Oracle® Application Server 10*g*

Advanced Topologies for Enterprise Deployments

10*g* (9.0.4)

Part No. B12115-01

September 2003

ORACLE®

Oracle Application Server 10*g* Advanced Topologies for Enterprise Deployments, 10*g* (9.0.4)

Part No. B12115-01

Primary Author: Orlando Cordero

Contents

6 Performance and Tuning Considerations

Index

Send Us Your Comments

Oracle Application Server 10*g* Advanced Topologies for Enterprise Deployments, 10*g* (9.0.4)

Part No. B12115-01

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

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

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

- Electronic mail: appserverdocs_us@oracle.com
- FAX: (650) 506-7375 Attn: Oracle Application Server Documentation Manager
- Postal service:

  Oracle Corporation
  Oracle Application Server Documentation
  500 Oracle Parkway, M/S 1op6
  Redwood Shores, CA 94065
  USA

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

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

Preface

The Oracle Application Server 10g Advanced Topologies for Enterprise Deployments covers requirements, new features in the installer, Oracle Application Server concepts that affect installation, compatibility with other products, and managementin information for an enterprise topology.

Intended Audience

This guide is intended for users who are comfortable performing basic system administration tasks, such as creating users and groups, adding users to groups, and installing operating system patches on the computer where Oracle Application Server will be installed. During the install process, you will need to execute shell scripts as root.

Structure of This Guide

This guide contains the following chapters and appendixes:

Chapter 1, "Enterprise Topology Overview"

Contains overview information about the several Oracle Application Server enterprise deployment topologies.

Chapter 2, "Installation and Configuration Considerations for an Enterprise Topology"

Contains pre-installation requirements, installation, post-installation, and configuration information for each topology.

Chapter 3, "Configuring Single Sign-On in an Enterprise Deployment Topology"

Contains information about configuring Oracle Application Server Single Sign-On in a variety of middle-tier configurations and topologies.

Chapter 4, "Networking"

Contains information about networking considerations, such as port numbering, load balancers, and firewalls.

Chapter 5, "Managing an Enterprise Deployment Topology"

Contains information about some of the tools and techniques for managing an enterprise deployment topology.

Chapter 6, "Performance and Tuning Considerations"

Contains information about the most common performance and tuning issues, including where to find additional sources of information.

Related Documents

For more information, see the following guides:

- Oracle Application Server 10g Administrator's Guide
- Oracle Application Server 10g Concepts

Conventions

This guide uses the following conventions:

Convention	Meaning
boldface text	Boldface type in text indicates objects (such as buttons and fields) on screens.
`code`	Text in the code font indicates filenames, commands, or contents of configuration files.
`italicized code`	Italicized code indicates placeholder text that you need to replace with an appropriate value.
[ ]	Brackets enclose optional clauses from which you can choose one or none.
. . .	Ellipses indicate that extraneous information have been omitted.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

1 Enterprise Topology Overview

This chapter contains the following:

1.1 About Enterprise Topologies and Why Oracle Recommends Them

An enterprise topology is an advanced installation and configuration of Oracle Application Server, usually in a large setting such as a data center.

In an enterprise deployment topology, there are three main application server deployment goals:

- Ensuring that quality of service exists in the software and hardware configurations in any given topology:
  - The enterprise systems efficiently managed and balanced workloads;
  - Applications run efficiently when resources such as hardware, network tools, etc., are added or removed in a deployment topology;
  - Planned and unplanned activities such as system management tasks have zero downtime in the topology.
- Provide a secure application server platform;
- Security and Identity Management:
  - Ensure that users can be provisioned and managed centrally;
  - Ensure that delegation of administration is possible and done consistently;
  - Provide the ability to integrate with other security and identity management systems in an enterprise topology.
- Software Provisioning and Management:
  - Simplify and automate application distribution and accessibility;
  - Ensure that systems can be self managed;
  - Monitor and manage many systems as one logical unit;

- Introduce Oracle Enterprise Manager as a one-stop management tool for managing an enterprise.

To learn more about Oracle Application Server concepts, see *Oracle Application Server 10g Concepts*.

For requirements and installation information for each of the topologies, see Chapter 11 of the *Oracle Application Server 10g Installation Guide*.

1.2 Recommended Topologies

The following sections describe several configurations in an enterprise topology:

- Enterprise Data Center Topology: J2EE Applications
- Departmental Topology
- Development Life Cycle Topology

1.3 Enterprise Data Center Topology: J2EE Applications

This deployment topology is optimized to support J2EE applications. It contains the components required to run J2EE applications in a secure, high availability environment.

If you have applications that use components from the Portal and Wireless or the Business Intelligence and Forms middle tier types, see Section 1.4, "Enterprise Data Center Topology: Portal, Wireless, and Business Intelligence Applications".

Target Users

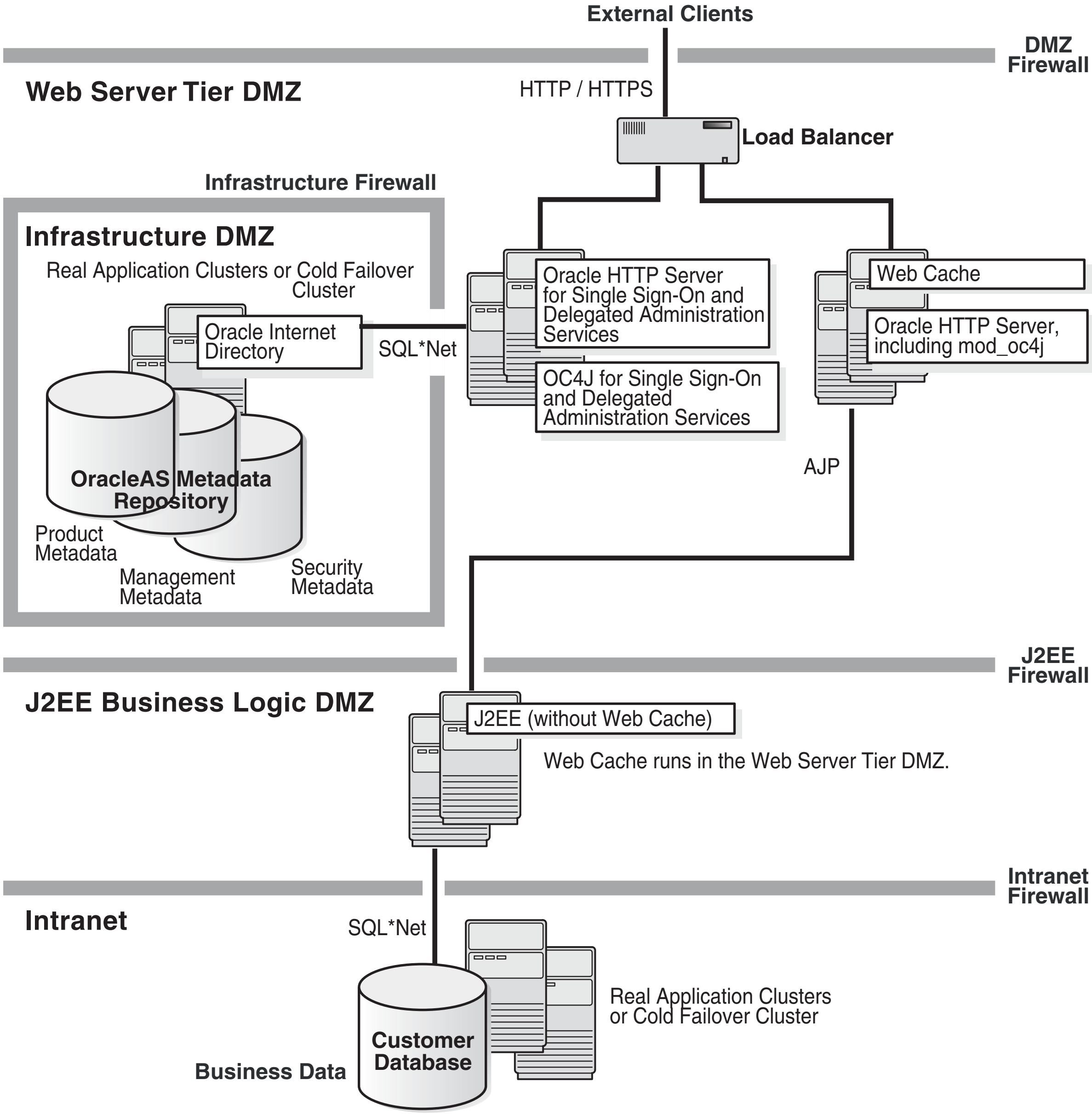
This topology is intended for enterprises who have users internal as well as external to the organization. Requests from external users go through firewalls.

Description

This topology (Figure 1–1) distributes Oracle Application Server components over multiple computers and tiers. Access to the computers in each tier is guarded by firewalls. Generally, you do not want Web servers, which are high risk components for Internet attacks, to have direct access to other computers in the enterprise. You want the requests to go through firewalls.

The distributed topology enables you to scale the number of computers in each tier (to increase performance and availability) without affecting computers in other tiers. For example, if you discover a bottleneck in the computers running OracleAS Web Cache and Oracle HTTP Server, you can add more computers to run those components.

Figure 1–1 Enterprise Data Center Topology: J2EE Applications


External Clients
DMZ Firewall
Web Server Tier DMZ
HTTP / HTTPS
Load Balancer
Infrastructure Firewall
Infrastructure DMZ
Real Application Clusters or Cold Failover Cluster
Oracle Internet Directory
SQL*Net
Oracle HTTP Server for Single Sign-On and Delegated Administration Services
OC4J for Single Sign-On and Delegated Administration Services
Web Cache
Oracle HTTP Server, including mod_oc4j
OracleAS Metadata Repository
Product Metadata
Management Metadata
Security Metadata
AJP
J2EE Firewall
J2EE Business Logic DMZ
J2EE (without Web Cache)
Web Cache runs in the Web Server Tier DMZ.
Intranet Firewall
Intranet
SQL*Net
Real Application Clusters or Cold Failover Cluster
Customer Database
Business Data

Single Sign On Middle Tier (Web Server Tier DMZ)

This tier is located just inside the outermost firewall. The load balancer gets requests from external users and forwards them to the two sets of computers in this tier. For each set of computers, you should have at least two computers, to serve as a backup and also to improve performance. You can add more computers to each set as necessary.

Internal users also access the Web servers running in this tier.

The computers in this tier run the following components:

- One set of computers runs OracleAS Web Cache and Oracle HTTP Server.

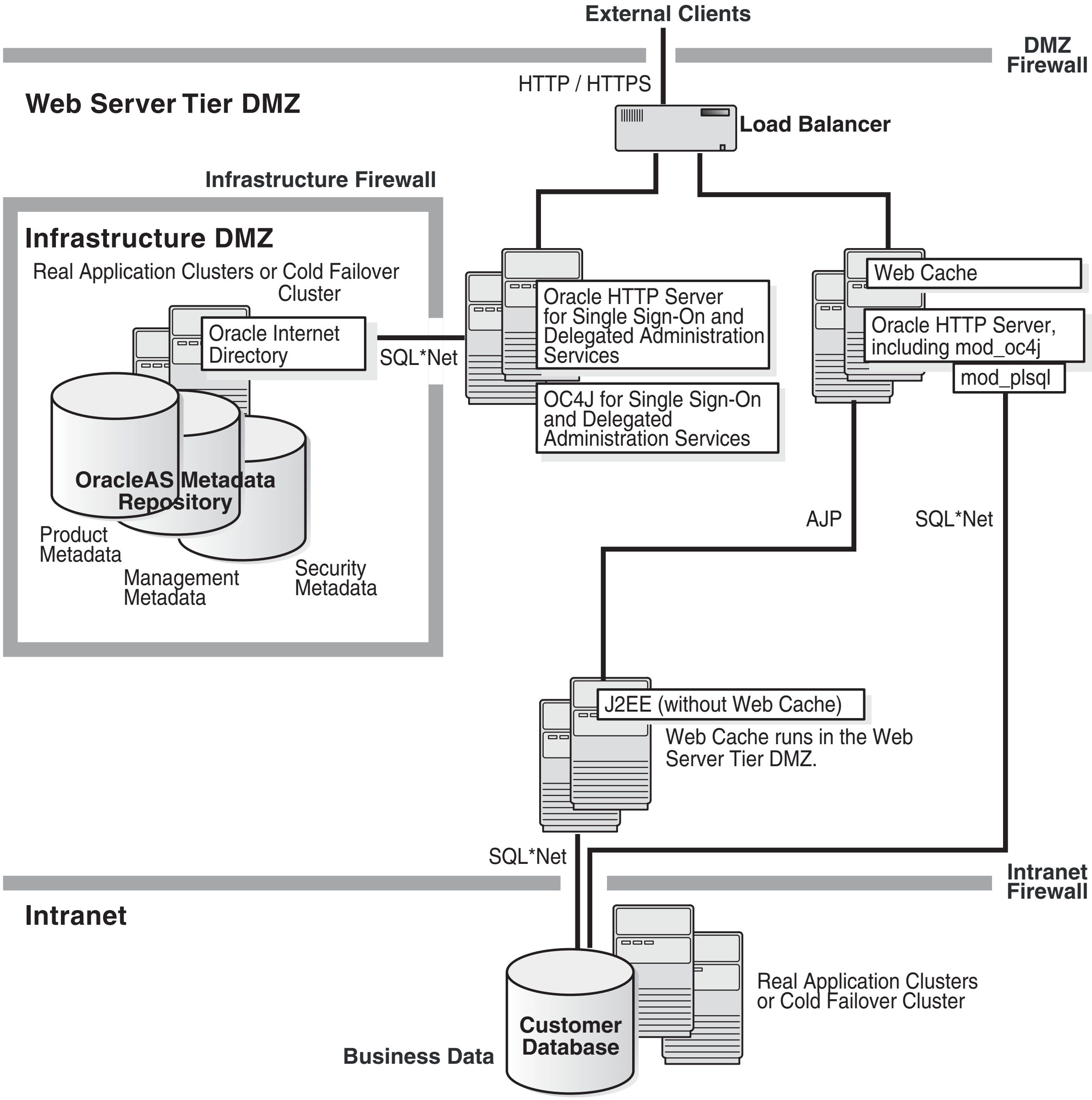
  This tier runs all the Web servers. Oracle HTTP Server and OracleAS Web Cache handle requests for static objects and J2EE applications. They send the requests to computers in the J2EE Business Logic DMZ tier. To increase performance and availability, the `mod_oc4j` module in Oracle HTTP Server performs load balancing and failover.

- Another set of computers runs Oracle Application Server Single Sign-On and Oracle Delegated Administration Services.

  Oracle Application Server Single Sign-On authenticates internal and external users, and Oracle Delegated Administration Services enable users to edit their profiles in the Oracle Internet Directory.

mod_plsql: If you need the Web servers to invoke mod_plsql applications stored in the customer database, you do not need the J2EE firewall (compare Figure 1–1 and Figure 1–2). The main purpose of the J2EE firewall is to block SQL*Net access from Web servers to the intranet. If you are using mod_plsql, which uses SQL*Net, then you do not want the messages blocked.

Figure 1–2 Enterprise Data Center Topology: J2EE Applications that need to access mod_plsql


External Clients
DMZ Firewall
HTTP / HTTPS
Web Server Tier DMZ
Load Balancer
Infrastructure Firewall
Infrastructure DMZ
Real Application Clusters or Cold Failover Cluster
Oracle Internet Directory
SQL*Net
Oracle HTTP Server for Single Sign-On and Delegated Administration Services
OC4J for Single Sign-On and Delegated Administration Services
Web Cache
Oracle HTTP Server, including mod_oc4j
mod_plsql
OracleAS Metadata Repository
Product Metadata
Management Metadata
Security Metadata
AJP
SQL*Net
J2EE (without Web Cache)
Web Cache runs in the Web Server Tier DMZ.
SQL*Net
Intranet Firewall
Intranet
Real Application Clusters or Cold Failover Cluster
Customer Database
Business Data

Infrastructure DMZ

In this tier, you run all components of OracleAS Infrastructure 10g, except for Oracle Application Server Single Sign-On and Oracle Delegated Administration Services, which run in the Web Server Tier DMZ.

You install the OracleAS Infrastructure 10g behind another firewall so that Web servers do not have direct access to other computers in the enterprise. Oracle Application Server Metadata Repository and Oracle Internet Directory contain critical data used by Oracle Application Server instances.

OracleAS Metadata Repository contains security metadata, management metadata, and product metadata. J2EE and Web Cache instances and the infrastructure components such as Oracle Application Server Single Sign-On use this repository.

The Oracle Internet Directory contains data for external and internal users. Oracle Application Server Single Sign-On authenticates users based on the data in Oracle Internet Directory.

You can install the OracleAS Metadata Repository and the Oracle Internet Directory in a Real Application Clusters or Oracle Application Server Cold Failover Clusters environment.

J2EE Business Logic DMZ

In this tier, you deploy and run your applications on J2EE and Web Cache instances. The applications can access the business data in the customer database.

The number of J2EE and Web Cache instances and computers depend on the number of applications that you are running and the number of users. You should have at least two instances so that you can cluster them using OracleAS Clusters. Clustered instances provide greater availability and scalability, and improve performance.

The J2EE firewall prevents Web servers (in the Web Server Tier DMZ) from directly accessing the computers in this tier.

Intranet

This tier contains the computers that run enterprise processes, including databases that contain the business data. The databases can be in a high availability environment such as Real Application Clusters or Oracle Application Server Cold Failover Clusters. Applications running in the J2EE Business Logic tier can access the databases. If Web servers in the Web Server Tier DMZ become compromised, the intranet firewall prevents the Web servers from accessing the entire corporate intranet.

1.4 Enterprise Data Center Topology: Portal, Wireless, and Business Intelligence Applications

This deployment topology supports J2EE applications as well as applications that use components in the Portal and Wireless, and the Business Intelligence and Forms middle tiers. If you do not need these components, see Section 1.3, "Enterprise Data Center Topology: J2EE Applications", which describes a topology that uses only the components in the J2EE and Web Cache middle tier.

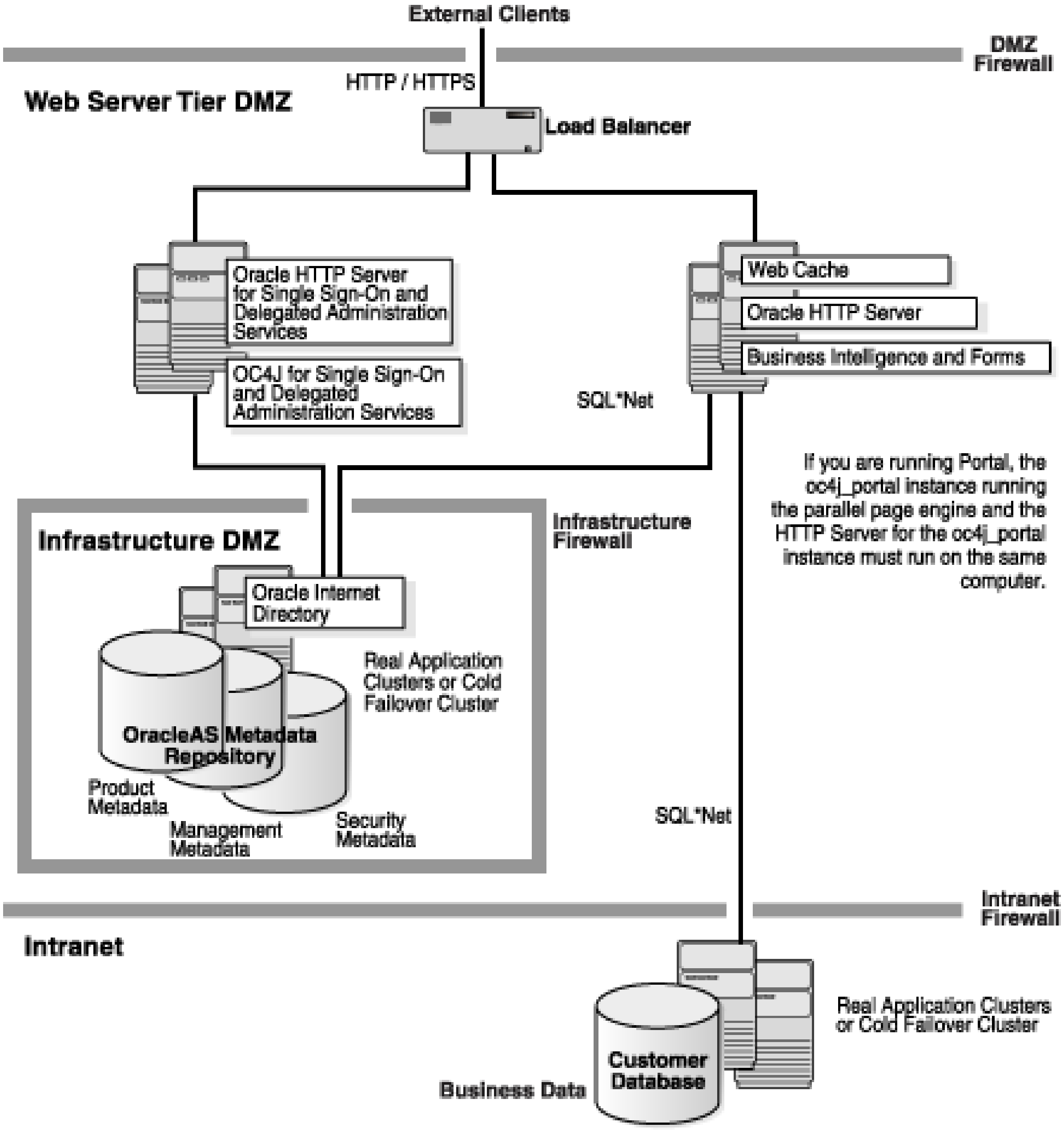
Target Users

This topology is intended for enterprises who have users internal as well as external to the organization. Requests from external users go through firewalls.

Description

This topology (Figure 1–3) distributes Oracle Application Server components over multiple computers and tiers. Access to the computers in each tier is guarded by firewalls. This distributed topology enables you to scale the number of computers in each tier (to increase performance and availability) without affecting computers in other tiers. For example, if you discover a bottleneck in the computers running your applications, you can add computers to the Web Server Tier DMZ and run Business Intelligence and Forms middle tiers on them.

Figure 1–3 Enterprise Data Center Topology: Portal, Wireless, and Business Intelligence Applications


External Clients
DMZ Firewall
HTTP / HTTPS
Web Server Tier DMZ
Load Balancer
Oracle HTTP Server for Single Sign-On and Delegated Administration Services
OC4J for Single Sign-On and Delegated Administration Services
Web Cache
Oracle HTTP Server
Business Intelligence and Forms
SQL*Net
If you are running Portal, the oc4j_portal instance running the parallel page engine and the HTTP Server for the oc4j_portal instance must run on the same computer.
Infrastructure Firewall
Infrastructure DMZ
Oracle Internet Directory
Real Application Clusters or Cold Failover Cluster
OracleAS Metadata Repository
Product Metadata
Management Metadata
Security Metadata
SQL*Net
Intranet Firewall
Intranet
Real Application Clusters or Cold Failover Cluster
Customer Database
Business Data

1.5 Departmental Topology

A departmental configuration topology is a subset of considerations and requirements that overlap the enterprise data center configuration.

Target Users

This topology is a smaller scale version of the topology described in Section 1.3, "Enterprise Data Center Topology: J2EE Applications". It consists of an OracleAS Infrastructure 10g with two metadata repositories, and multiple middle tiers. This topology can be used by individual departments within an organization. Users who access this topology are internal to the organization. As such, this topology does not consider security requirements that involve external users.

Description

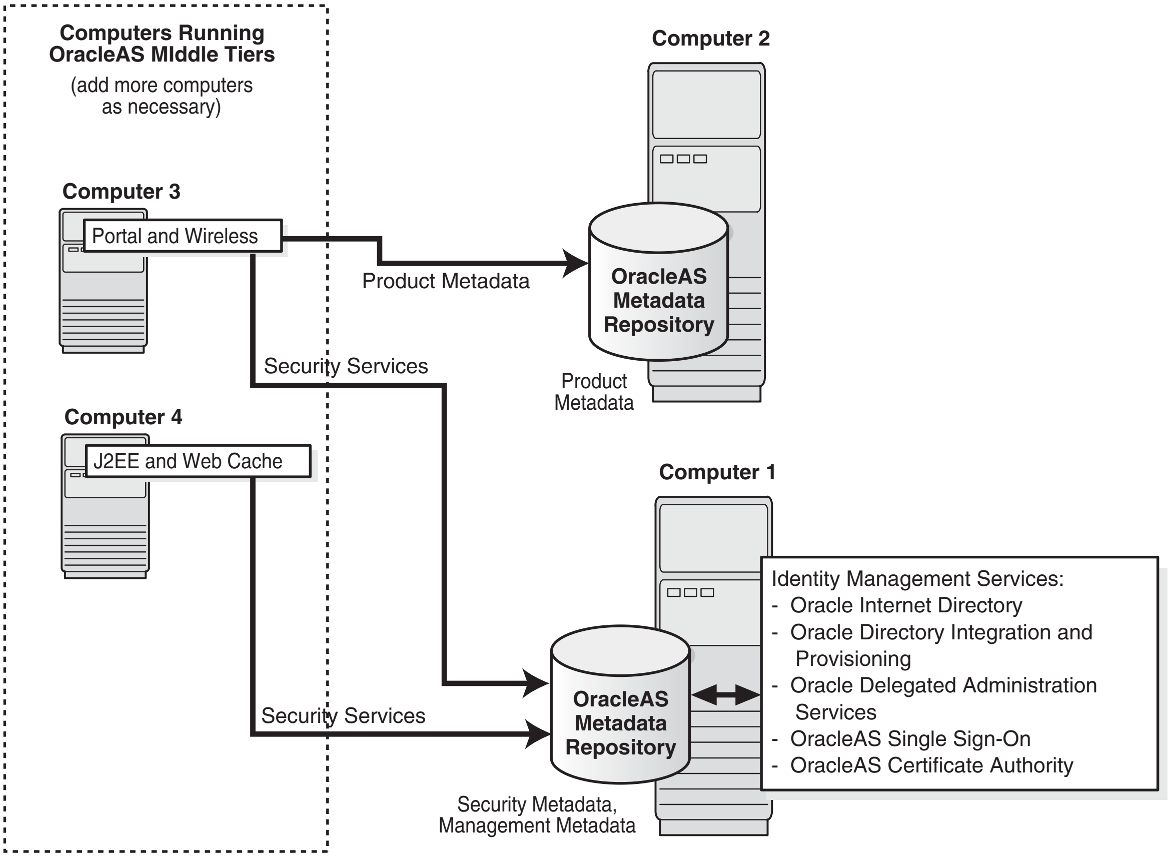
This topology (Figure 1–4) consists of an OracleAS Infrastructure, plus several middle tiers, including at least one Portal and Wireless middle tier. This topology uses two metadata repositories:

- one for product metadata (installed on computer 2). The Portal and Wireless middle tier uses this metadata repository.
- one for Identity Management services (installed on computer 1). All the middle tiers use this metadata repository for Identity Management services.

Expanding the Topology

You can install Oracle Application Server middle tiers on additional computers, as needed. You would associate these middle tiers with either metadata repository. For more information, see *Oracle Application Server 10g Administrator's Guide*.

Figure 1–4 Departmental Topology



Adding High Availability Features

You can install the infrastructure in a Real Application Clusters or Oracle Application Server Cold Failover Clusters environment. See Chapter 9, "Installing in High Availability Environments" in the *Oracle Application Server 10g Installation Guide* for specific steps.

This topology makes the following assumption:

- When you install the OracleAS Infrastructure 10g, you create a new Oracle Internet Directory.

1.5.1 Installation Sequence

Install the items in the following order. The computers are listed in Figure 1–4.

1. Computer 1: Install an OracleAS Infrastructure 10g with Identity Management services and OracleAS Metadata Repository. See Section 6.14, "Installing OracleAS Infrastructure 10*g*" in the *Oracle Application Server 10g Installation Guide* for specific steps.This creates a database to contain the OracleAS Metadata Repository. It also creates an Oracle Internet Directory.
2. Computer 2: Install a second OracleAS Metadata Repository. See Section 6.16, "Installing OracleAS Metadata Repository in a New Database" in the *Oracle Application Server 10g Installation Guide* for specific steps.When the installer prompts you to register the OracleAS Metadata Repository, enter the connect information for the Oracle Internet Directory created in step 1.The Portal and Wireless middle tier will use this second metadata repository for its product metadata. See Section 6.10, "Can I Use Multiple Metadata Repositories?" in the *Oracle Application Server 10g Installation Guide* for specific steps.
3. Computer 3: Install a Portal and Wireless middle tier. See Section 7.10, "Installing Portal and Wireless or Business Intelligence and Forms" in the *Oracle Application Server 10g Installation Guide* for specific steps.When the installer prompts for Oracle Internet Directory, enter the connect information for the Oracle Internet Directory created in step 1. This Oracle Internet Directory contains the registration for the OracleAS Metadata Repository installed in steps 1 and 2.When the installer prompts for the OracleAS Metadata Repository, select the OracleAS Metadata Repository installed in step 2.
4. Computer 4: Install a J2EE and Web Cache middle tier. See Section 7.8, "Installing J2EE and Web Cache with OracleAS Cluster and Identity Management Access" in the *Oracle Application Server 10g Installation Guide* for specific steps.When the installer prompts for Oracle Internet Directory, enter the connect information for the Oracle Internet Directory created in step 1.When the installer prompts for the OracleAS Metadata Repository, select the OracleAS Metadata Repository installed in step 1.

1.6 Development Life Cycle Topology

This topology is a combination of other topologies to support moving applications from test to stage to production environments:

Test environment: Application developers test their applications in their own environments. Examples of testing environments can be found in the *Oracle Application Server 10g Installation Guide*:

- Section 10.1, "Java Developer Topology"
- Section 10.2, "Portal and Wireless Developer Topology"
- Section 10.3, "Forms, Reports, and Discoverer Developer Topology"

Stage environment: Quality assurance personnel test all applications before deploying them to the production environment. In this environment, you can use the topology described in Section 1.5, "Departmental Topology". This topology in a stage environment runs applications from all departments, not just from a single one.

Production environment: Applications are ready for use by users internal and external to the enterprise. See Section 1.3, "Enterprise Data Center Topology: J2EE Applications"

1.6.1 Moving Applications from Test to Stage

To move applications from a test to a stage environment, you deploy them on middle tiers in the stage environment. The applications use the Identity Management and Oracle Application Server Metadata Repository of the stage environment.

If an application uses custom data in a database, you need to move that data from that database to a database in the stage environment.

1.6.2 Moving Applications from Stage to Production

You can move applications from a stage environment to a production by deploying the applications and moving any application-specific data from the stage environment to the production environment.

Another method is to use the rejoin feature, which enables you to unjoin a middle tier from its infrastructure and associate it with a different infrastructure. You can use this feature to move middle tiers (and their applications) from stage to production.

You still need to move application-specific data stored in a stage database to a database in the production environment.

Rejoining middle tiers is convenient if you need additional computers and application server resources for the production environment. In one step, you can add a computer that already has a middle tier and deployed applications.

See the *Oracle Application Server 10g Administrator's Guide* for details on rejoining middle tiers.

2

Installation and Configuration Considerations for an Enterprise Topology

The following sections contain installation and configuration considerations for these topologies:

- J2EE Applications Topology
- Enterprise Topology: Portal, BI, Wireless, Forms and Reports Services Installation and Configuration
- Departmental Topology: Departments Hosting Their Applications
- Enterprise Topology: Development Life Cycle Topology Installation and Configuration
- Enterprise Topology Post-Installation Tasks
- J2EE Applications Topology Post-Installation Tasks
- What to Read Next

2.1 J2EE Applications Topology

Table 2–1 summarizes considerations when installing and configuring a J2EE Applications topology in an enterprise environment such as a data center.

Table 2–1 Installation Considerations for the J2EE Application Developer Topology

Consideration	Deployment Scenarios
Install	Multiple Host installations on hardware clusters, NFS machines Multiple Middle Tier instances Dedicated Product Metadata Services for Portal applications Shared Product Metadata Services for some applications Shared Security Services for throughout the enterprise Central Management Services Support for Test to Stage to Production cycles Oracle Application Server won't break if there are hard disk replacements, CPU changes, or RAM upgrades

Table 2–1 (Cont.) Installation Considerations for the J2EE Application Developer

Consideration	Deployment Scenarios
Management	Central Management Services
	Oracle Application Server plugs into existing central management services
	Role-based management (initial functionality in 904 and major functionality in Oracle Application Server)
	Multiple administrators
	Backup and Recovery: Complete cold backup of the entire distributed environment
Security	Global OID/SSO or logical SSO (consisting of 1 or more SSO instances) sharing the same logical OID (consisting of 1 or more OID instances)
	Both SSO and OID behind the external firewall for internal users
	When hosting applications for both internal and external users (such as MOC), security considerations will need to make sure some security services can be shared by both users.
	Integrating with departmental third-party directories (iPlanet, Active Directory, eDirectory)
	Provisioning/De-Provisioning users
Application Deployment and Performance	J2EE applications deployed on Oracle Application Server Clusters with or without Web Cache
	Portal application using Web Cache, even on a single node environment
	Forms applications working against a OLTP System with no SSO
	BI applications working against a data warehouse with tighter security
	All applications accessible by Portal and Wireless devices
	Self Service Applications (using IP and Workflow)
High Availability (HA)	Infrastructure HA: Multiple types of HA solutions for different Infrastructure Services
	Optional: OPMN based cluster management for middle tier applications
Third-Party Products	Firewall, load balancers, hardware clusters, hardware accelerators

2.1.1 Hardware Requirements

You can look at Table 2–2 to get an idea of some of the hardware requirements you'll need to meet to successfully install, configure, and run various components of an enterprise deployment topology.

2.1.2 Installation Sequence

Install the items in the following order:

1. Infrastructure DMZ: Install an OracleAS Infrastructure 10g with Identity Management services and Oracle Application Server Metadata Repository. See Chapter 5, Section 5.14, "Installing OracleAS Infrastructure" in *Oracle Application Server 10g Installation Guide* for complete installation information.

> **Note:** Do not select Oracle Application Server Single Sign-On or **Oracle Delegated Administration Services** in the Select Configuration Options screen. You will install these components in the next step.

2. Web Server Tier DMZ: Install Oracle Application Server Single Sign-On and Oracle Delegated Administration Services.

   See "Installing Identity Management Components Only (Excluding Oracle Internet Directory)" in *Oracle Application Server 10g Installation Guide*. Note the following points:

   - In the Select Configuration Options screen, select only **Oracle Delegated Administration Services** and Oracle Application Server Single Sign-On.
   - When the installer prompts you for Oracle Internet Directory information, enter the connect information for the Oracle Internet Directory installed in step 1.

3. Web Server Tier DMZ: Install Business Intelligence and Forms (or Portal and Wireless) middle tier. This installs Oracle HTTP Server and OracleAS Web Cache as well.

   For more information, see Chapter 6, "Installing Portal and Wireless or Business Intelligence and Forms" in the *Oracle Application Server 10g Installation Guide*.

2.2 Enterprise Topology: Portal, BI, Wireless, Forms and Reports Services Installation and Configuration

The following table is a summary of the user considerations when installing and configuring Portal, BI, Wireless, and Forms and Reports

Table 2–2 Considerations when installing and configuring Portal, BI, Wireless, and Forms and Reports

Consideration	User Consideration
Overview	Web Server Tier: OHS stand alone installs on multiple machines Application Server Tier: Middle tiers hosted on one big machine or multiple machines for multiple applications Infrastructure: Dedicated or shared Product Metadata Services. Shared Security Service, Centralized Management Special Install Requirements: Cluster Machine installs Cloning, Reassociation: NFS Machine installs Hardware Cluster Support Co-existence of other Oracle Products: Oracle Application Server and Oracle Application Server Infrastructure in 2 different Oracle Home, IP Platform Build time environment in another Oracle Home Criteria for Best User Experience regarding Install: Easy to install and clone No patch requirements immediately after install Installations that can be easily cloned Flexible Distributed Infrastructure Services
Hardware Details	Web server tier/Application Server tier: Single big Host or farm of small machines for Middle tier Single big Host machine details: OS: Solaris (Of the order of E280’s or above) or HP or IBM AIX CPU: 2 – 4 (400Mhz or greater) RAM: 8G Hard Disk: 80GB Small machine details (min. 2-3, high end 6-8): OS: Linux, or Solaris or HP or IBM AIX CPU: 1 - 2 (400Mhz or greater for Solaris, 600Mhz or greater for Linux) RAM: 512M – 1G per node Hard Disk: 10 – 20 GB Infrastructure: OS: Solaris or HP or IBM AIX CPU: 1 – 2 CPU RAM: 512M - 1G Hard Disk: 10 – 20 GB

Table 2–2 (Cont.) Considerations when installing and configuring Portal, BI, Wireless, and Forms and Reports

Consideration	User Consideration
Distributed Install Topology	Web Server Tier: OHS in DMZ – 1, separate from application server. Application Server Tier: Application Server in DMZ – 2 Product Metadata Services: In DMZ – 2 for most cases. Dedicated host running just Product Metadata Services used by either dedicated or a small set of middle tier instances Security Services: Behind the firewall. Dedicated host running just Security Services. Shared by all middle tier instances Management Services: Central management inside the firewall
User Profile	System Administrator (Advanced User)

2.3 Departmental Topology: Departments Hosting Their Applications

Table 2–3 describes the considerations for installing and managing a departmental topology:

Table 2–3 Considerations for the Departmental Topology

Consideration	User Considerations
Installation and Management	Multiple Host installations on cluster machines, NFS machines Multiple Middle Tier instances used No Infrastructure used if deploying only Java or J2EE applications Dedicated Product Metadata Services for Portal applications Shared Product Metadata Services for some applications Shared Security Services to secure subset of enterprise level users Management Services -> Number of instances managed is less than enterprise data center. All other management issues are the same Oracle Application Server should not break if there are hard disk replacement, or CPU change or RAM upgrades or Network Interfaces
Security	Single install which would contain both Infrastructure Software and OID/SSO data Contains subset of users as compared to the enterprise OID
Application Deployment and Performance	Important not to pay overhead for enterprise configuration services Use OHS as load balancer for multiple OC4J instances. J2EE applications deployed on Oracle Application Server Clusters with or without Web Cache Portal application using Web Cache
High Availability (HA)	HA requirement for departmental deployment depends on the nature of the application If there is a requirement, recommendation would be Local Data Guard or Cold Failover ClusterIf there is no requirement, complete cold backup and recovery methodology is used

Table 2–3 (Cont.) Considerations for the Departmental Topology

Consideration	User Considerations
Third-Party Products	Depending on the load on the application, Load balancers might be needed

2.4 Enterprise Topology: Development Life Cycle Topology Installation and Configuration

Table 2–4 describes the installation and management considerations for the development life cycle topology:

Table 2–4 Considerations for the Development Life Cycle Enterprise Topology

Consideration	User Considerations
Install	Test Environment: Single host for mid tier and Infrastructure (all services from one DB). Staging Environment: Multiple mid tiers on one single big machine or multiple machines with either dedicated or shared product metadata services, but always shared security services. Production Environment: Very similar to Staging environment, except now using enterprise wide security service Oracle Application Server won't break when there are hard disk replacements, CPU changes, or RAM upgrades
Management	Test - Stand Alone or command line tools Development - Stand Alone or centralized management Production - Centralized Management
Security	Fluid Security requirements Re-association of security services is mandatory
Application Deployment and Performance	Shutdown/startup, deploy time are prioritiesFrequent reconfiguration of tunable parameters, needs to be fastMay have multiple versions installed and possibly runningThis is the environment for testing load balancing, combinations of applications on one box.
High Availability (HA)	Testing Environment: Not a concern. Applications and specific configuration files will be backed up. Staging Environment: Cold Failover Cluster or Local DG. Complete cold backup. Production Environment: RAC or Cold Failover Cluster and Remote DG for Disaster Recovery. Complete cold backup.
Third-Party Products	Depending on the load on the application, DMZ, firewalls, load balancers, routers might be needed.

2.5 Enterprise Topology Post-Installation Tasks

This section describes post-installation tasks you'll need to perform for these areas of your enterprise deployment topology:

- Infrastructure
- OracleAS Portal and Oracle Application Server Wireless
- Oracle Application Server Single Sign-On

2.5.1 Infrastructure

OracleAS Portal needs post-installation steps with Oracle Internet Directory and OracleAS Web Cache at the Infrastructure level.

2.5.1.1 OracleAS Portal and Oracle Internet Directory

Every OracleAS Portal middle-tier installation drops and recreates the Portal users in Oracle Internet Directory (OID). This means that the Oracle Application Server instance password of the last run middle-tier installation should be used for Portal runtime access.

After all the middle-tier installations are performed, users can change their Portal user passwords in OID. This does not require any other changes in the OracleAS Metadata Repository.

2.5.1.2 OracleAS Portal and OracleAS Web Cache

Detailed steps for setting up Oracle Application Server Web Cache in a multiple middle-tier environment are described in section 5.1.2 of the *Oracle Application Server Portal Configuration Guide*.

2.5.2 OracleAS Portal and Oracle Application Server Wireless

If Oracle Application Server Wireless is configured with OracleAS Portal during the middle-tier installation, the middle-tier install registers the Portal on the Oracle Application Server Wireless service. In case of multiple middle-tier installs, the last configured Oracle Application Server Wireless service URL is stored in the OracleAS Portal instance. You can change this to your choice of Oracle Application Server Wireless service by running the following scripts in the Oracle Application Server middle-tier selected for the Oracle Application Server Wireless service:

UNIX:

```
ORACLE_HOME/wireless/sample/portalRegistrar.sh
```

Windows:

```
ORACLE_HOME/wireless/sample/portalRegistrar.bat
```

Portal Provider UI Framework

Multiple Portal middle-tier installations overwrite the existing Default JPDK Instance URL that is used for creating the Providers. Users can change this to their choice of JPDK Instance URL using the following steps:

1. Log in to Portal using the browser.
2. Click on the Builder link.
3. Click the Administrator tab.
4. Click on Global Settings in the Services portlet.
5. Click the Configuration tab.
6. Enter the Default JPDK Instance URL of any installed Portal middle-tier.

See also: *Oracle Application Server Portal Configuration Guide*

2.6 J2EE Applications Topology Post-Installation Tasks

This section describes the post-installation tasks for the J2EE applications that are part of the Web Tier of an Enterprise Deployment Topology:

- Oracle Application Server Web Cache
- Oracle HTTP Server
- Oracle Application Server Forms Services
- Oracle Application Server Reports Services
- Oracle Application Server Discoverer
- Oracle Application Server Single Sign-On
- OracleAS Portal
- Oracle Enterprise Manager

2.6.1 Oracle Application Server Web Cache

Here is a post installation and configuration check list for OracleAS Web Cache.

1. Configure a Ping URL

   For Watchdog to check the health status of Web Cache, the configurable URL recommend being a cacheable. When a non-cacheable URL is configured, Web Cache will try to connect to the origin server. If the origin server is not responding with the time out from Watchdog, Watchdog will restart Web Cache.

2. Optimize connection limits

   The Application Server (origin server) connection limit and the Inbound Connection limit should be set to an optimum number.This number depends on the volume of traffic from client requests from OracleAS Web Cache to the origin server when it caches missed requests.

3. Physical memory

   To reduce disk swapping with objects in the cache, install enough memory for the cache. Oracle recommends a minimum of 256MB.

4. Set up apology pages (Network Error, Server Busy, and ESI Fragment)

   The default apology pages for network error, Origin server busy and ESI fragment may not match the format (look-and-feel) of the application.

5. Set up SSL Certificates

   To set up the client side SSL certificate:

   a. Create a new wallet with the Oracle Wallet manager

   b. Specify the new wallet in the Listen Ports page (Ports -> Listen Ports) of the OracleAS Web Cache Manager administrative interface.

   To set up the origin server (OS) SSL certificate:

   a. Create a new wallet with the Oracle Wallet manager

   b. Specify the new wallet in the Origin Servers, Sites, and Load Balancing page (Origin Servers, Sites, and Load Balancing -> Origin Server Wallet)

6. Set up Site Definitions (virtual hosting)

Site definitions enable Web Cache to apply different caching rules for different sites. Requests for different sites can also be routed to specific origin servers through Site-to-Server Mappings.

Site Definitions in Web Cache must match the visibly external host name. By default Web Cache takes on the default name and port numbers of the host it is installed on.

Alias definitions enable the mapping of multiple host names to a single site. For example, site www.company.com:80 may have an alias of company.com:80. By specifying the alias of company.com:80 for site www.company.com:80, Web Cache can cache the same content from either company.com:80 or www.company.com:80. Site and alias definitions also affect Error Pages configuration.

7. Logging

   Make sure to disable verbose event logging while Web Cache is running in normal mode. Verbose logging is for debugging purposes and is system-resource intensive.

   For more information, see Chapter 10, "Administering Oracle Application Server Web Cache", in Oracle Application Server Web Cache Administrator's Guide.

8. Invalidation Requests

   For advance invalidation request use the invalidation index option.

   For more information, see Chapter 10, "Administering Oracle Application Server Web Cache", in *Oracle Application Server Web Cache Administrator's Guide*.

2.6.2 Oracle HTTP Server

Be aware that you may need to make changes to the Oracle HTTP Server based on components and services that are reconfigured. See the appropriate sections in the respective component guide for configuration information.

2.6.3 Oracle Application Server Forms Services

There is no additional post-installation task to configure Oracle Application Server Forms Services. See chapter 8 of the Oracle Application Server Forms Services Deployment Guide for more information about how Oracle Application Server Forms Services works. You should also consult the *Oracle Application Server Forms Services Release Notes* for last minute issues and workarounds.

2.6.4 Oracle Application Server Reports Services

There is no additional post-installation task to configure Oracle Application Server Reports Services. You should also consult the *OracleAS Reports Services Release Notes* for last minute issues and workarounds.

2.6.5 Oracle Application Server Discoverer

In the Discoverer Configuration and Communications Protocols page, change the value from default to tunneling to work with the load balancer and the firewall.

2.6.6 Oracle Application Server Single Sign-On

If you are working with multiple Single Sign-on servers, you may need to perform additional configurations to the Oracle HTTP Server. See Chapter 3.3, "Multiple Single Sign-On Middle Tiers with One Oracle Internet Directory" for more information.

2.6.7 OracleAS Portal

Post-installation tasks for Oracle Portal include:

- Chapter 4.3, "Load Balancing Considerations"
- Chapter 4.4, "Configuring Multiple Middle-Tiers with a Load Balancing Router"
- Chapter 4.5, "Configuring Reverse Proxy Servers"

2.6.8 Oracle Enterprise Manager

Make sure that EM is only accessible within a firewall setup. Port 1814 must be open to the various tiers behind a firewall for Application Server Control to work correctly.

For more information about using Application Server Control to administer an enterprise deployment topology, see Chapter 5, "Managing an Enterprise Deployment Topology", and the *Oracle Enterprise Manager Advanced Configuration* guide.

2.7 What to Read Next

After installing Oracle Application Server, you should read the *Oracle Application Server 10g Administrator's Guide*. It contains an excellent chapter called "Getting Started After Installing Oracle Application Server".

If you plan to use any of the components listed in this chapter, you need to perform some steps specific to the component after installation before you can use the component. Table 2–5, " Component Configuration Guides" lists the component guides that describe the steps.

Table 2–5 Component Configuration Guides

Component	Guide That Describes the Post-Installation Steps
OracleAS Portal	*Oracle Application Server Portal Configuration Guide*
Oracle Application Server Forms Services	*Oracle Application Server Forms Services Deployment Guide* *Oracle Application Server Forms Services Release Notes*
Oracle Application Server Single Sign-On	*Oracle Application Server Single Sign-On Administrator's Guide*
Oracle Application Server Discoverer	*Oracle Application Server Discoverer Configuration Guide* **Note:** You can find this guide on the documentation CD-ROM for Oracle Developer Suite, not Oracle Application Server.
Oracle Application Server Reports Services	*Oracle Application Server Reports Services Publishing Reports to the Web*
OracleAS Web Cache	*Oracle Application Server Web Cache Administrator's Guide*
Oracle HTTP Server	*Oracle HTTP Server Administrator's Guide*

3 Configuring Single Sign-On in an Enterprise Deployment Topology

The following sections provide brief information and additional resources for OracleAS Single Sign-On in an enterprise deployment topology:

- About High Availability
- About Security
- Multiple Single Sign-On Middle Tiers with One Oracle Internet Directory

3.1 About High Availability

The availability of a system or any component in that system is defined by the percentage of time that it works normally. A system works normally when it meets its correctness and performance specifications.

You should become familiar with basic concepts of how high availability affects Oracle Application Server security features such as Oracle Internet Directory and OracleAS Single Sign-On.

For more information, see the *Oracle Application Server 10g High Availability Guide*.

3.2 About Security

Oracle Application Server provides a comprehensive security framework supporting all its components, as well as third-party and custom applications deployed on the application server. The framework is based on OracleAS Single Sign-On for authentication, Oracle Internet Directory for authorization and centralized user provisioning, Oracle HTTP Server for the Web server component, and the Oracle Application Server Java Authentication and Authorization Service (JAAS) provider for security in Java2 Enterprise Edition (J2EE) applications.

For complete information about security in Oracle Application Server, see the *Oracle Application Server 10g Security Guide*. Updated information can always be found on the Oracle Technology Network (OTN) at http://otn.oracle.com/.

Additionally, refer to the documentation for each component regarding security in that component.

3.3 Multiple Single Sign-On Middle Tiers with One Oracle Internet Directory

The simplest high availability scenario involves failover within the single sign-on instance itself, at the middle tier. Adding middle tiers increases scalability and therefore makes the single sign-on server more available.

In this configuration, a single HTTP load balancer is placed in front of two or more Oracle HTTP servers. At the backend is one directory server and one identity management infrastructure database. The purpose of the load balancer is to publish a single address to single sign-on partner applications while providing a farm of single sign-on middle tiers that actually service the application requests. The HTTP load balancer can detect when one of these Oracle HTTP server instances has failed and can then fail over requests to another instance.

3.3.1 Usage Scenario

The usage scenario presented here assumes the following hypothetical configurations:

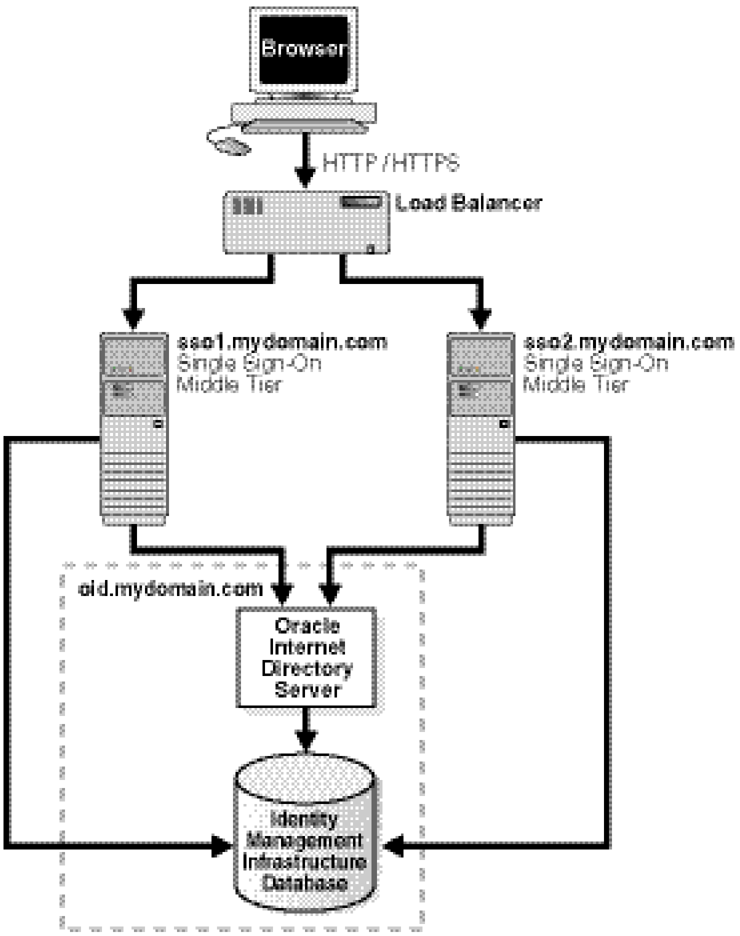
- The directory server and identity management infrastructure database are located at oid.mydomain.com.
- There are two single sign-on middle tiers. One is installed on host sso1.mydomain.com, IP address 138.1.34.172. The other is installed on sso2.mydomain.com, IP address 138.1.34.173. Both servers listen on non-SSL port 7777. Both are configured to use the directory and identity management infrastructure database located at oid.mydomain.com.
- The address of the single sign-on server that is published to partner applications is sso.mydomain.com, IP address 138.1.34.234. The HTTP load balancer is configured to listen on sso.mydomain.com, port 80. It load balances user requests between sso1.mydomain.com and sso2.mydomain.com.

Notes:

- In this scenario, the load balancer is listening on port 80, a non-SSL port number. If the load balancer is configured to use SSL to interact with the browser, a different port number must be selected. The default SSL port number is 443.
- In this scenario and the one immediately following, two single sign-on middle tiers are used. There can, in fact, be any number of middle tiers.

Figure 3–1 shows two single sign-on middle tiers configured to use a single instance of Oracle Internet Directory.

Figure 3–1 Two Single Sign-On Middle Tiers, One Oracle Internet Directory



3.3.2 Configuration Steps

Setting up the single sign-on system presented in Figure 3–1 involves the following tasks:

- Install the identity management infrastructure database, the directory server and the single sign-on servers
- Configure the Oracle HTTP servers on the single sign-on middle tiers
- Configure the HTTP load balancer
- Configure the identity management infrastructure database
- Reregister mod_osso on the single sign-on middle tiers

Install the identity management infrastructure database, the directory server and the single sign-on servers

1. Choose a single sign-on server name that will be published to partner applications. This will also be the address of the load balancer. In the scenario presented here, the address is sso.mydomain.com.
2. Install the Oracle Application Server infrastructure on oid.mydomain.com, choosing the option "Identity Management and Oracle Application Server

Metadata Repository." When presented with the component list for this installation type, choose Oracle Internet Directory only.

3. Install the Oracle Application Server infrastructure on the middle tiers sso1.mydomain.com and sso2.mydomain.com, again choosing the option "Identity Management and Oracle Application Server Metadata Repository."
4. When presented with the component list for this installation type, choose Oracle Application Server Single Sign-On only. When the Oracle Universal Installer asks you to name the directory server associated with these single sign-on instances, enter oid.mydomain.com.

> **Note:** The Oracle Application Server installer, by default, assigns port numbers from a range of numbers. If you want to assign a different port number to a component, see "Static Port Numbers" in *Oracle Application Server 10g Installation Guide*

Configure the Oracle HTTP servers on the single sign-on middle tiers

When a load balancer is placed between the user and the Oracle HTTP Server, the effective URL of the single sign-on server changes. The Oracle HTTP configuration file `httpd.conf` on both single sign-on middle tiers must be modified to reflect this change. This file can be found at `$ORACLE_HOME/Apache/Apache/conf`.

1. Add the following lines to the `httpd.conf` file on sso1.mydomain.com and sso2mydomain.com:

   ```
   KeepAlive off
   ServerName sso.mydomain.com
   Port 80
   ```

   This step configures the Oracle HTTP servers at the single sign-on middle tiers to listen at the externally published name, which, in the scenario presented, is sso.mydomain.com.

2. If you configure the HTTP load balancer to use SSL, configure mod_certheaders on both sso1.mydomain.com and sso2.mydomain.com. This module enables the Oracle HTTP Server to treat requests that it receives over HTTP as SSL requests. The sequence is as follows:

   a. In the `httpd.conf` file on both middle tiers, enter the following line:

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

   b. If you are using Oracle Application Server Web Cache as a load balancer, enter the following line:

   ```
   AddCertHeader HTTPS
   ```

   If you are using a hardware load balancer, enter the following line:

   ```
   SimulateHttps on
   ```

   c. Synchronize system clocks between both middle tiers.

   d. Execute the following command to update the Distributed Cluster Management (DCM) schema with the changes:

   ```
   $ORACLE_HOME/dcm/bin/dcmctl updateConfig -v -d
   ```

Configure the HTTP load balancer

The HTTP load balancer used can be hardware such as BigIP, Alteon, or Local Director or software such as Oracle Application Server Web Cache.

- Hardware Load Balancer

  If you are using a hardware load balancer, configure one pool of real servers with the addresses 138.1.34.172 and 138.1.34.173. Configure one virtual server with the address 138.1.34.234. This virtual server is the external interface of the load balancer. For instructions, consult the documentation provided by your load balancer vendor.

- Software Load Balancer

  If you are using Oracle Application Server Web Cache to load balance connection requests, see both of the following links:

  "Routing Single Sign-On Server Requests" and "Leveraging Oracle Identity Management Infrastructure" in Oracle Application Server Web Cache Administrator’s Guide.

Note: For optimal performance, use a hardware load balancer.

Configure the identity management infrastructure database

Run the script `ssocfg` on one of the single sign-on middle tiers. This script configures the single sign-on server to accept authentication requests from the externally published address of the single sign-on server. Using the example provided, the script would be executed in the following way:

- UNIX:

  ```
  $ORACLE_HOME/sso/bin/ssocfg.sh http sso.mydomain.com 80
  ```

- Windows NT/2000:

  ```
  %ORACLE_HOME%\sso\bin\ssocfg.bat http sso.mydomain.com 80
  ```

Note that the command example provides the listener protocol, host name, and port number of the load balancer as arguments. Recall that the load balancer address is the externally published address of the single sign-on server. If the load balancer is configured to use SSL, replace non-SSL port `80` with SSL port `443` and `http` with `https`.

After executing `ssocfg`, restart the single sign-on middle tiers:

```
$ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY
```

Finally, test the application:

```
http://sso.mydomain.com/pls/orasso
```

Reregister mod_osso on the single sign-on middle tiers

On both middle tier machines, reregister mod_osso as the partner application sso.mydomain.com.

To reregister mod_osso on sso1.mydomain.com:

1. On the computer sso1.mydomain.com, log in to the single sign-on administration pages as the single sign-on administrator. Be sure to log in to `http://sso.mydomain.com/pls/orasso`.

2. Use the Administer Partner Applications page to delete the existing entry for the partner application sso1.mydomain.com.
3. Set the environment variable `ORACLE_HOME` to point to the Oracle home for sso1.mydomain.com. Include `$ORACLE_HOME/jdk/bin` in the `PATH` variable.
4. Run the registration script. For the URLs, be sure to substitute values appropriate for your installation. The script creates a partner application called sso.mydomain.com.

   ```
   $ORACLE_HOME/jdk/bin/java -jar $ORACLE_HOME/sso/lib/ossoreg.jar
   -oracle_home_path orcl_home_path
   -site_name site_name
   -config_mod_osso TRUE
   -mod_osso_url mod_osso_url
   -u userid
   [-virtualhost virtual_host_name]
   [-update_mode CREATE | DELETE | MODIFY]
   [-config_file config_file_path]
   [-admin_id adminid]
   [-admin_info admin_info]
   ```

   For a description of command parameters, please see "Registering mod_sso" in Chapter 4 of the *Oracle Application Server Single Sign-On Administrator's Guide*.

To reregister mod_osso on sso2.mydomain.com:

1. On the computer sso2.mydomain.com, log in to the single sign-on administration pages as the single sign-on administrator. Be sure to log in to `http://sso.mydomain.com/pls/orasso`.
2. Use the Administer Partner Applications page to delete the existing entry for the partner application sso2.mydomain.com.
3. Create a clear text `osso.conf` file using the following steps:
   a. Click the Edit Partner Application Page for sso.mydomain.com.
   b. On the Edit Partner Application page, make a note of the parameters `sso_server_version`, `cipher_key`, `site_id`, `site_token`, `login_url`, `logout_url, and cancel_url`. You will use the same values that you used when you registered the application on sso1.mydomain.com. The idea is to maintain the same site id, site token, and cipher key between both middle tiers. This enables these servers to act as clones of each other.
   c. Create the `osso.conf` file, using a text editor:

      ```
      sso_server_version=v1.2
      cipher_key=encryption_key
      site_id=id
      site_token=token
      login_url=http://sso.mydomain.com/pls/orasso/orasso.wwsso_app_admin.ls_
      login
      logout_url=http://sso.mydomain.com/pls/orasso/orasso.wwsso_app_admin.ls_
      logout
      cancel_url=http://sso.mydomain.com:80/
      ```

4. Log in to sso2.mydomain.com as root; then navigate to the `osso.conf` file that you created in Step 3. Obfuscate the file:

   ```
   $ORACLE_HOME/Apache/Apache/bin/iasobf osso.conf $ORACLE_HOME/Apache/Apache/
   conf/osso/osso.conf
   ```

5. Restart the Oracle HTTP Server:

   ```
   $ORACLE_HOME/opmn/bin/opmctl restartproc type=ohs
   ```

6. Change the base URL for the Delegated Administration Service (DAS), using the oidadmin tool:

   a. Start the tool:

      ```
      $ORACLE_HOME/bin/oidadmin
      ```

   b. Log in to Oracle Directory Manager as `cn=orcladmin`.

   c. Navigate to the entry that contains the attribute `orcldasurlbase`:

      ```
      cn=OperationalURLs,cn=DAS,cn=Products,cn=OracleContext
      ```

   d. Change the attribute to the following value:

      ```
      http://sso.mydomain.com/
      ```

      Make sure that you include the backslash after the host name. When you click `useradmin` in a portal, the URL for `useradmin` is appended to this value.

7. Test the partner application `oiddas`:

   ```
   http://sso.mydomain.com/oiddas
   ```

4 Networking

The following sections contains networking considerations in an Oracle Application Server topology:

- Oracle Application Server Networking Overview
- Firewall Considerations: Opening the Right Ports
- Load Balancing Considerations
- Configuring Reverse Proxy Servers

4.1 Oracle Application Server Networking Overview

Oracle Application Server has several features to connect and manage the various parts of an enterprise deployment topology, including:

- Distributed Configuration Management (DCM)
- Oracle Process Manager and Notification (OPMN)
- LDAP and Oracle Internet Directory
- Enterprise Manager Server Control

4.1.1 Distributed Configuration Management (DCM)

DCM is a management framework that enables you to manage the configurations of multiple Oracle Application Server instances across an enterprise deployment topology. DCM consists of clients, a daemon, and a metadata repository.

DCM features enable you to:

- Manage clusters and farms of Oracle Application Server instances. Manage the configuration of individual components, such as Oracle Application Server Containers for J2EE instances, Oracle HTTP Server instances, and Oracle Process Management and Notification, or Java Authentication and Authorization Service.
- Perform cluster-wide Oracle Application Server Containers for J2EE application deployment, especially in Development Life Cycle topology.
- Manage versions of configurations with archive, save and restore, and import and export functions. You can automate some of these functions as part of routine systems maintenance.

dcmctl is the Distributed Configuration Management command-line utility. You can use it to manage configurations and deploy applications. Instructions on using dcmctl and complete descriptions of all commands are described in Chapter 2, "dcmctl Commands "in the *Distributed Configuration Management Reference Guide*.

All configuration and topology data is stored in the Distributed Configuration Management metadata repository, which may be part of the Oracle Application Server Metadata Repository.

For additional information on working with DCM, see the *Distributed Configuration Management Reference Guide*.

4.1.2 Oracle Process Manager and Notification (OPMN)

OPMN is installed and configured with every Oracle Application Server installation type and is essential for running Oracle Application Server.

OPMN features the following functionality:

- Provides a command-line interface for process control and monitoring for single or multiple Oracle Application Server components and instances.
- Provides an integrated way to manage Oracle Application Server components.
- Enables management of Oracle Application Server subcomponents and sub-subcomponents.
- Channels all events from different Oracle Application Server component instances to all Oracle Application Server components that can utilize them.
- Solves interdependency issues between Oracle Application Server components by enabling you to start and stop components in order.
- Enables customizing of enterprise functionality by using event scripts.
- Enables gathering of host and Oracle Application Server process statistics and tasks.
- Provides automatic restart of Oracle Application Server processes when they become unresponsive, terminate unexpectedly, or become unreachable as determined by ping and notification operations.
- Provides automatic death detection of Oracle Application Server processes
- Does not depend on any other Oracle Application Server component being up and running before it can be started and used.

The OPMN server should be started as soon as possible after turning on the host. OPMN must be running whenever OPMN-managed components are turned on or off.

Oracle Application Server components managed by OPMN should never be started or stopped manually. Do not use command line scripts or utilities from previous versions of Oracle Application Server for starting and stopping Oracle Application Server components. OPMN must be the last service turned off whenever you reboot or turn off your computer.

Use the Application Server Control and the opmnctl command line utility to start or stop Oracle Application Server components.

For more information about OPMN, see *Oracle Process Manager and Notification Server Administrator's Guide*

4.1.3 LDAP and Oracle Internet Directory

LDAP is a standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate.

Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralized management of information about dispersed users and network resources. It combines Lightweight Directory Access Protocol (LDAP) Version 3 with the high performance, scalability, robustness, and availability of Oracle9i.

For more information on working with LDAP and Oracle Internet Directory, see Oracle Internet Directory Administrator's Guide. Make sure your application developers read *Oracle Internet Directory Application Developer's Guide*.

4.1.4 Enterprise Manager Server Control

Oracle Enterprise Manager Application Server Control enables Web site administrators to configure Oracle Application Server instances, to monitor and optimize them for performance and scalability, and to respond proactively to problem conditions.

The Application Server Control allows administrators to stop and restart Oracle Application Server instances from the Oracle Application Server Instance Home Page. They can also modify the configuration settings based on performance statistics collected to improve performance and scalability or to address any problems.The Application Server Control provides performance metrics for each component in both tabular and chart formats so you can identify problem conditions at a glance. When you drill down on an Oracle Application Server, you can view the status, historical uptime statistics, and the current performance and availability for each Oracle Application Server instance.

Metrics vary from one component type to another, but typical metrics include:

- Up/down status
- Memory usage
- Error rate
- Start time
- Number of connections

4.2 Firewall Considerations: Opening the Right Ports

In a distributed installation of Oracle Application Server, such as an Enterprise Topology, you'll need to configure ports in the firewalls to allow Oracle Application Server services to work correctly. Specifically, you'll need to allow for:

- HTTP and HTTPS to be open for users (clients) to contact the web server
- Application servers (middle tier installations) to communicate with the Infrastructure (SQL*Net, ORCL-LDAP, ORCL-LDAP-SSL, ONS, OPMN)
- Application servers to databases, SQL*Net, and LDAP protocols if necessary
- Application servers to use ONS outbound
- Port 1814 for Enterprise Manager (for Infrastructure and middle tier installations) and for any other tools and services, such as LDAP ports.
- AJP to be opened for mod_oc4j to OC4J communications

> **Note:** Default ports may differ between operating systems (Solaris, Windows, and Linux). Use Application Server Control to discover and manage ports.

Oracle Enterprise Manager Application Server Control is the preferred way to track port information if default ports have been changed. For default port information refer to the default ports section of the Oracle Application Server 10g Administrator's Guide.

Firewall Stateful Inspection is not used between DMZ, mid-iers, and infrastructure and Oracle recommends that FSI be used in the external internet interface.

For information about configuring and managing firewalls, see your administrator or the documentation for your firewall implementation.

4.2.1 mod_oc4j and OC4J in Different Tiers and Across Firewalls

mod_oc4j is located within Oracle HTTP Server and (1) identifies the requests it needs to act on, (2) determines which OC4J to route those requests to, and (3) communicates with that process. Mod_oc4j now extracts some relevant parameters (for example SSL information, certain environment variables, etc.) and forwards them to OC4J, using AJP13 protocol.

mod_oc4j analyzes the response from OC4J and takes appropriate actions, for example, if a Single Sign-On redirect is required.

By default, OPMN processes on all Oracle Application Server instances in the farm notify each other of the up/down status of OC4J within their instance. In turn, every OPMN also notifies its local mod_oc4j of changes in the OC4J status on all machines within the cluster. This allows mod_oc4j to keep its routing table updated, without any intervention from an administrator.

4.2.2 Opening the Right Ports for mod_oc4j

As a security practice, you can place mod_oc4j in one tier (usually in a DMZ tier) and have it communicate with OC4J processes that are located in another tier (usually another DMZ tier). Since mod_oc4j uses AJP to communicate to other OC4J instances, it is important to have the correct ports opened for AJP and OPMN.

For more information about OC4J architecture, see the whitepaper Oracle9i Application Server: mod_oc4j Technical Overview at http://otn.oracle.com/products/ias/ohs/collateral/r2/mod_oc4j_wp.pdf.

4.2.3 Configuring iASPT

The Application Server 10*g* Port Tunneling (iASPT) feature reduces the number of ports required to communicate to multiple OC4J processes to one. The iASPT process acts as a communication concentrators for connections between Oracle HTTP Server (OHS) and the Java virtual machine (JVM). (OHS) does not connect directly to the servlet engines, instead, OHS connects to an iASPT. iASPT then forwards communication on to the servlet engine. Each iASPT routes requests to multiple servlet engines. By doing this concentration of connections, you're only required to open one port per iASPT process on the internal firewall DMZ rather than one port per OC4J container.

As part of configuring iASPT, you'll need to need to tell iASPT where mod_oc4j lives and where the OC4J containers are. There are several directives to add in mod_oc4j, such as wallet files and their passwords. On the server containing the target OC4J instance, you'll need to configure opmn.xml and set the iASPT status to enabled, as well as specify the port or range of ports use. Finally, modify iaspt.conf to validate for the correct location of wallet and port information.

For complete information on configuring iASPT, see Chapter 10 of *Oracle HTTP Server Administrator's Guide*.

4.3 Load Balancing Considerations

In a configuration where there is a pool of applications servers (called a resource pool), and a pool of Single Sign-On servers, you'll need to add a virtual IP address to the load balancers (either software or hardware) then add pools to the virtual IP addresses. The application server pool needs to have persistence specified. Often, this is an active HTTP cookie setting in the software or hardware configuration page in the load balancer. See your administrator or documentation for your load balancer.

With SSL, cookies are problematic because of how encryption works. Often, you'll need to use the SSL session ID to specify persistence in your load balancer. Chapter 5 of *Oracle Application Server Portal Configuration Guide* contains extensive information on load balancing. Some of that information is presented in the following section.

4.4 Configuring Multiple Middle-Tiers with a Load Balancing Router

This section describes how you can set up multiple middle-tiers, front-ended by a load balancing router (LBR) to access the same OracleAS Metadata Repository.

The purpose of a Load Balancing Router (LBR) is to provide a single published address to the client tier, and front-end a farm of servers that actually service the requests, based on the distribution of the requests done by the LBR. The LBR itself is a very fast network device that can distribute Web requests to a large number of physical servers.

Let us assume that we want to configure the multiple middle-tier configuration, shown in Figure 4–1. In the example, we show OracleAS Web Cache on the same machine as the Portal and Wireless middle-tier, although they can theoretically be on different machines.

Figure 4–1 Multiple Middle-Tier Configuration with Load Balancer

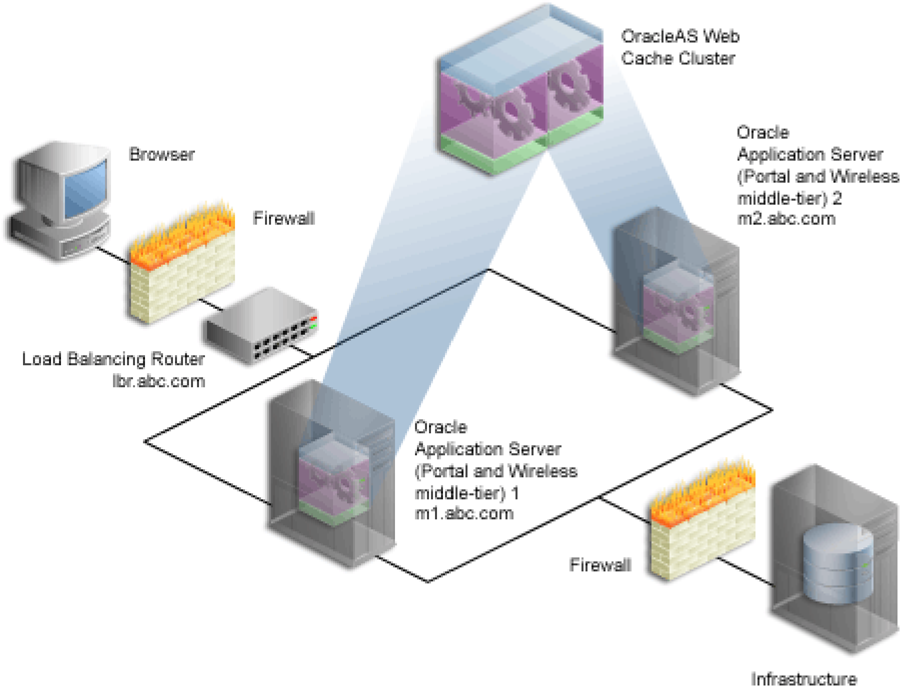

OracleAS Web Cache Cluster
Browser
Firewall
Oracle Application Server (Portal and Wireless middle-tier) 2 m2.abc.com
Load Balancing Router lbr.abc.com
Oracle Application Server (Portal and Wireless middle-tier) 1 m1.abc.com
Firewall
Infrastructure

Table 4–1 Additional information About the Graphic

Machine	Details
Load balancing router	Machine Name: `lbr.abc.com` IP Address: `L1.L1.L1.L1` Listening Port: `80` Invalidation Port: `4001` (accessible only from inside)
Oracle Application Server (Portal and Wireless middle-tier) 1	Machine Name: `m1.abc.com` IP Address: `M1.M1.M1.M1` Oracle HTTP Server Listening Port: `7778` OracleAS Web Cache Listening Port: 7777 OracleAS Web Cache Invalidation Port: 4001
Oracle Application Server (Portal and Wireless middle-tier) 2	Machine Name: `m2.abc.com` IP Address: M2.M2.M2.M2 Oracle HTTP Server Listening Port: 7778 OracleAS Web Cache Listening Port: 7777 OracleAS Web Cache Invalidation Port: 4001

To understand how to configure OracleAS Portal with LBR, it is important to understand the internal architecture of Portal:

- The Parallel Page Engine (PPE) in Portal makes loopback connections to Oracle Application Server Web Cache for requesting page metadata information. In a default configuration, OracleAS Web Cache and the OracleAS Portal middle-tier are on the same machine and the loopback is local. When Oracle Application Server is front-ended by an LBR, all loopback requests from the PPE will start contacting OracleAS Web Cache through the LBR. Assume that the OracleAS Portal middle-tier and OracleAS Web Cache are on the same machine, or even on the same subnet. Then, without additional configuration, loopback requests result in network handshake issues during the socket connection calls.

- In order for loopbacks to happen successfully, you must set up a Network Address Translation (NAT) bounce back rule in the LBR, which essentially configures the LBR as a proxy for requests coming to it from inside the firewall. This causes the response to be sent back to the source address on the network, and then forwarded back to the client.

- OracleAS Portal leverages OracleAS Web Cache to cache a lot of its content. When cached content in OracleAS Web Cache changes, OracleAS Portal sends Web Cache invalidation requests from the database to OracleAS Web Cache. OracleAS Portal can only send invalidation messages to one Web Cache node. In an OracleAS Web Cache cluster, Portal relies on one OracleAS Web Cache member to invalidate content in the other member of the cluster.

- When *Oracle Application Server* is front-ended by an LBR, the LBR must be configured to accept invalidation requests from the database and balance the load among the cluster members.

Note: You will notice that the infrastructure is behind the LBR. The infrastructure can be one host, or distributed over multiple hosts. In order to configure the infrastructure properly, refer to the Chapter titled "Advanced Configurations" in the *Oracle Application Server Single Sign-On Administrator's Guide*

To configure the server so that the PPE loops back to the LBR for the loopback connections, you must perform the following steps:

Install a Single Portal and Wireless Middle-Tier

- Step 1: Install a Single Portal and Wireless Middle-Tier (M1)
- Step 2: Configure OracleAS Portal on M1 to Be Accessed Through the LBR
- Step 3: Confirm That OracleAS Portal is Up and Running
- Step 5: Configure the New Middle-Tier (M2) to Run Your Existing Portal

  For complete information about these steps, see Chapter 5 of the *Oracle Application Server Portal Configuration Guide*.

See Also: For information on the platform used, see *Oracle Application Server 10g Installation Guide*.

4.5 Configuring Reverse Proxy Servers

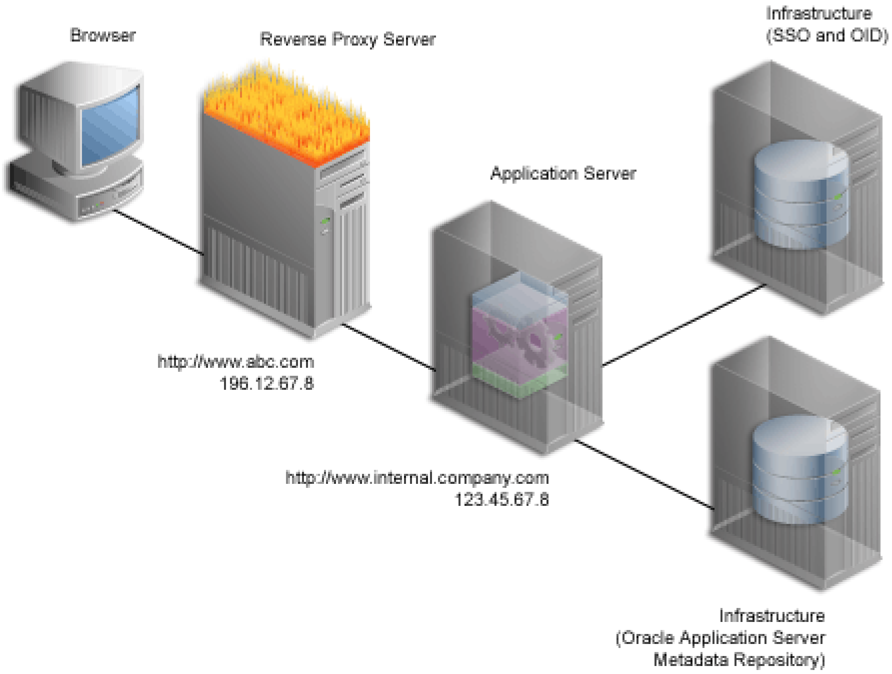
A reverse proxy server is a host process that is used as part of a firewall architecture to isolate the internal hosts from the externally accessible host(s). It does this by providing a proxy through which external requests must pass to access internal services. Typically, a proxy server takes the form of a dual-homed host. This means that it is a host with two network interface cards. One interface connects to the external network, and the other interface connects to the internal network, or demilitarized zone (DMZ) of the firewall.

Figure 4–2 shows an architecture in which the browser accesses the server through the hostname that is published by the proxy server. The proxy server then forwards the request to the actual host within the firewall.

For this example, we will assume that you have properly configured the OracleAS Single Sign-On server to work with the reverse proxy server.

See Also: Chapter 9, "Deploying Oracle Application Server Single Sign-On with a Proxy Server" in the *Oracle Application Server Single Sign-On Administrator's Guide.*

Figure 4–2 Internet Configuration with Reverse Proxy Server



For this example, let’s assume the following:

- The published address is www.abc.com.
- Internal to the firewall, the server name for the Oracle Application Server middle-tier is internal.company.com. This Application Server middle-tier machine hosts contains both OracleAS Web Cache, as well as the Oracle HTTP Server.
- Externally, the server is addressed with the default port 80; however, internally, the internal.company.com is listening on port 7777.

Information to complete these steps to configure OracleAS Portal for the architecture shown in Figure 4–1 can be found in Chapter 5 of the Oracle Application Server Portal Configuration Guide.

You’ll find additional information about how to set up proxy servers in the paper "A Primer on Proxy Servers," on Portal Center, http://portalcenter.oracle.com. Click the Search icon in the upper right corner of any Portal Center page.

5 Managing an Enterprise Deployment Topology

This chapter provides information on managing an enterprise deployment:

- General Management Considerations
- Enterprise Data Center Topology: Multiple Departments Sharing the Same Data Center
- Departmental Topology: Departments Hosting Their Applications
- Development Life Cycle Topology

5.1 General Management Considerations

Regardless of the type of topology you are managing, here are some general considerations:

- Rotating Log Files
- Periodic Restarting of OC4J
- Starting and Stopping Servers and Applications
- Rolling Out Upgrades, Patches, and Configuration Changes
- Backup and Recovery
- Taking Advantage of NFS
- Port Management
- Using Static and Dynamic IP Addresses
- Mining Log Files
- Leaving and Joining Different Infrastructures

5.1.1 Rotating Log Files

Many services and components generate their own log files that need to be maintained regularly. This need for maintenance varies on the size and scale of an enterprise topology.

Log files in Oracle Application Server have a maximum limit of 2 gigabytes before application server performance becomes adversely affected. You need to make sure that log files are archived and reset before they near the 2 gigabyte limit. This task may have to be performed daily or several times per week.

One way of managing log files is by using a "waterfall" approach, i.e. working on one server or component at a time during non-peak load times. This approach allows a data center to maintain high availability when a server is taken off-line, or when it is not brought down properly. Then, when that server or component has restarted, you can bring down the next server for log file maintenance, for example, one hour later.

You can also automate these tasks with "chron" jobs as a way to ensure this task is done. For more information, see the *Oracle Application Server 10g Administrator's Guide*.

5.1.2 Periodic Restarting of OC4J

For increased performance of OC4J, Oracle recommends regular restarting of OC4J. Sometimes memory leaks from applications or from the virtual machine (VM) within OC4J itself can degrade application server performance. You determine how often you need to restart OC4J based on daily observation and if automatic restarting does not happen. Your business needs may also affect how often you'll have to restart OC4J.

5.1.3 Starting and Stopping Servers and Applications

Starting and stopping servers and any applications depends on which servers are involved and the needs of users and the applications they use. Starting and stopping servers and applications can be automated through shell scripts and chron jobs as necessary.

When implementing automated starting and stopping of servers, you should take into account any applications that need to be started with the server. You should also consider the effects on high availability while a server is brought down for restarting, or if a server or application fails to start correctly.

You can also plan stopping and restarting procedures on a tier-by-tier basis. For example, you may only need to restart the application server, but not the database, in the case of rolling out patches.

5.1.4 Rolling Out Upgrades, Patches, and Configuration Changes

When rolling out configuration changes for upgrade and patching purposes, you do it once for each virtual host in httpd.conf. For information on configuring httpd.conf, see *Oracle HTTP Server Administrator's Guide*.

5.1.5 Backup and Recovery

You can use the Archive feature in Oracle Application Server as part of the disaster and backup and recovery strategies for your enterprise topology. Possible daily strategies include:

1. Making a complete operating system TAR of the entire code tree.
2. Backup of the file repository (database) for all installation types.

You can also use archives in a development environment where a new server comes online and you need data for research and development.

Your actual backup and recovery strategies should also take into account your business needs and security issues.

5.1.6 Taking Advantage of NFS

You can take advantage of NFS in your data center to:

- Keep static content on NFS partitions and mount it as needed to a server or application as needed
- Deploy static content quickly
- Resynch data across an enterprise topology quickly (sometimes minutes versus hours without NFS)

5.1.7 Port Management

Sometimes it can get difficult to track ports and port conflicts in a large enterprise topology, especially when specialized port configurations are implemented. It can also be difficult to figure out what the next available port to assign is.

You can associate many ports with one IP address as necessary.

Use Oracle Enterprise Manager to view information and manage port usage in your enterprise topology.

5.1.8 Using Static and Dynamic IP Addresses

Choosing and using static and dynamic IP addresses can be influenced by:

- The virtual IP structure in your enterprise topology
- How the hardware or software load balancer controls IP addressing
- Firewall configurations and implementations

5.1.9 Leaving and Joining Different Infrastructures

A new feature in Oracle Application Server is the ability to reassociate a middle tier with a new SSO/OID instance (infrastructure).

For example, you could point a middle tier instance to an SSO/OID instance that is strictly for development purposes, allowing you to develop, test, or upgrade before rolling out, then reassociate that middle tier to its original SSO/OID instance. For more information about joining or leaving an infrastructure, see *Oracle Application Server 10g Administrator's Guide*.

The following sections provide information that is relevent to the type of topology you may be managing.

5.1.10 Mining Log Files

Mining the log files in an enterprise topology has several advantages:

- Assists development teams in debugging before deploying to production environments
- Provides security information such as hacker attempts
- Provides information about errors at many different levels
- Provides information about automated processes

5.2 Enterprise Data Center Topology: Multiple Departments Sharing the Same Data Center

The following sections describe considerations for managing an enterprise deployment topology:

5.2.1 Management Considerations Checklist

- Use the monitoring and alerting capabilities of Oracle Enterprise Manager to ensure you are notified of any potential performance problems in your system(s). Use the default alerting thresholds or configure custom thresholds if needed for monitoring and alerts. Use historical data collected by Oracle Enterprise Manager to specify baselines for thresholds.
- Create Web applications for monitoring availability and response for applications deployed.

5.2.2 Oracle Enterprise Manager Application Server Control Checklist

Use Oracle Enterprise Manager Application Server Control for application server administration. It's installed automatically with the application server. You access this console from the Administer link in the Application Server Control.

Use Oracle Enterprise Manager Application Server Control for:

- Starting and Stopping components as needed
- Enable/Disabling unused components so they do not consume system resources
- Setting or changing configuration parameters for any of the application server components
- Deploying and configuring applications
- Managing application security
- Monitoring application and component performance and resource consumption in real-time
- Viewing and setting ports
- Browsing and searching log files
- Managing infrastructure schemas
- Command line utilities are available for scripting and automation.

5.2.3 Backup and Recovery Consideration

- Complete cold backup of the entire distributed environment.

5.2.4 Application Deployment and Performance Considerations

Use this checklist to ensure that:

- J2EE applications are deployed on Oracle Application Server clusters with or without Web Cache
- Portal application are using Web Cache, even on a single node environment
- Forms applications are working against an OLTP system with no Single Sign-On

- Business Intelligence (BI) applications are working against a data warehouse with tighter security
- All applications are accessible by Portal and Wireless devices
- Self Service Applications are using IP and Workflow

5.3 Departmental Topology: Departments Hosting Their Applications

The following sections describe considerations for managing a departmental topology:

- Management Considerations
- Backup and Recovery Consideration
- Application Deployment and Performance Considerations

5.3.1 Management Considerations

- Use the monitoring and alerting capabilities of Enterprise Manager to ensure you are notified of any potential performance problems in your system. Use the out-of-box alerting thresholds or configure custom thresholds if needed for monitoring and alerts. Use historical data collected by Enterprise Manager to specify baselines for thresholds.
- Create Web Applications for monitoring availability and response for applications deployed.
- Use Oracle Enterprise Manager Application Server Control for application server administration. Oracle Enterprise Manager Application Server Control is installed automatically with the application server.

  Use the Oracle Enterprise Manager Application Server Control for these tasks:

  - Starting and Stopping components as needed
  - Enable/Disabling unused components so they do not consume system resources
  - Setting or changing configuration parameters for any of the application server components
  - Deploying and configuring applications
  - Managing application security
  - Monitoring application and component performance and resource consumption in real-time
  - Viewing and setting ports
  - Browsing and searching log files
  - Managing infrastructure schemas
  - Command line utilities are available for scripting and automation

5.3.2 Backup and Recovery Consideration

- Complete cold backup of the entire distributed environment.

5.3.3 Application Deployment and Performance Considerations

- OHS used as load balancer for multiple OC4J instances

- J2EE applications deployed on Oracle Application Server clusters with or without Web Cache
- Portal applications using Web Cache
- Monitor application performance and availability using the Oracle Enterprise Manager Application Server Control.

5.4 Development Life Cycle Topology

Test Environment: For application server installation use Oracle Enterprise Manager Application Server Control. For standalone components use command line tools.

Staging Environment: For application server installation use Oracle Enterprise Manager Application Server Control. For standalone components use command line tools.

Production Environment: For application server installation use Oracle Enterprise Manager Application Server Control. For standalone components use command line tools.

6

Performance and Tuning Considerations

The most important factor in optimizing the performance of your enterprise deployment topology is understanding how to monitor its behavior and resource usage. Oracle Application Server provides several tools to help. See *Oracle Application Server 10g Performance Guide* for more information on how to monitor your installation. In addition, most hardware vendors supply a number of tools to monitor hardware resource usage.

This chapter contains the following reference information to help you tune your deployment topology's performance.

- Origin Server (OS) Network Parameters
- Oracle HTTP Server (OHS)
- SSL
- Oracle Internet Directory (OID)
- JVM parameters
- JSPs
- Web Cache
- Logging Level
- Database Connections
- Portal

6.1 Origin Server (OS) Network Parameters

Ensure that your OS network parameters have been set for performance and that you have sufficient network capacity. See the *Oracle Application Server 10g Performance Guide* for more information.

6.2 Oracle HTTP Server (OHS)

Understand how to use the MaxClients parameter for OHS to control concurrency for your Application Server configuration. Understand when to use persistent connections with OHS (keep alive) and how long to maintain a persistent connection. Each persistent connection will use an Apache child process (on Unix). See the *Oracle Application Server 10g Performance Guide* for more information.

6.3 SSL

Remember that the use of SSL can add substantial performance overhead and use it appropriately. The first request in an SSL session takes more longer than subsequent requests. You should also understand how to configure session duration for SSL. See the *Oracle Application Server 10g Performance Guide* and *Oracle Application Server Certificate Authority Administrator's Guide* for more information

6.4 Oracle Internet Directory (OID)

When using OID, use LDAP caching. you can also improve your performance with jazn-xml if it is sufficient for your security requirements. See these guides for more information;

- *Oracle Application Server 10g Performance Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle Application Server 10g Security Guide*

6.5 JVM parameters

Set the appropriate Java Virtual Machine (JVM) parameters for your Java application and your platform. Use the most recently certified JVM if possible. For example, JDK 1.4.1 is faster than JDK 1.3.1 in Oracle Corporation's tests. See *Oracle Application Server 10g Performance Guide* for more information.

6.6 JSPs

You can improve JSP performance by disabling timestamp checking and disabling session generation if they are not required.

6.7 Web Cache

Using of Web Cache can dramatically improve the performance of your application. Evaluate your application for caching potential. Provide sufficient memory and network bandwidth for Web Cache and use the fastest CPU possible. The increase in throughput that is achievable with Web Cache can make network bandwidth the primary bottleneck.

For more information, see *Oracle Application Server Web Cache Administrator's Guide*.

6.8 Logging Level

By default, Oracle Application Server components have been set to logging levels appropriate for a production system. More detailed logging can be enabled to provide additional information, but will add performance overhead to your system. Reserve the use of debug log levels for troubleshooting.

6.9 Database Connections

Several Oracle Application Server components provide database connectivity and allow you to tune the number of database connections maintained and the duration of database sessions. See *Oracle Application Server 10g Performance Guide* for more information on tuning database connections and working with JDBC and PL/SQL metrics.

6.10 Portal

For portal installations with high usage, you can increase the concurrency of the Portal Parallel Page Engine. However, if your system(s) lack sufficient resources to handle the increased concurrency, this can have a negative impact on your overall performance.

Index