList>
```

```
<NameValPair ParamName="maxSessionTime" Value="0"></
NameValPair>
</SimpleList>
<!-- # Minimun number of active primary ldap servers after which
failover to a secondary server will occur -->
<SimpleList>
NameValPair ParamName="failoverThreshold" Value="1">
</NameValPair>
</SimpleList>
<!-- # Specify the list of all secondary ldap servers here -->
<ValList xmlns="http://www.oblix.com"
ListName="secondary_server_list">
<ValListMember Value="sec_ldap_server">
</ValListMember>
</ValList>
<!-- # Specify the details of each secondary ldap server here -->
<ValNameList xmlns="http://www.oracle.com"
ListName="sec_ldap_server">
<NameValPair ParamName="ldapSecurityMode" Value="Open">
</NameValPair>
<NameValPair ParamName="ldapServerName" Value="oidhost.mycompany.com">
</NameValPair>
<NameValPair ParamName="ldapServerPort" Value="389">
</NameValPair>
<NameValPair ParamName="ldapRootDN" Value="cn=orcladmin">
</NameValPair>
<NameValPair ParamName="ldapRootPasswd"
Value="000A0259585F5C564C">
</NameValPair>
<NameValPair ParamName="ldapSizeLimit" Value="0"></
NameValPair>
<NameValPair ParamName="ldapTimeLimit" Value="0"></
NameValPair>
</ValNameList>
</CompoundList>
```

4.17.2.1.2 Configuring Identity Server Directory Failover for Oracle Data

To configure directory failover, access the Directory Profile page for the directory profile that contains the Oracle branch of the tree, as described in Section 4.17.1, "Configuring Directory Failover for User Data".

4.17.2.1.3 Creating the Encrypted Password for the Bind DN

Follow these steps to create the encrypted password:

1. Locate the `obencrypt` tool in the *`AccessServer_install_directory`*`/access/oblix/tools/ldap_tools` directory.
2. Issue this command:

   `obencrypt` ***`password`***

   In the preceding command, *password* is the password to encrypt.
3. Copy and paste the encrypted password into the `ldapRootPasswd` parameter value.

4.18 Configuring Access Server Directory Failover for Oracle and Policy Data

Perform the procedures in this section to configure directory failover for the Access Server.

4.18.1 Adding a Failover Directory Server Using the ConfigureAAAServer Tool

1. Navigate to the directory containing the configureAAAServer tool:

   AccessServer installation directory/access/oblix/tools/configureAAAServer

2. Issue this command:

   configureAAAServer reconfig *AccessServer installation directory*

   In the preceding command, *AccessServer installation directory* is the directory in which the Access Server is located.

3. Type 2 to specify the Simple security mode for the Access Servers that will connect to the directory servers.

   You are asked if you want to specify failover information for Oracle or policy data.

4. Select `Y` (Yes).

   You are prompted to specify the location of the data.

5. Type the number that corresponds to the location of the data (`1` for **Oracle tree**, `2` for **Policy tree**).

   You are prompted for the action to take.

6. Type `1` (**Add a failover server**).

7. Complete the following fields:

   Directory server name

   Directory server port

   > **Note:** For LDAP in an Active Directory forest environment, use port 3269 for SSL mode. These are the global catalog ports.

   Directory server login DN

   Directory server password

8. Select `2 (Open)` for **Security Mode** and `2 (Secondary)` for **Priority**.

9. Type `5` and press Enter to quit.

   You are prompted to commit the changes.

10. Select `1 (Y)` and press **Enter** to commit the changes.

    The `ConfigureAAAServer` tool automatically creates the following `.xml` files in the *`Access Server installation directory`*`/access/oblix/config/ldap` directory:

    - `AppDBfailover.xml`
    - `ConfigDBfailover.xml`
    - `WebResrcDBfailover.xml`

4.19 Configuring Policy Manager Failover

1. Copy the `WebResrcDBfailover.xml` file from the Access Server configuration directory to the Policy Manager install directory.
2. Copy the `AppDBfailover.xml` file from the Access Server configuration directory to the Policy Manager install directory.
3. Copy the `ConfigDBfailover.xml` file from the Access Server configuration directory to the Policy Manager install directory.

4.20 Creating Failover LDAP Directory Server Profiles for the Identity and Access Servers

Each Identity and Access Server must have a failover directory server profile for user data. A directory server profile is created for each Identity and Access Server at installation time. Each Identity and Access Server must also have a second profile that gives connection information to another directory server, so that if the default directory server is unavailable, the Identity or Access server can connect to another directory server.

4.20.1 Creating a Directory Server Profile for the Identity Servers

1. Access the Identity Server system console at this URL:

   `http://`*`ADMINHOST`*`:`*`port`*`/identity/oblix`

   The **Identity Administration** page appears.
2. Select **Identity System Console**.

   A login dialog appears.
3. Provide the user ID and password and click **Login**.

   The **System Configuration** page appears.
4. Click **System Configuration**, then **Directory Profiles**.

   The **Configure Profiles** screen appears as shown in Figure 4–2.

Figure 4–2 Oracle Access Administration Configure Profiles Screen

5. Click the link for the first Identity Server directory server profile in the **Configure LDAP Directory Server Profiles** section.

   The **Modify Directory Server Profile** screen appears.

6. In the **Database Instances** section, click **Add**.

   The **Create Database Instance** screen appears.

7. Specify *oidhost2.mycompany.com*, and select **Secondary** from the Server Type drop-down list.

8. Click **Save**.

   The **Modify Directory Server Profile** screen appears.

9. Click the link for the second Identity Server directory profile in the **Configure LDAP Directory Server Profiles** section.

10. In the **Database Instances** section, click **Add**.

    The **Create Database Instance** screen appears.

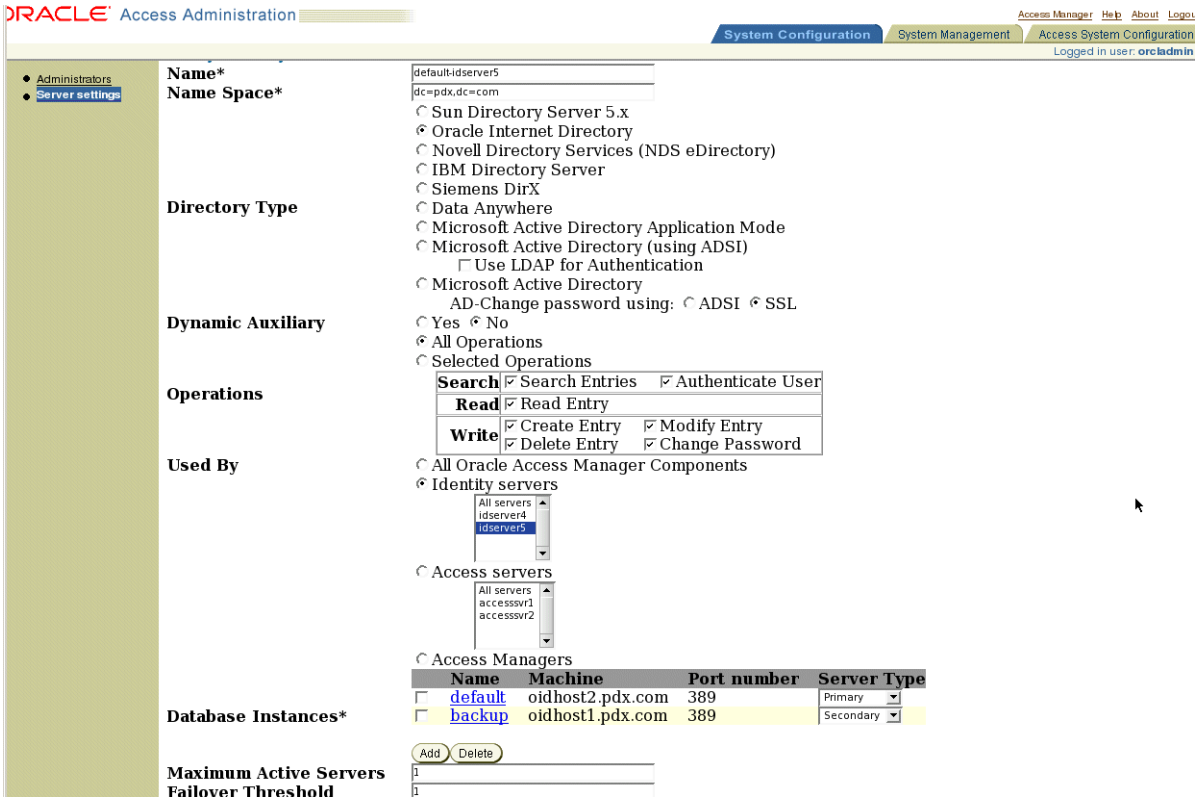
11. Specify *oidhost1.mycompany.com*, and select **Secondary** from the Server Type drop-down list.

12. Click **Save**.

    The **Modify Directory Server Profile** screen appears.

13. Restart both Identity Servers.

Figure 4–3 Oracle Access Administration Create Directory Server Profile Screen



4.20.2 Creating a Directory Server Profile for the Access Servers

1. Access the Identity System console at this URL:

   `http://ADMINHOST:port/access/oblix`

   The **Identity Administration** page appears.

2. Select **Identity System Console**.

   A login dialog appears.

3. Provide the user ID and password and click **Login**.

   The **System Configuration** page appears.

4. Click **System Configuration**, then **Directory Profiles**.

   The **Configure Profiles** screen appears as shown in Figure 4–2.

5. Click the link for the first Access Server directory server profile in the **Configure LDAP Directory Server Profiles** section.

   The **Modify Directory Server Profile** screen appears.

6. Record all entries and selections for the first Access Server's directory server profile (print the screen or write the entries and selections).

7. In the **Used By** section, select the **Access Servers** radio button and select Access Server 1 from the drop-down list.

8. In the **Database Instances** section, click **Add**.

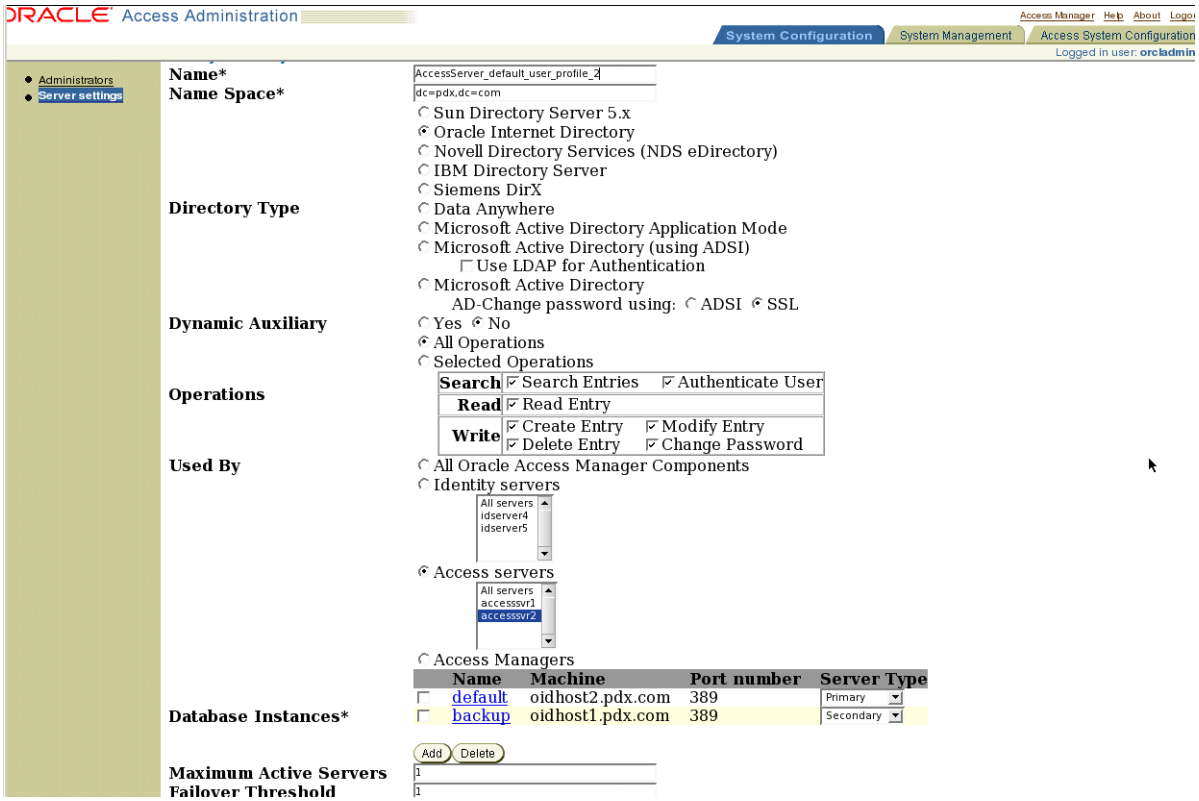
   The **Create Database Instance** screen appears.

9. Specify *oidhost2.mycompany.com*, and select **Secondary** from the Server Type drop-down list.
10. Click **Save**.

    The **Modify Directory Server Profile** screen appears.
11. Click **Add** in the **Configure LDAP Directory Server Profiles** section.

    The Create Directory Server Profile screen appears.

Figure 4–4 Oracle Access Administration Create Directory Server Profile Screen



12. Complete the **Name** field with a descriptive name for the directory server profile for the second Access Server on IDMHOST2.
13. Specify these entries and selections:

    Directory Type: Oracle Internet Directory

    Dynamic Auxiliary: No

    Operations: All Operations

    Used By: Access Servers (select Access Server 2 from the drop-down list)

    Database Instances: *oidhost1.mycompany.com* (select Secondary from the drop-down list), *oidhost2.mycompany.com* (select Primary from the drop-down list)
14. Click **Save**.

    A confirmation dialog appears.
15. Click **OK**.

    IDMHOST2 now has a default and a failover profile.

4.21 Verifying the Status of the Identity Servers

You can stop and start servers, perform operations, and then view the status to verify that failover is working.

1. Access the Identity System console at this URL:

   `http://IDMHOST1:port/identity/oblix`

   The Identity Administration page appears.

2. Select **Identity System Console**.

   A login dialog appears.

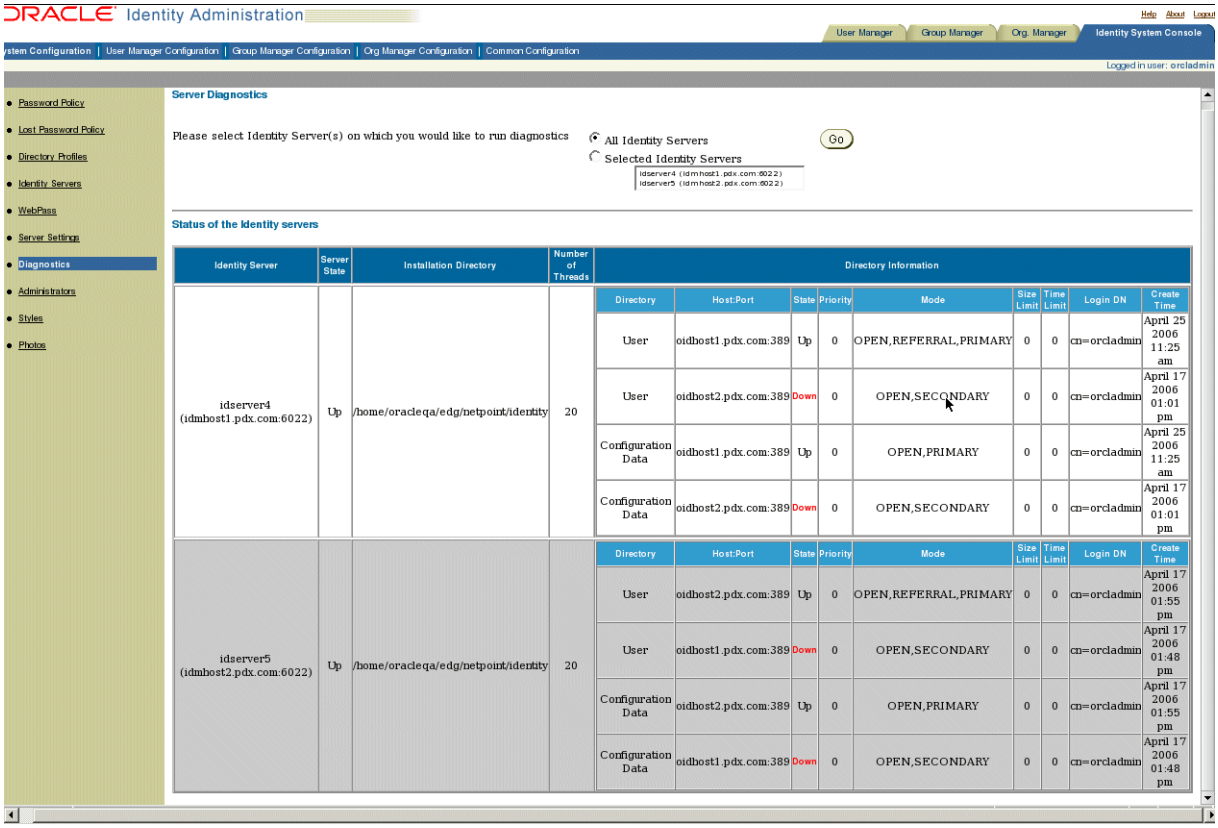
3. Provide the user ID and password and click **Login**.

   The **System Configuration** page appears.

4. Click **System Configuration**, then **Diagnostics**.

   The **Server Diagnostics** screen appears as shown in Figure 4–2.

Figure 4–5 Oracle Identity Administration Server Diagnostics Screen



5

Installing and Configuring Oracle Single Sign-On and Oracle Delegated Administration Services

Setting up the Load Balancing Router

Installing the Oracle HTTP Servers on WEBHOST3 and WEBHOST4

Installing and Configuring Oracle Single Sign-On

Reconfiguring Oracle Single Sign-On and Oracle Delegated Administration Services with the Oracle HTTP Servers

Configuring Session State Replication for the OC4J_SECURITY Instance

Disabling the Oracle HTTP Server on the Identity Management Tier

5.1 Setting up the Load Balancing Router

Before installing the Identity Management components, you must set up the Load Balancing Router to listen for requests to sso.mycompany.com on port 443 (https), and balance the requests to the Oracle HTTP Servers' listening port 7777 (http). The Load Balancing Router should perform the protocol conversion, and must be configured for persistent HTTP sessions.

5.2 Installing the Oracle HTTP Servers on WEBHOST3 and WEBHOST4

Use the Advanced option of the Oracle Universal Installer to install the Oracle HTTP Server instances.

1. Ensure that the system, patch, kernel and other requirements are met as specified in the *Oracle Application Server Installation Guide* for the platform you are using. You can find this guide in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Copy the `staticports.ini` file from the `Disk1/stage/Response` directory to a local directory, such as TMP. You will provide the path to this file during installation.
3. Edit the `staticport.ini` file to assign the following custom ports:

   ```
   Oracle HTTP Server port = 7777
   ```

> **Note:** Ensure that these ports are not already in use by any other service on the computer. Using the Static Ports feature to install the the Application Server Tier ensures that the port assignments will be consistent, if the ports are correctly specified in the file and the port is not already in use. If a port is incorrectly specified, the Oracle Universal Installer will assign the default port. If a port is already in use, the Oracle Universal Installer will select the next available port.

4. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Oracle Application Server 10.1.3.1.0 Installation** screen appears.
5. Specify an installation directory for the instance.
6. Select **Advanced Installation Mode**.
7. Click **Install**.

   The **Select Installation Type** screen appears.
8. Select **Web Server** and click **Next**.

   The **Specify Port Configuration Options** screen appears.
9. Select **Manual**, specify the location of the `staticports.ini` file, and click **Next**.

   The **Specify Instance Name** screen appears.
10. Specify the instance name and click **Next**.

    The **Cluster Topology Configuration** screen appears.
11. Check the box to configure the instance to be part of an Oracle Application Server cluster.
12. Specify the multicast address and port.

> **Note:** An example of a multicast address is `225.0.0.20`, with port `8001`. The address and port should be the same for each computer in a farm.

13. Click **Next**.

    The **Summary** Screen apears.
14. click **install**.
15. The **Configuration Assistants** screen appears. When the configuration process completes, the **End of Installation** screen appears.
16. Click **Exit**, and then confirm your choice to exit.
17. Verify that the installation was successful by viewing the Oracle HTTP Server instance. Start a browser and access:

    `http://`*`hostname`*`:7777`

Note: The *ORACLE_HOME*/install/readme.txt file contains the URLs for the installation and a command to verify the status of processes.

5.2.1 Renaming Apache 2.0 Web Server Instances

If you installed the Oracle HTTP Server based on Apache 2.0 from the Companion CD on WEBHOST3 and WEBHOST4, the instance name on both computers will be the default name assigned by the installer. In a cluster, you will want the instance names to be unique when you view the instances with the `opmnctl @cluster status` command. Follow these steps to rename an instance:

1. Stop the instance by issuing this command:

   ```
   opmnctl stopall
   ```

2. Modify the *ORACLE_HOME*/opmn/conf/opmn.xml file to change the instance id and name as shown:

   ```
   <ias-instance id="IAS-1
    name="IAS-1">
   ```

   Replace both occurrences of the existing instance name (IAS-1 in the example) with a unique instance name.

3. Save and close the file.

4. Restart the instance by issuing this command:

   ```
   opmnctl startall
   ```

5.2.2 Configuring the Oracle HTTP Server with the Load Balancing Router

The Load Balancing Router (soa.mycompany.com, shown in Figure 1–1, "mySOACompany with JSSO and Oracle Internet Directory") must be configured to receive client requests and balance them to the two Oracle HTTP Server instances on the Web tier. See the load balancing router documentation for instructions on configuring the load balancer, and follow the instructions in this section configure the Oracle HTTP Server.

Incoming requests must be associated with the Load Balancing Router hostname and port in the mySOACompany configuration. To configure this, perform these steps on WEBHOST3 and WEBHOST4:

1. Open the Oracle HTTP Server configuration file:

   Apache 1.3:

   ORACLE_HOME/Apache/Apache/conf/httpd.conf

   Apache 2.0:

   ORACLE_HOME/ohs/conf/httpd.conf

2. Perform the following steps:

   a. Add the `LoadModule certheaders_module` directive for the appropriate platform.

      UNIX Apache 1.3:

      ```
      LoadModule certheaders_module libexec/mod_certheaders.so
      ```

UNIX Apache 2.0; use this directive if you plan to use Apache 2.0 on UNIX:

```
LoadModule certheaders_module modules/mod_certheaders.so
```

Windows:

```
LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll
```

b. Add the lines shown for the Apache version you are using to create a `NameVirtualHost` directive and a `VirtualHost` container for soa.mycompany.com and port 443.

Apache 1.3:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soa.mycompany.com
  Port 7777
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>

NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soa.mycompany.com:443
  Port 443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Apache 2.0 (UNIX):

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soa.mycompany.com:7777
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>

NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName soa.mycompany.com:443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Notes: The `LoadModule` directives (in particular, the `LoadModule rewrite_module` directive) must appear in the `httpd.conf` file at a location preceding the `VirtualHost` directives. The server must load all modules before it can execute the directives in the `VirtualHost` container.

It is a good idea to create the `VirtualHost` directives at the end of the `httpd.conf` file.

The `LoadModule rewrite_module` directive must appear before the `LoadModule certheaders_module` directive.

3. Save the `httpd.conf` file.
4. Restart the components using these commands in *ORACLE_HOME*`/opmn/bin`:

   `opmnctl stopall`

   `opmnctl startall`

5. Verify that you can access these URLs:

   `http://soa.mycompany.com:7777/j2ee`

   `https://soa.mycompany.com/j2ee`

5.2.3 Configuring the esbd.myco.com URL for Internal Use

The Load Balancing Router must be configured to provide internal access to the ESBD instances on the Web tier. See the load balancing router documentation for instructions on configuring the load balancer, and follow the instructions in this section configure the Oracle HTTP Server for this URL.

Incoming requests must be associated with the Load Balancing Router hostname and port in the mySOACompany configuration. To configure this, perform these steps on WEBHOST3 and WEBHOST4:

1. Open the Oracle HTTP Server configuration file:

   Apache 1.3:

   ORACLE_HOME`/Apache/Apache/conf/httpd.conf`

   Apache 2.0:

   ORACLE_HOME`/ohs/conf/httpd.conf`

2. Perform the following steps:

   a. Add the `LoadModule certheaders_module` directive for the appropriate platform.

      UNIX Apache 1.3:

      `LoadModule certheaders_module libexec/mod_certheaders.so`

      UNIX Apache 2.0; use this directive if you plan to use Apache 2.0 on UNIX:

      `LoadModule certheaders_module modules/mod_certheaders.so`

      Windows:

      `LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll`

b. Add the lines shown for the Apache version you are using to create a `NameVirtualHost` directive and a `VirtualHost` container for esb.mycompany.com.

Apache 1.3:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName esbd.myco.com
  Port 7777
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>
```

Apache 2.0 (UNIX):

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName esbd.myco.com:7777
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
</VirtualHost>
```

Notes: The `LoadModule` directives (in particular, the `LoadModule rewrite_module` directive) must appear in the `httpd.conf` file at a location preceding the `VirtualHost` directives. The server must load all modules before it can execute the directives in the `VirtualHost` container.

It is a good idea to create the `VirtualHost` directives at the end of the `httpd.conf` file.

The `LoadModule rewrite_module` directive must appear before the `LoadModule certheaders_module` directive.

---

3. Save the `httpd.conf` file.
4. Restart the components using these commands in *ORACLE_HOME*`/opmn/bin`:

   `opmnctl stopall`

   `opmnctl startall`

5. Verify that you can access these URLs:

   `http://esbd.myco.com:7777/j2ee`

   `https://esbd.myco.com/j2ee`

5.3 Installing and Configuring Oracle Single Sign-On

Follow these steps to install the Identity Management components and configure Oracle Single Sign-On on IDMHOST1 and IDMHOST2.

5.3.1 Installing the First Identity Management Configuration

Follow these steps to install Identity Management on IDMHOST1:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.
3. Edit the `staticport.ini` file and uncomment these entries:

   ```
   Oracle HTTP Server port = 7777
   Oracle HTTP Server Listen port = 7777
   Application Server Control port = 1810
   ```

4. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **`runInstaller`**

   On Windows, double-click **`setup.exe`**

   The **Welcome** screen appears.

5. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.

6. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.
7. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.

8. Open a window and run the script, following the prompts in the window.
9. Return to the Oracle Universal Installer screen and click **Next**.

   The **Specify File Locations** screen appears with default locations for:

   - The product files for the installation (Source)
   - The name and path to an Oracle home (Destination)

   Note: Ensure that the Oracle home directory path for IDMHOST1 is the same as the path to the Oracle home location of IDMHOST2. For example, if the path to the Oracle home on IDMHOST1 is:

   `/u01/app/oracle/product/AS10gSSO`

   then the path to the Oracle home on IDMHOST2 must be:

   `/u01/app/oracle/product/AS10gSSO`

   ---

10. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

11. Select OracleAS Infrastructure 10g and click **Next**.

    The **Select Installation Type** screen appears.

12. Select **Identity Management** and click **Next**.

The **Confirm Pre-Installation Requirements** screen appears.

13. Ensure that the requirements are met and click **Next**.

    The **Select Configuration Options** screen appears.

14. Select **Oracle Single Sign-On, Oracle Delegated Administration Services**, and **High Availability and Replication**

    The **Specify Port Configuration Options** screen appears.

15. Select **Manual**, specify the location of the `staticports.ini` file, and click **Next**.

    The **Select High Availability Option** screen appears.

16. Select **OracleAS Cluster (Identity Management)** and click **Next**.

    The **Create or Join an OracleAS Cluster (Identity Management)** screen appears.

17. Select **Create a New OracleAS Cluster** and click **Next**.

    The **Specify New OracleAS Cluster Name** screen appears.

18. Complete the **New OracleAS Cluster Name** field with a name for the cluster and click **Next**.

    Note: Write down the cluster name. You will need to provide it in subsequent installations of instances that will join the cluster.

    The **Specify LDAP Virtual Host and Ports** screen appears.

19. Enter the name of the Load Balancing Router, the SSL port, and the non-SSL port.

20. Click **Next**.

    The **Specify OID Login** screen appears.

21. Complete the fields and click **Next**.

    The **Specify HTTP Load Balancer and Listen Ports** screen appears.

22. Enter the listen port of the HTTP Server and the host name and port of the HTTP Load Balancer, enabling the SSL option for the load balancer.

23. Click **Next**.

    The **Specify Instance Name and ias_admin Password** screen appears.

24. Specify the instance name and password and click **Next**.

    The **Summary** screen appears.

25. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.

26. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.

27. Click **Exit**, and then confirm your choice to exit.

5.3.2 Testing the Identity Management Components With Oracle Internet Directory

Follow these steps to test the first Identity Management installation with the Oracle Internet Directory:

1. Stop all components on OIDHOST1, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl stopall**

2. Ensure that all components on OIDHOST2 are running:

   ***ORACLE_HOME*/opmn/bin/opmnctl status**

3. Access the following URL:

   https://IDMHOST1.mycompany.com/pls/orasso

4. Stop all components on OIDHOST2, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl stopall**

5. Ensure that all components on OIDHOST1 are running:

   ***ORACLE_HOME*/opmn/bin/opmnctl status**

6. Access the following URL:

   https://IDMHOST2.mycompany.com/pls/orasso

5.3.3 Installing the Second Identity Management Configuration

Follow these steps to install Identity Management on IDMHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Application Server Quick Installation Guide* in the Oracle Application Server platform documentation library for the platform and version you are using.
2. Copy the `staticport.ini` file from the `Disk1/stage/Response` directory to the Oracle home directory.
3. Edit the `staticport.ini` file and uncomment these entries:

   ```
   Oracle HTTP Server port = 7777
   Oracle HTTP Server Listen port = 7777
   Application Server Control port = 1810
   ```

4. Start the Oracle Universal Installer as follows:

   On UNIX, issue this command: **runInstaller**

   On Windows, double-click **setup.exe**

   The **Welcome** screen appears.

5. Click **Next**.

   On UNIX systems, the **Specify Inventory Directory and Credentials** screen appears.

6. Specify the directory you want to be the `oraInventory` directory and the operating system group that has permission to write to it.
7. Click **Next**.

   On UNIX systems, a dialog appears, prompting you to run the `oraInstRoot.sh` script.

8. Open a window and run the script, following the prompts in the window.

9. Return to the Oracle Universal Installer screen and click **Next**.

   The **Specify File Locations** screen appears with default locations for:

   - The product files for the installation (Source)
   - The name and path to an Oracle home (Destination)

   Note: Ensure that the Oracle home directory path for IDMHOST1 is the same as the path to the Oracle home location of IDMHOST2. For example, if the path to the Oracle home on IDMHOST1 is:

   `/u01/app/oracle/product/AS10gSSO`

   then the path to the Oracle home on IDMHOST2 must be:

   `/u01/app/oracle/product/AS10gSSO`

   ---

10. Specify the **Destination Name** and **Path**, if different from the default, and click **Next**.

    The **Select a Product to Install** screen appears.

11. Select **OracleAS Infrastructure 10**g, and click **Next**.

    The **Select Installation Type** screen appears.

12. Select **Identity Management** and click **Next**.

    The **Confirm Pre-Installation Requirements** screen appears.

13. Ensure that the requirements are met and click **Next**.

    The **Select Configuration Options** screen appears.

14. Select **Oracle Single Sign-On, Oracle Delegated Administration Services**, and **High Availability and Replication**.

15. Click **Next**.

    The **Select High Availability Option** screen appears.

16. Select **OracleAS Cluster (Identity Management)** and click **Next**.

    The **Create or Join an OracleAS Cluster (Identity Management)** screen appears.

17. Select **Join an Existing OracleAS Cluster** and click **Next**.

    The **Specify Existing OracleAS Cluster Name** screen appears.

18. Complete the **Existing OracleAS Cluster Name** field with the name you provided for the cluster when installing the first instance and click **Next**.

    The **Specify LDAP Virtual Host and Ports** screen appears.

19. Enter the name of the Load Balancing Router, the SSL port, and the non-SSL port.

20. Click **Next**.

    The **Specify OID Login** screen appears.

21. Complete the fields and click **Next**.

    The **Specify HTTP Load Balancer and Listen Ports** screen appears.

22. Enter the listen port of the HTTP Server and the host name and port of the HTTP Load Balancer, enabling the SSL option for the load balancer.

23. Click **Next**.

    The **Specify Instance Name and ias_admin Password** screen appears.

24. Specify the instance name and password and click **Next**.

    The **Summary** screen appears.

25. Review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

    The **Install** screen appears with a progress bar. On UNIX systems, a dialog opens prompting you to run the `root.sh` script.

26. Open a window and run the script.

    The **Configuration Assistants** screen appears. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, the **End of Installation** screen appears.

27. Click **Exit**, and then confirm your choice to exit.

28. Repeat the tests in Section 5.3.2, "Testing the Identity Management Components With Oracle Internet Directory".

5.4 Reconfiguring Oracle Single Sign-On and Oracle Delegated Administration Services with the Oracle HTTP Servers

Follow the steps in this section to reconfigure Oracle Single Sign-On and Oracle Delegated Administration Services.

1. Ensure that:
   - The Oracle Identity Management instance is started (status is Up).
   - You have the Oracle Internet Directory host and port numbers.
   - You have the password for cn=orcladmin, or another user who is a member of the iASAdmins group

2. Issue the command **`ssocfg.sh`** (UNIX) or (Windows) in *`IDMHOST1_ORACLE_HOME`*`/sso/bin` and *`IDMHOST2_ORACLE_HOME`*`/sso/bin`:

   `ssocfg.sh https` ***`sso.mycompany.com`*** **`443`**

   In the preceding command, *sso.mycompany.com* is the VIP hostname for the Load Balancing Router.

3. On IDMHOST1 and IDMHOST2, set the environment variables `ORACLE_HOME` and `ORACLE_SID`.

4. Issue the command **`ssoreg.sh`** (UNIX), or **`ssoreg.bat`** (Windows) in *`IDMHOST1_ORACLE_HOME`*`/sso/bin`:

   `ssoreg.sh -oracle_home_path $ORACLE_HOME`

   `-config_mod_osso TRUE`

   `-site_name` ***`sso.mycompany.com`*****`:443`**

   `-remote_midtier`

   `-config_file $ORACLE_HOME/Apache/Apache/conf/osso/`***`myosso.conf`***

   `-mod_osso_url https://`***`sso.mycompany.com`*****`:443`**

In the example, *myossof.conf* is the name of the resulting obfuscated osso configuration file created.

5. Copy the *myosso.conf* file to *WEBHOST3_ORACLE_HOME*/Apache/Apache/conf/osso and *WEBHOST4_ORACLE_HOME*/Apache/Apache/conf/osso.

6. Configure mod_osso by following the instructions for the Oracle HTTP Server version in use:

   Release 3 (10.1.3):

   a. Issue this command on WEBHOST3 and WEBHOST4:

      (UNIX) ***ORACLE_HOME*/Apache/Apache/bin/osso1013 config_file**

      (Windows) **perl *ORACLE_HOME*/Apache/Apache/bin/osso1013 config_file**

   Release 3 (10.1.2):

   a. Copy the obfuscated osso configuration file created in Step 4 to the ***ORACLE_HOME*/Apache/Apache/conf/osso** directory in WEBHOST3 and WEBHOST4:

   b. Modify the *ORACLE_HOME*/Apache/Apache/conf/httpd.conf file by uncommenting the Include mod_osso.conf directive.

   c. Modify the *ORACLE_HOME*/Apache/Apache/conf/mod_osso.conf file to add this directive:

      ```
      OssoConfigFile $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf
      ```

7. Copy the *IDMHOST1_ORACLE_HOME*/sso/conf/sso_apache.conf file to WEBHOST3.

8. Modify the *WEBHOST3_ORACLE_HOME*/Apache/Apache/conf/httpd.conf file to add this directive:

   ```
   Include sso_apache.conf
   ```

9. Modify the sso_apache.conf file on WEBHOST3 to enable the SSL section and comment out the rewrite section (only the section shown in the example is enabled).

   ```
   <IfDefine SSL>
      Oc4jExtractSSL on
      <Location /sso>
          SSLOptions +ExportCertData +StdEnvVars
      </Location>
   </IfDefine>
   ```

10. Copy the sso_apache.conf file from WEBHOST3 to WEBHOST4.

11. Modify the *WEBHOST4_ORACLE_HOME*/Apache/Apache/conf/httpd.conf file to add this directive:

    ```
    Include sso_apache.conf
    ```

12. Use these commands to identify the AJP port on IDMHOST1 and IDMHOST2:

    IDMHOST1_ORACLE_HOME/opmn/bin/opmnctl status -l

    IDMHOST2_ORACLE_HOME/opmn/bin/opmnctl status -l

13. Modify the *WEBHOST3_ORACLE_HOME*/Apache/Apache/conf/mod_oc4j.conf and *WEBHOST4_ORACLE_HOME*/Apache/Apache/conf/mod_oc4j.conf files by substituting the port values obtained in Step 21 for *AJP port 1* and *AJP port 2* in the Oc4jMount directives). This configuration directs Oracle Single Sign-On and Oracle Delegated Administration Services requests to the identity management server using the AJP protocol.

```
<IfModule mod_oc4j.c>
...
Oc4jMount /oiddas ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /oiddas/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /sso ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /sso/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /ssohelp ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /ssohelp/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /pls ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
Oc4jMount /pls/* ajp13://IDMHOST1:AJP port1,IDMHOST2:AJP port2
...
</IfModule>
```

14. Configure Oracle Delegated Administration Services by adding the following to *WEBHOST3_ORACLE_HOME*/Apache/Apache/conf/mod_osso.conf:

```
<IfModule mod_osso.c>
# for oiddas protected region
  <Location /oiddas/ui/oracle/ldap/das>
   require valid-user
   AuthType Basic
  </Location>
</IfModule>
<IfModule mod_alias.c>
# Define the alias which maps the "/uixi/" URI to
# the current version of the UIX installables
  Alias /uixi/ "ORACLE_HOME/uix/cabo/"
# Turn on browser caching for the UIX installables
  <Location /uixi>
# Use mod_headers to set the cache-control header
   Header set cache-control "Public"
# Use mod_expires to set the expires header to some
# date in the distant future
    ExpiresActive on
    ExpiresDefault "access plus 364 days"
  </Location>
</IfModule>
```

15. Copy *WEBHOST3_ORACLE_HOME*/Apache/Apache/conf/mod_osso.conf to *WEBHOST4_ORACLE_HOME*/Apache/Apache/conf/, changing the *ORACLE_HOME* value in `Alias /uixi/ "ORACLE_HOME/uix/cabo/"` to specify *WEBHHOST4_ORACLE_HOME*.

16. Configure the Oracle HTTP Server with the Load Balancing Router by adding the following to *WEBHOST3_ORACLE_HOME*/Apache/Apache/conf/httpd.conf:

    a. Add the `LoadModule certheaders_module` directive for the appropriate platform.

    b. UNIX Apache 1.3:

    ```
    LoadModule certheaders_module libexec/mod_certheaders.so
    ```

    UNIX Apache 2.0; use this directive if you plan to use Apache 2.0 on UNIX:

```
LoadModule certheaders_module modules/mod_certheaders.so
```

Windows:

```
LoadModule certheaders_module modules/ApacheModuleCertHeaders.dll
```

c. Add the following lines to create a `NameVirtualHost` directive and a `VirtualHost` container for **sso.mycompany.com** and port **443**.

Apache 1.3:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName sso.mycompany.com
  Port 443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Apache 2.0:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
  ServerName sso.mycompany.com:443
  ServerAdmin you@your.address
  RewriteEngine On
  RewriteOptions inherit
  SimulateHttps On
</VirtualHost>
```

Notes: The `LoadModule` directives (in particular, the `LoadModule rewrite_module` directive) must appear in the `httpd.conf` file at a location preceding the `VirtualHost` directives. The server must load all modules before it can execute the directives in the `VirtualHost` container.

It is a good idea to create the VirtualHost directives at the end of the `httpd.conf` file.

---

17. Copy *WEBHOST3_ORACLE_HOME*`/Apache/Apache/conf/httpd.conf` to *WEBHOST4_ORACLE_HOME*`/Apache/Apache/conf/`.

18. Restart the Oracle HTTP Server.

5.5 Testing the Identity Management Tier Components

After both Identity Management configurations are complete, test the configurations as follows:

1. Stop all components on IDMHOST1, using this command:

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

2. Ensure that all components on IDMHOST2 are running, using this command:

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

3. Access the following URLs from two browsers:

   https://sso.mycompany.com/pls/orasso

   https://sso.mycompany.com/oiddas

4. Start all components from IDMHOST1, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl startall**

5. Stop all components on IDMHOST2, using this command:

   ***ORACLE_HOME*/opmn/bin/opmnctl stopall**

6. Ensure that the login session is still valid for the `orasso` and `oiddas` logins.

5.6 Configuring Session State Replication for the OC4J_SECURITY Instance

1. Access the Application Server Control Console at:

   http://mycompany.com:8888/em

   A login dialog opens.

2. Provide the user name and password that was set during installation and click **Login**.

   The **Farm** page appears.

3. Select the application server instance.

   A login dialog opens.

4. Provide the user name and password that was set during installation and click OK.

5. Select the OC4J_SECURITY OC4J instance.

   The OC4J_SECURITY page appears.

6. Click **Administration**.

7. Click **Replication Properties**.

8. Check the **Replicate session state** box and enter values for Multicast Host and Multicast Port.

9. Click **Apply**.

10. Restart the OC4J_SECURITY instance.

5.7 Disabling the Oracle HTTP Server on the Identity Management Tier

Follow these instructions on IDMHOST1 and IDMHOST2 to disable the Oracle HTTP Server on the Identity Management tier.

1. 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>
```

2. Issue this command in *ORACLE_HOME*/opmn/bin:

   opmnctl stopall

3. Issue this command in *ORACLE_HOME*/opmn/bin:

   opmnctl startall

6

Maintaining the SOA Suite

Managing the SOA Suite

Enabling Disaster Recovery

6.1 Managing the SOA Suite

Common administration operations are listed in Table 6–1. You can monitor and manage the system using consoles or command line tools.

Table 6–1 System administration tasks, tools, and related documentation

Task or operation	Tool	Where documented
Access the Application Server Control Console	Application Server Control Console	*Oracle Application Server Administrator's Guide*
Start and stop Oracle Application Server	Application Server Control Console	*Oracle Application Server Administrator's Guide*
Create and delete OC4J instances	Application Server Control Console	*Oracle Application Server Administrator's Guide*
List and view log files	Application Server Control Console	*Oracle Application Server Administrator's Guide*
Back up and restore instances	Command line	*Oracle Application Server Administrator's Guide*
Change hostname, domain name, or IP address	Command line	*Oracle Application Server Administrator's Guide*
Manage wallets and Certificate Revocation Lists	Command line	*Oracle Application Server Administrator's Guide*
Start and stop the BPEL Process Manager server	Command line	*Oracle Application Server Administrator's Guide*
Manage, administer, and debug processes deployed to Oracle BPEL server	Oracle BPEL Console	*Oracle BPEL Process Manager Quick Start Guide*
Deploy Oracle Web Services Manager components	Web Services Manager Control Console	*Oracle Web Services Manager Deployment Guide*

6.2 Enabling Disaster Recovery

For recommendations and instructions on enabling disaster recovery, see the *Oracle Application Server High Availability Guide*

Index

A

Access Gate, creating instance, 4-27
Access Manager
  Access Server and, 4-18
  configuring, 4-16
  defined, 4-2
  isolated subnet and, 4-2
  WebGate and, 4-21
Access Server
  Access Manager and, 4-2
  configuring as failover server, 4-34
  configuring failover with Web Gate, 4-35
  defined, 4-14
  installing, 4-18
  installing, user account privileges and, 4-3
  management of login session, 4-2
  password file and starting, 4-21
  role in Access System, 4-14
  service name, 4-21
  starting, 4-21
  user account on Microsoft Windows, 4-18
  WebGate and, 4-2
Access Server SDK
  functions, 4-25
  GCC runtime libraries and, 4-27
  installing, 4-25
  obtaining, 4-25
active failover, 4-37
administrator access, Oracle Access Manager, 4-2
administrator privileges, Oracle Acccess Manager
    installation and, 4-3
AJP
  port range, 3-7
  protocol, Access SDK and, 4-3
  protocol, request routing and, 5-13
ant-orabpel.properties file, 3-13
AppDBfailover.xml file, 4-41
application error, 3-23
Application Server Control Console, disabling, 3-6
application server instance, naming, 3-5
Application Tier
  defined, 1-3
  installing myJ2EECompany, 3-1
auditing rules, Oracle Internet Directory, 4-2
authentication
  and authorization, J2EE applications, 4-3
  OracleAS Single Sign-On, 5-6
availability
  Load Balancing Router tuning and, 2-8
  system, 2-8

B

back up instance, 6-1
bind distinguished name, example, 4-9
BPEL Console, error, 3-15
BPEL Process Manager server, starting and
    stopping, 6-1
bpel.xml file, 3-13

C

cache synchronization problems, 4-37
ccore, disabling application, 3-20
Certificate Revocation Lists, managing, 6-1
clocks
  synchronization, Oracle Internet Directory
      and, 2-2
  synchronizing, 4-3
ClusterName property, BPEL, 3-12
Cold Failover Cluster (Identity Management)
    solution, 1-10
collaxa-config.xml file, 3-12, 3-13
communication
  Access Manager, 4-16
  in Enterprise Deployments, 1-2
ConfigDBfailover.xml file, 4-41
ConfigureAAAServer utility
  failover and, 4-36
  using, 4-40
connection
  component and firewall time out values, 3-27
  failure, OC4Japplication, 3-23
coreman, disabling application, 3-20
credentials, Identity Server and, 4-2

D

Data Tier
  configuration, 2-8
  defined, 1-3
database connections, time out and, 3-27
data-sources.xml file, 3-26
default-web-site.xml file, 3-6, 3-20
directory server
  failover, 4-36
  failover solutions, 4-37
  profile for failover, creating, 4-41
distinguished name permissions, Oracle Access Manager, 4-5
DMZs, communication across, 1-2
domain name, changing, 6-1

E

enableCluster property, BPEL, 3-12
enterprise deployment, defined, 1-1
errno=110, 3-23
error
  BPEL Console, 3-15
  installing Oracle Access Manager products, 4-35
esb_config.ini file, 3-16
esbparam.properties file, 3-17
etc/services file, 2-3
external traffic, routing, 1-2

F

F5 load balancer, proxy settings, SSL, 4-25
failed request, 3-23
failover
  directory server, 4-36
  directory server profile, creating, 4-41
  in Oracle Application Server, 1-10
  sequence, Identity Server, 4-37
  solutions, 4-37
failover.xml file, 4-38
Fast Connection Failover
  configuring on application tier, 3-26
  configuring on Data TIer, 2-2
  firewall zones, 3-28
file
  ant-orabpel.properties, 3-13
  AppDBfailover.xml, 4-41
  bpel.xml, 3-13
  collaxa-config.xml, 3-12, 3-13
  ConfigDBfailover.xml, 4-41
  data-sources.xml, 3-26
  default-web-site.xml, 3-6, 3-20
  esb_config.ini, 3-16
  esbparam.properties, 3-17
  etc/services, 2-3
  failover.xml, 4-38
  httpd.conf, 4-16, 5-12
  install.properties, 3-30
  jgroup-protocol.xml, 3-13
  mod_oc4j.conf, 5-13
  opmn.xml
    default ports in, 3-22
    disabling Oracle HTTP Server, 5-15
    Fast Connection Failover and, 3-26
    instance names in, 3-3, 5-3
    MaxPermSize parameter and, 3-15
    service failover and, 3-16
    static discovery and, 3-25
    Web Pass and, 4-8
  osso.conf, 5-12
  readme.txt, 3-6
  sqlnet.ora, 2-2
  sso_apache.conf, 5-12
  WebResrcDBfailover.xml, 4-41
  wsdl, 3-13
firewall
  cluster gateway and, 3-3
  communication restrictions and security, 1-2
  dropped connections and, 3-27
  ports open, 3-27
  reverse proxy server and, 1-11
forward proxy, defined, 1-10

G

gateway, disabling application, 3-20
GCC
  3.3.2 runtime libraries, 4-4
  runtime libraries, 4-7, 4-11, 4-15, 4-20
  runtime libraries, Access Server SDK and, 4-27
  runtime libraries, Oracle Access Manager and, 4-23, 4-27
group, Identity Server and, 4-2
-gui installation option, error, 4-4
GUI installation, Oracle Access Manager, 4-4

H

hardware
  cluster, 1-10
  requirements, 1-8
high availability, enterprise deployment and, 1-2
hostname, changing, 6-1
HTTP
  persistent sessions, Load Balancing Router, 5-1
  requests, Web Gate and, 4-2
httpd.conf file, 4-16, 5-12
hw_services application, 3-29

I

ias_admin password, 2-7
identity store, defined, 1-3
installation error
  Oracle Access Manager, 4-6
  Oracle Access Manager products, 4-35
install.properties file, 3-30
install.sso.support property, 3-30
instance name, application server, 3-5
IP address, changing, 6-1
IS_SSL value, Load Balancing Router, 4-25

J

J2EE applications
  authentication and authorization, 4-3
jgroup-protocol.xml file, 3-13
JMX notifications, Application Server Control Console and, 3-6
JSSO
  hw_services application and, 3-29
  OWSM configuration, 3-30

L

LD_ASSUME_KERNEL environment variable, 4-8, 4-29
LDAP
  traffic, failover, 2-8
ldapbind, Oracle Internet Directory monitoring, 2-8
ldapRootPasswd parameter, 4-39
listener, Net, restarting, 2-2
load balancing
  and cache synchronization, 4-37
  directory server, 4-37
Load Balancing Router
  function, 1-1
  IS_SSL value, 4-25
  LDAP traffic, 2-8
  OID hosts and, 2-7
  Oracle Access Manager Access Server and, 4-25
  protocol conversion, 5-1
  tuning monitoring, 2-8
Log on as a service privilege, 4-3
login session management, Access Server and, 4-2

M

managing OC4J instance, 3-5
MaxPermSize parameter, 3-15
memory requirements, 1-8
Microsoft Windows
  Access Server user account, 4-18
  Oracle Access Manager components and, 4-2
mod_oc4j
  Web Gate and, 4-3
mod_oc4j
  error, 3-23
mod_oc4j.conf file, 5-13
monitoring Oracle Internet Directory processes, 2-8
multicast addresses, 3-26
multicast traffic, eliminating, 3-25
multimaster replication, Oracle Internet Directory, 1-9

N

NameVirtualHost directive, 3-8, 3-10, 5-4, 5-6
naming application server instance, 3-5
Net listener, restarting, 2-2
netstat command, 2-3, 3-7, 3-22

O

obencrypt tool, 4-39
ObSSOCookie, Access Server and, 4-3
OC4J
  application error, 3-23
  applications, single sign-on and, 4-3
  instance, Application Server Control Console and, 3-5
  instance, installing, 3-4
ODS password, 2-7
ohs-routing, 3-6
ohs-routing tag, disabling Application Server Control Consoles and, 3-6
oidadmin tool, starting, 2-8
oid.mycompany.com, configuring for Load Balancing Router, 2-7
ONS remote port, firewall zones, 3-28
opmn.xml file
  configuring for static discovery, 3-25
  default ports in, 3-22
  disabling Oracle HTTP Server, 5-15
  Fast Connection Failover and, 3-26
  instance names in, 3-3, 5-3
  MaxPermSize parameter and, 3-15
  service failover and, 3-16
  Web Pass and, 4-8
Oracle Access Manager
  Identity server, defined, 4-2
  installation error, 4-6, 4-35
Oracle Access Manger
  installation account, 4-3
Oracle BPEL server, process management, 6-1
Oracle HTTP Server, non-SSL port, 4-25
Oracle Internet Directory
  clocks, 2-2
  installing, 2-2
  monitoring processes, 2-8
  multimaster replication and, 1-9
  security, 1-2
Oracle Web Services Manager, deploying components, 6-1
ORACLE_HOME environment variable, 5-11
ORACLE_SID environment variable, 5-11
OracleAS Cold Failover Cluster (Identity Management) solution, 1-10
OracleAS Metadata Repository, installing, 2-1
organization, Identity Server and, 4-2
osso.conf file, 5-12

P

passive failover, 4-37
password error, -gui installation option, 4-4, 4-10
path, Oracle home, specifying, 2-4, 2-6
persistent HTTP sessions, Load Balancing Router and, 5-1
Policy, 4-14

Policy Manager
confirming installation, 4-18
defined, 4-14
WebPass and, 4-14
policy store, defined, 1-3
policymanager, disabling application, 3-20
pooled connections, time out and, 3-27
port
determining availability with netstat, 2-3
freeing, 2-3
Identity Server instance, 4-15
Oracle HTTP Server, 3-1, 5-1
Oracle Internet Directory, 2-3
Oracle Internet Directory servers, 2-7
port, freeing, 2-5
primary (hot) node, 1-10
processes, managing, Oracle BPEL server, 6-1
protocol conversion, Load Balancing Router, 5-1
ProxySSLHeaderVar parameter, 4-25

R

readme.txt file, 3-6
replication mode, load balancing with directory server, 4-37
request failed, 3-23
restore instance, 6-1
reverse proxy, defined, 1-11
round robin load balancing, time out value and, 2-8
routing of external traffic, 1-2

S

secondary (cold) node, 1-10
secondary Identity Server failover, WebPass, 4-34
security
enterprise deployment configurations and, 1-1, 1-2
firewalls and, 1-2
service, Oracle Access Manager on Microsoft Windows, 4-3
session management (login), Access Server and, 4-2
single sign-on,OC4J applications, 4-3
singleton adapter, Enterprise Service Bus and, 3-16
soapCallbackUrl, 3-13
soapServerUrl, 3-13
SQLNET.EXPIRE_TIME parameter, configuring, 2-2
sqlnet.ora file, 2-2
SSL acceleration, 4-25
sso_apache.conf file, 5-12
synchronization
cache, load balancing and, 4-37
time, 4-3
synchronizing system time, 2-7
system availability, 2-8

T

TCP session time out value, 2-2
time
synchronization, 4-3
system, synchronizing, 2-7
time out
Load Balancing Router, 2-8
tuning Load Balancing Router values, 2-8
values, Oracle Application Server components and firewall/load balancer, 3-27
tuning time out values, Load Balancing Router, 2-8

U

user account
Access Server on Microsoft Windows, 4-18
in Enterprise Deployments, 1-1

V

VirtualHost container, 3-8, 3-10, 5-4, 5-6

W

wallets, managing, 6-1
WebGate
Access Server and, 4-2
and Access Server failover, 4-33
configuring failover, 4-35
confirming installation, 4-25
creating instance, 4-21
defined, 4-2
GCC runtime libraries and, 4-23
installation directory, 4-21
installing, 4-21
oracle directory, 4-21
role in Access System, 4-14
user account privileges for installation, 4-21
virtual sites and, 4-21
web server and, 4-21
WebPass
Access Manager and, 4-14
and Oracle Access Manager Server failover, 4-33
configuring failover with secondary Identity Server, 4-34
configuring with Oracle Access Manager Server, 4-8
confirming installation, 4-8
defined, 4-2
WebResrcDBfailover.xml file, 4-41
worklist application, disabling, 3-31
wsdl file, 3-13