Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle WebCenter Interaction

10*g* Release 4 (10.3.3.0.0)

E26810-01

December 2011

Provides an information on planning and implementing an Oracle WebCenter Interaction deployment, and describes how to define administrative roles, stage deployments, and provision hardware.

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Interaction, 10*g* Release 4 (10.3.3.0.0)

E26810-01

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents ix
Conventions x

1 Enterprise Deployment Overview

1.1 Oracle WebCenter Interaction Architecture 1-1
1.1.1 Oracle WebCenter Interaction Components 1-1
1.1.1.1 Portal 1-1
1.1.1.2 Document Repository 1-1
1.1.1.3 Search 1-1
1.1.1.4 Automation Service 1-1
1.1.1.5 Image Service 1-2
1.1.1.6 ALUI Directory 1-2
1.1.1.7 Common Notification Service 1-2
1.1.2 Portal Features 1-2
1.1.2.1 Experience Definitions 1-2
1.1.2.2 Knowledge Directory 1-2
1.1.3 Oracle WebCenter Analytics 1-2
1.1.4 Oracle WebCenter Collaboration 1-2
1.1.5 Oracle WebCenter Portal's Pagelet Producer 1-2
1.1.6 Oracle WebCenter BPM Workspace Extensions 1-2
1.1.7 Developer Tools 1-2
1.1.7.1 Oracle WebCenter Interaction Development Kit (IDK) 1-3
1.1.7.2 Oracle WebCenter WSRP Producer for .NET 1-3
1.1.8 Integration Services 1-3
1.1.8.1 Documentum 1-3
1.1.8.1.1 Oracle WebCenter Interaction Content Service for Documentum 1-3
1.1.8.2 IBM/Lotus Notes 1-3
1.1.8.2.1 Oracle WebCenter Interaction Content Service for Lotus Notes 1-3
1.1.8.3 LDAP 1-3
1.1.8.3.1 Oracle WebCenter Interaction Identity Service for LDAP 1-3
1.1.8.4 Microsoft 1-4
1.1.8.4.1 Oracle WebCenter Interaction Content Service for Windows Files 1-4

1.1.8.4.2 Oracle WebCenter Interaction Identity Service for Active Directory 1-4
1.1.8.4.3 Oracle WebCenter Interaction Content Service for Microsoft Exchange 1-4
1.1.8.4.4 Oracle WebCenter Console for Microsoft SharePoint.................................... 1-4
1.2 Oracle WebCenter Interaction Deployment Documentation 1-4
1.2.1 Other Documentation 1-4
1.2.1.1 Product Documentation 1-5
1.2.1.2 Online Help 1-5
1.2.1.3 Development Documentation.. 1-5

2 Planning Portal Structure and Content

2.1 Single Portals and Federated Portals 2-1
2.2 Experience Definitions 2-2
2.3 Communities 2-2
2.3.1 Business Unit Resource Center (Line of Business Communities)................................ 2-3
2.3.2 Interactive Workspace (Collaborative Communities).. 2-3
2.3.3 Customer or Partner Management Site (Sales and Service-Oriented Communities) 2-4
2.3.4 Dashboards (Analytic Communities) 2-4
2.3.5 Business Process Applications (Process Communities)... 2-5
2.4 Portlets... 2-5
2.5 Oracle WebCenter Interaction Search 2-6
2.5.1 Searchable Content 2-6
2.5.2 Grid Search 2-7
2.5.2.1 Grid Search Best Practices 2-7

3 Provisioning Computers

3.1 Component Host Requirements 3-1
3.2 Optimization Strategies.. 3-7
3.3 Evaluating Hardware Requirements for the Portal 3-8
3.4 Portal Performance on Various Hardware Hosts 3-9
3.4.1 Pages per Second on Oracle WebCenter Interaction 10.3.0 3-10

4 Migration and Staging

5 Securing Oracle WebCenter Interaction

5.1 Determining Your Security Needs 5-1
5.1.1 Understand Your Environment.. 5-1
5.1.2 Hire Security Consultants or Use Diagnostic Software 5-2
5.1.3 Read Security Publications.. 5-2
5.2 Security Architecture.. 5-2
5.2.1 Component Communication.. 5-2
5.2.2 Oracle WebCenter and the DMZ.. 5-3
5.3 Ensuring the Security of Your Production Environment.. 5-4
5.3.1 Securing the Oracle WebCenter Hosts 5-4
5.3.2 Securing Your Database.. 5-5
5.4 Configuring SSL 5-5
5.4.1 Security Modes.. 5-6

5.4.2 Configuring Oracle WebCenter for SSL 5-6
5.4.3 Importing CA Certificates 5-7
5.4.3.1 Importing CA Certificates Into a Java Application Server or Standalone Oracle WebCenter Product 5-8
5.4.3.2 Importing CA Certificates into IIS and .NET 5-8
5.4.4 Configuring Oracle WebCenter Applications to Use a Secure Portal or Image Service ... 5-9
5.4.4.1 Configuring Oracle WebCenter Collaboration to Use a Secure Portal or Image Service 5-9
5.4.4.2 Configuring Oracle BPM Suite to Use a Secure Portal or Image Service 5-9
5.5 Authentication and SSO 5-9
5.5.1 Delegating Authentication 5-10
5.5.1.1 Delegating to a Remote Authentication Tier 5-10
5.5.1.1.1 Additional resources 5-11
5.5.1.2 Delegating to an SSO Provider 5-11
5.5.1.2.1 Additional resources 5-11
5.5.1.3 Delegating to Windows Integrated Authentication 5-11
5.5.1.3.1 Additional resources 5-11
5.5.2 Access Control Lists and Profile Sources 5-12
5.5.2.1 Additional Resources 5-12
5.5.3 Brokering Credentials 5-12
5.5.3.1 Additional resources 5-12

6 Defining Administrative Roles

6.1 Access Control Lists and Activity Rights 6-1
6.1.1 Access Control Lists 6-1
6.1.2 Activity Rights 6-1
6.2 Creating a Group Hierarchy 6-1
6.3 Assigning Activity Rights 6-2
6.4 Defining an Administrative Object Hierarchy 6-3
6.5 Managing Quality through Object Migration 6-4

7 Localization

7.1 About Localization in Oracle WebCenter 7-1
7.1.1 Localization and the Oracle WebCenter Interaction User Interface 7-1
7.1.2 Localization and Oracle WebCenter Collaboration and Oracle BPM Suite 7-1
7.1.3 Localization and Search 7-1
7.2 Localizing Portal Objects 7-2
7.2.1 The Localization Manager 7-3
7.3 Adding Custom Languages 7-4
7.3.1 Adding the Language Directory 7-4
7.3.2 Adding Language Style Sheets 7-4
7.3.3 Adding an Online Help Language 7-4
7.3.4 Adding Javascript Language Files 7-5

8 Load Balancing

8.1 Load Balancing Oracle WebCenter 8-1
8.1.1 Load Balancing the Oracle WebCenter Interaction Portal Component 8-1
8.1.2 Load Balancing the Image Service 8-3
8.1.3 Load Balancing the Document Repository Service 8-3
8.1.4 Load Balancing the Automation Service 8-3
8.2 Load Balancing Oracle WebCenter Applications 8-4
8.2.1 PPE-LB Load Balancing Oracle WebCenter Applications 8-4
8.2.1.1 Configuring the PPE-LB 8-4
8.2.1.2 PPE-LB and SSL 8-5
8.2.1.3 PPE Configuration Settings 8-5
8.2.2 Clustering Oracle WebCenter Collaboration 8-6

9 Performance Tuning

9.1 Tuning a Java Application Server or Standalone Oracle WebCenter Product 9-1
9.1.1 Garbage Collection Concepts 9-1
9.1.2 Garbage Collection Logs 9-2
9.1.3 Analyzing the Garbage Collection Log 9-2
9.1.4 Resolving Garbage Collection Performance Issues 9-3

10 Developing a Production Maintenance Plan

10.1 Periodic Tasks 10-1
10.2 Monitoring Oracle WebCenter Services 10-1
10.3 Monitoring Databases and Java Application Servers 10-2
10.4 Monitoring Usage 10-2
10.5 Troubleshooting Tools 10-3
10.5.1 Oracle WebCenter Logging Utilities 10-3
10.5.2 View Source 10-4
10.5.2.1 When to Use View Source 10-4
10.5.2.2 How to Use View Source 10-4
10.5.2.3 What Is Available in View Source 10-4

A Java Virtual Machine Configuration

A.1 Java Memory Switches A-1
A.2 Application Servers A-2
A.2.1 Tomcat 6.x A-2
A.2.2 Oracle WebLogic Portal 10.3.0 .... A-2
A.2.3 IBM Websphere A-2
A.3 Oracle WebCenter Standalone Components A-2
A.3.1 Oracle WebCenter Analytics A-2
A.3.2 Automation Service A-3
A.3.3 Oracle WebCenter Collaboration A-3
A.3.4 Document Repository A-3
A.3.5 Notification A-3
A.3.6 PTUpload A-4
A.3.7 Oracle BPM Suite A-4

A.3.8 Tagging Service A-5

Index

Preface

This book provides an overview of planning an Oracle WebCenter Interaction deployment, and describes how to define administrative roles, stage deployments, and provision hardware.

For an overview of all deployment documentation and the products and versions covered by the deployment documentation, see the *Oracle Fusion Middleware Deployment Overview for Oracle WebCenter Interaction*.

Audience

This guide is written to provide guidance to people responsible for the design and deployment of the Oracle WebCenter Interaction system. Access to resources with strong knowledge of the platform operating system, database, web and application servers, and any other third-party software is recommended.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following types of documents for the covered products:

- *Installation and Upgrade Guides*
- *Release Notes*
- *Administrator Guides*
- *User Guides*
- *Developer Guides*

Conventions

The following text conventions are used in this document:

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

1 Enterprise Deployment Overview

This chapter provides an overview of the enterprise topology for Oracle WebCenter Interaction, describing its components and features.

It contains the following sections:

- Section 1.1, "Oracle WebCenter Interaction Architecture"
- Section 1.2, "Oracle WebCenter Interaction Deployment Documentation"

1.1 Oracle WebCenter Interaction Architecture

Oracle WebCenter Interaction provides the framework for applications, supports virtual community workspaces, and integrates them all into a cohesive Web work environment.

1.1.1 Oracle WebCenter Interaction Components

The following components make up Oracle WebCenter Interaction.

1.1.1.1 Portal

The portal serves end user portal pages and content, and provides a gateway to back-end systems.

The portal enables end users to access portal content via My Pages, community pages, the knowledge directory, and search. The portal also enables some administrative actions, such as setting preferences on portlets or managing communities.

1.1.1.2 Document Repository

The Document Repository Service stores content uploaded into the portal, such as images or documents uploaded into Oracle WebCenter Collaboration.

1.1.1.3 Search

Search provides indexing and query services for content that is in the Oracle WebCenter deployment. Content that is indexed in the Oracle WebCenter system includes documents, portlets, communities, users, and other Oracle WebCenter objects.

1.1.1.4 Automation Service

The automation service runs jobs that perform tasks such as crawling documents into the knowledge directory, synchronizing groups and users with external authentication sources, and maintaining the search collection.

1.1.1.5 Image Service

The image service serves images, javascript, and other static content for use by the Oracle WebCenter system.

1.1.1.6 ALUI Directory

The ALUI Directory is a basic LDAP group store used by Oracle WebCenter Analytics and Oracle WebCenter BPM instead of accessing the Oracle WebCenter Interaction database directly.

1.1.1.7 Common Notification Service

The Common Notification Service is uses by Oracle WebCenter Interaction and Oracle WebCenter Collaboration.

1.1.2 Portal Features

The following features of Oracle WebCenter Interaction are key to your deployment.

1.1.2.1 Experience Definitions

Experience definitions allow different audiences to be presented with different branding and features in the portal.

1.1.2.2 Knowledge Directory

The knowledge directory is a portal area that users can browse to discover documents that have been uploaded by users or imported by content crawlers.

1.1.3 Oracle WebCenter Analytics

Oracle WebCenter Analytics delivers comprehensive reporting on activity and content usage within portals and composite applications, allowing you to know and meet user information needs.

1.1.4 Oracle WebCenter Collaboration

Oracle WebCenter Collaboration helps people work together via the Web, supporting task management, projects, communities, calendars, discussions, and document sharing with version control.

1.1.5 Oracle WebCenter Portal's Pagelet Producer

Oracle WebCenter Portal's Pagelet Producer acts as the backbone for integration with WebCenter services.

1.1.6 Oracle WebCenter BPM Workspace Extensions

Oracle WebCenter BPM is used to create and manage departmental, enterprise, and inter-enterprise business processes. Oracle WebCenter BPM Workspace Extensions is an extended version of Oracle WebCenter BPM, designed to integrate with the Oracle WebCenter Interaction portal to provide an enhanced set of administrative features and end user experiences.

1.1.7 Developer Tools

The following developer tools are available for Oracle WebCenter Interaction.

1.1.7.1 Oracle WebCenter Interaction Development Kit (IDK)

The Oracle WebCenter Interaction Development Kit (IDK) enables Java and .NET developers to rapidly build, deliver, and improve user-centric composite applications through Oracle WebCenter Interaction. The IDK provides interfaces for Integration Web Services -- authentication, profile, crawler, and search -- that integrate enterprise systems into Oracle WebCenter Interaction. IDK Extensions provide a framework for customized Oracle WebCenter Interaction-based applications. Additional developer tools include Oracle WebCenter Logging Utilities, standardized support for .NET Web Controls, WSRP, and JSR-168.

1.1.7.2 Oracle WebCenter WSRP Producer for .NET

The Oracle WebCenter WSRP Producer for .NET is a collection of libraries and Visual Studio .NET integration features that support easy authoring of ASP.NET 2.0 portlets. Portlets authored using the Oracle WebCenter WSRP Producer for .NET can be consumed in both Oracle portal environments: Oracle WebCenter Interaction and Oracle WebLogic Portal.

1.1.8 Integration Services

Integration services provide ways to combine the functionality of commonly deployed enterprise systems into composite applications.

1.1.8.1 Documentum

The following Oracle WebCenter products are available to integrate Documentum into your deployment.

1.1.8.1.1 Oracle WebCenter Interaction Content Service for Documentum Oracle WebCenter Interaction Content Service for Documentum scans Documentum Docbases for new content, categorizing links to Documentum content in the organized, searchable structure of the Oracle WebCenter Interaction Knowledge Directory.

1.1.8.2 IBM/Lotus Notes

The following Oracle WebCenter products are available to integrate Lotus Notes into your deployment.

1.1.8.2.1 Oracle WebCenter Interaction Content Service for Lotus Notes Oracle WebCenter Interaction Content Service for Lotus Notes scans Notes databases for new content, categorizing links to Notes content in the organized, searchable structure of the Oracle WebCenter Interaction Knowledge Directory. This allows customers to avoid the costs of replicating Notes databases by publishing Notes content in an enterprise-wide knowledge management system.

1.1.8.3 LDAP

The following Oracle WebCenter product is available to integrate LDAP into your deployment.

1.1.8.3.1 Oracle WebCenter Interaction Identity Service for LDAP Oracle WebCenter Interaction Identity Service for LDAP enables you to import and synchronize users and groups with associated profile information into Oracle WebCenter Interaction from an external LDAP source. At the time of login, the user's username and password are passed to the LDAP source for purposes of authentication, replacing native LDAP authentication.

1.1.8.4 Microsoft

The following Oracle WebCenter products are available to integrate Microsoft into your deployment.

1.1.8.4.1 Oracle WebCenter Interaction Content Service for Windows Files Oracle WebCenter Interaction Content Service for Windows Files scans Windows file systems for new content, categorizing links to content in the organized, searchable structure of the Oracle WebCenter Interaction Knowledge Directory. Windows NT, Windows 2000, and Windows 2003 are supported.

1.1.8.4.2 Oracle WebCenter Interaction Identity Service for Active Directory Oracle WebCenter Interaction Identity Service for Active Directory enables the authentication and synchronization of users between Microsoft's Active Directory (AD) and Oracle WebCenter Interaction. The Identity Service retrieves user information from AD, allowing for user information to be mapped (and leveraged) within Oracle WebCenter Interaction.

1.1.8.4.3 Oracle WebCenter Interaction Content Service for Microsoft Exchange Oracle WebCenter Interaction Content Service for Microsoft Exchange scans Exchange Servers for new content, categorizing links to Microsoft Exchange content in the organized, searchable structure of the Oracle WebCenter Interaction Knowledge Directory.

1.1.8.4.4 Oracle WebCenter Console for Microsoft SharePoint Oracle WebCenter Console for Microsoft SharePoint imports, indexes, and returns Microsoft Windows Sharepoint Services resources via Oracle WebCenter Interaction Search.

1.2 Oracle WebCenter Interaction Deployment Documentation

This guide includes the following chapters:

- Chapter 2, "Planning Portal Structure and Content"
- Chapter 3, "Provisioning Computers"
- Chapter 4, "Migration and Staging"
- Chapter 5, "Securing Oracle WebCenter Interaction"
- Chapter 6, "Defining Administrative Roles"
- Chapter 7, "Localization"
- Chapter 8, "Load Balancing"
- Chapter 9, "Performance Tuning"
- Chapter 10, "Developing a Production Maintenance Plan"
- Appendix A, "Java Virtual Machine Configuration"

1.2.1 Other Documentation

In addition to the deployment documentation in this guide, the following documentation will assist in the use and customization of Oracle WebCenter Interaction.

1.2.1.1 Product Documentation

Installation and Upgrade Guides, Administrator Guides, and other documentation are available for each Oracle WebCenter component. These guides are located in the product specific page on the Oracle Technology Network at http://www.oracle.com/technetwork/middleware/webcenter-interaction/documentation/index.htmll.

1.2.1.2 Online Help

Online help is accessible through the user interface of each of the Oracle WebCenter products. Online help covers context specific usage as well as procedures for performing end-user and administrative tasks.

1.2.1.3 Development Documentation

The development documentation describes how to install and use the Oracle WebCenter Interaction Development Kit (IDK), the Oracle WebCenter WSRP Producer for .NET, and other development tools.These guides are located in the product specific page on the Oracle Technology Network at http://www.oracle.com/technetwork/middleware/webcenter-interaction/documentation/index.html.

In addition, the Oracle Technology Network provides articles and discussion about Oracle WebCenter Interaction development.

2

Planning Portal Structure and Content

This chapter describes portal structure and content at a high level. The purpose of this chapter is to assist in planning portal structure and assigning administrative responsibility for managing portal content.

This chapter contains the following sections:

- Section 2.1, "Single Portals and Federated Portals"
- Section 2.2, "Experience Definitions"
- Section 2.3, "Communities"
- Section 2.4, "Portlets"
- Section 2.5, "Oracle WebCenter Interaction Search"

2.1 Single Portals and Federated Portals

It is possible to deploy a single portal or multiple, federated portals. Figure 2–1 illustrates a single portal deployment where different experience definitions provide a portal experience specific to each group of users. Figure 2–2 illustrates federated portals, where instead of experience definitions on a single portal, each federated portal provides a different portal experience.

Figure 2–1 Single Portal with Multiple Experience Definitions

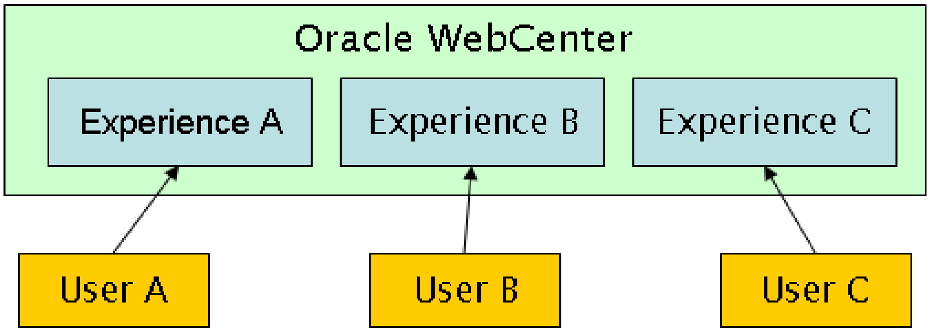
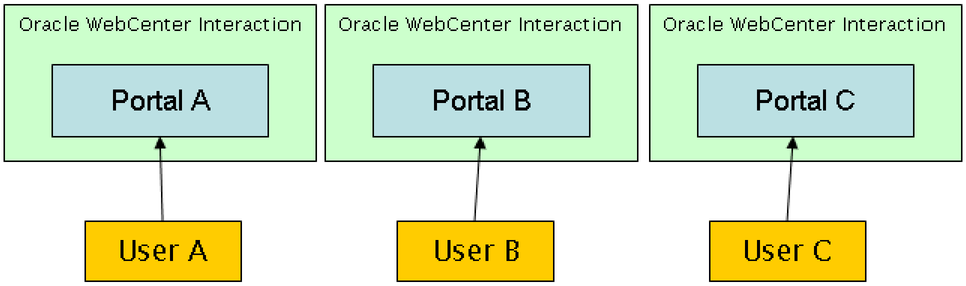


Figure 2–2 Federated Portals


Oracle WebCenter Interaction
Portal A
User A
Oracle WebCenter Interaction
Portal B
User B
Oracle WebCenter Interaction
Portal C
User C

Having a single portal with one or more experience definitions has benefits over deploying multiple federated portals. In a single portal deployment:

- Users have different experiences but are managed in a single place.
- The Oracle WebCenter deployment is easy to scale. IT needs only to look at total use for a single set of hardware versus fragmented use for multiple sets of hardware.
- It is easy to distribute enterprise-wide communications.
- It is easy to integrate enterprise-wide business processes.
- There is a common content management system

2.2 Experience Definitions

Experience definitions allow you to present different audiences with different branding and features in the portal.

For example, you could create an experience definition for a particular customer. The experience definition would include the customer's logo and company colors and include access to communities and knowledge directory folders specific to the needs of the customer.

Experience definitions are applied according to rules configured with the Experience Rules Manager.

For information on configuring experience definitions and rules, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

2.3 Communities

Communities are pages shared between members of a group to facilitate collaboration and communication on a particular project or on departmental goals.

Communities provide the following benefits:

- A consistent user experience for members of a department or project group.
- Discussion forums in which community-pertinent information is discussed and archived.
- A version-controlled repository for project or departmental documentation.

For details on implementing communities, see the documentation for Oracle WebCenter Collaboration.

The following are potential use cases for communities:

- Business Unit Resource Center (Line of Business Communities)
- Interactive Workspace (Collaborative Communities)
- Customer or Partner Management Site (Sales and Service-Oriented Communities)
- Dashboards (Analytic Communities)
- Business Process Applications (Process Communities)

2.3.1 Business Unit Resource Center (Line of Business Communities)

This section describes a use case for a business unit resource center (a line of business community).

Audience:

- Business unit or department
- Customers of that business unit or department

Content:

- Community documents, links, calendar
- Metrics
- Expert finder
- Q&A

Success indicators:

- Strong departmental or group identity
- Existing intranet as content source
- Motivated community owner

Pitfalls to avoid:

- Static page that people visit and forget

Suggested Oracle WebCenter tools:

- Oracle WebCenter Content
- KD Browser portlet included with Oracle WebCenter Interaction

2.3.2 Interactive Workspace (Collaborative Communities)

This section describes a use case for an interactive workspace (a collaborative community).

Audience:

- Ad hoc or established project workgroups

Content:

- Project task list
- Document management and archive
- Project calendar
- Threaded discussions
- Project metrics

Success indicators:

- Members spread out
- Project has specific objectives and milestones
- Project has outgrown e-mail and file-shares

Pitfalls to avoid:

- Dustbin of history: old projects, communities that do not go away
- Ghost town: two or three people are probably not enough

Suggested Oracle WebCenter tools:

- Oracle WebCenter Collaboration
- Oracle WebCenter Interaction Services

2.3.3 Customer or Partner Management Site (Sales and Service-Oriented Communities)

This section describes a use case for a customer or partner management site (a sales and service-oriented community).

Audience:

- Customers or partners

Content:

- Key customer or partner resources: documents, calendar
- Self-service access to CRM or PRM system
- Feedback mechanism
- Customer-to-customer or partner-to-partner: facilitate community

Success indicators:

- Portal-only access for critical information
- Responsiveness to customer/partner feedback

Pitfalls to avoid:

- No human input

Suggested Oracle WebCenter tools:

- Oracle WebCenter Collaboration
- Oracle WebCenter Interaction Services
- Oracle WebCenter Content
- Oracle WebCenter Portal's Pagelet Producer

2.3.4 Dashboards (Analytic Communities)

This section describes a use case for a dashboard (an analytic community).

Audience:

- Management

Content:

- Performance metrics

- Financial documents

Success indicators:

- Support to enforce consistent data formatting
- Portal-only access for critical information
- Culture of accountability based on metrics

Pitfalls to avoid:

- Make sure the dashboards have fresh data
- Make sure security works appropriately

Suggested Oracle WebCenter tools:

- Oracle WebCenter Collaboration
- Oracle WebCenter Analytics
- Oracle WebCenter Portal's Pagelet Producer

2.3.5 Business Process Applications (Process Communities)

This section describes a use case for a business process application (a process community).

Audience:

- Users involved in process

Content:

- Published content
- Data from multiple systems
- Workflow
- Metrics

Success indicators:

- Simple navigation, consistent branding a priority
- Unified search criteria
- Looking to utilize reusable components, common foundation

Pitfalls to avoid:

- If you do not have a process, the software will not do it for you

Suggested Oracle WebCenter tools:

- Oracle WebCenter Collaboration
- Oracle Business Process Management

2.4 Portlets

Portlets are applications embedded in a portal and can be interactive or solely informational. They are able to communicate preferences with the portal and to communicate with other portlets.

A portlet must be based on a web service. The web service controls the bulk of the portlet settings, such as the URL and cache settings. The portlet definition in the portal contains the name, width, type, and administrative preferences, if any.

Portlet templates allow multiple instances of the same portlet to be created, with each instance potentially different in appearance or information.

Oracle WebCenter Interaction includes pre-made portlets and the ability to easily implement portlets.

Portlets can also be developed from scratch using the Oracle WebCenter Interaction Development Kit (IDK). For details on portlet development, see the Oracle WebCenter Interaction Development Kit (IDK) documentation.

2.5 Oracle WebCenter Interaction Search

Oracle WebCenter Interaction Search allows users to quickly and efficiently find a wide variety of information from sources across the enterprise, both inside and outside the Oracle WebCenter products. Search can be distributed across a multiple server cluster.

2.5.1 Searchable Content

There are a number of possible sources of searchable content, and it is important to understand the options for providing that content to end-users:

- **Knowledge Directory**: The core of the Oracle WebCenter knowledge management infrastructure is the Knowledge Directory—a hierarchy of folders that contain links to files of various formats, stored in different types of repositories. Files can be crawled into the Knowledge Directory or manually submitted and can be filtered into the folder hierarchy (also known as a taxonomy) in order to provide an entry point to high-quality, organized content. In addition to the out-of-the-box functionality, virtually any repository can be made searchable through the creation of Content Services. All items in the Knowledge Directory can be searchable.
- **Oracle WebCenter Collaboration**: The project workspaces provided by Oracle WebCenter Collaboration contain documents, threaded discussions, announcements, task lists, wikis and blogs contributed and managed by distributed teams. All items in Oracle WebCenter Collaboration can be searchable.
- **Portal Administrative Objects**: Users, web services, portlets, Content Services—all the objects that make up the administrative infrastructure of a portal are searchable. End-users can search for users (to view profile and expertise information), communities (to visit or join), and portlets (to add to a My Page). Administrators (who need to create and manipulate all types of objects) can search for a wider variety of items and have more advanced options in their search results.
- **Non-portal Searchable Content**: Legacy search engines and repositories with pre-existing search or query functionality can often contain valuable sources of content that for various reasons cannot be crawled into the portal or managed through Oracle WebCenter Collaboration. With search web services, any repository that can respond to queries can be extended with a web services adapter so that it can be searched from the portal. Results from a number of disparate search providers (both inside the enterprise and on the internet) can be aggregated in this way.

- **Tagging Service**: The Tagging Service utilizes users' tags to rank content and provide more usable search results.

The Search administrator is responsible for creating and scheduling the initial search index jobs as well as update jobs. The Search administrator is also responsible for customizing search "Best Bets" and the search thesaurus.

2.5.2 Grid Search

Grid Search refers to distributing Oracle WebCenter Interaction Search nodes over multiple servers. Search servers can be configured to be stand-alone or a node in a *search cluster*. In a search cluster, the search index is divided, or partitioned, across multiple search nodes.

You can manage the search cluster using the *Search Cluster Manager* or the command line utility *cadmin*.

For more information on administering Grid Search, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

2.5.2.1 Grid Search Best Practices

1. Do not deploy multiple nodes on a single host in a production environment.
2. Schedule checkpoints when there is little or no planned indexing activity. This will help ensure that the checkpoint reflects the most up to date information and minimize recovery time.
3. Set the Search Cluster Manager Service to manual or disabled on all but one server. Only one instance of this service can be utilized by the portal.
4. A single search sever can be installed as a search cluster with one node, rather than a stand-alone search deployment. This helps streamline the process of adding future search nodes.
5. In a multiple node deployment, configure the cluster home directory on a server other than the search servers themselves. If the cluster home is located on one of the search servers, that server is a single point of failure for the entire cluster.
6. Cluster home should be located on a high-availability file system with fast connectivity to the search node host machines. Ideally, the cluster home should be on a RAID file system to ensure availability and fault tolerance.
7. Search nodes should be located within the same subnet on the network, and ideally on the same switch.

3 Provisioning Computers

This chapter summarizes host configuration and sizing requirements for an Oracle WebCenter deployment. The purpose of this chapter is to assist in planning hardware provisioning for Oracle WebCenter deployment. For further assistance in provisioning hardware, contact your Oracle representative.

3.1 Component Host Requirements

The following table provides guidelines for provisioning host computers for Oracle WebCenter components.

Component	Host Requirements
Portal Service	Estimate hardware needs specific to anticipated load. For details, see Section 3.3, "Evaluating Hardware Requirements for the Portal." **Scaling Guide** For large deployments, install multiple portal components and configure load balancing and failover. For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."
Administrative Portal	**Minimum** Can additionally function as a portal component in a Web farm. Can be installed on the same host as portal component and/or Image Service. If not functioning as a portal component, can be on the same host as Automation Service. **Recommended** A dedicated CPU. Some administrative actions are CPU-intensive. **Scaling Guide** No more than one Administrative Portal should be installed. **Security Guide** The Administrative Portal can be installed in a network environment that is only accessible by the Oracle WebCenter administrator.

Component	Host Requirements
Image Service	**Minimum** 1 GB RAM Can be installed on the same host computer as the portal component. **Recommended** 2 GB RAM More processing power is required if you use SSL or compression. **Scaling Guide** For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."
Document Repository Service	**Minimum** 1 GB RAM **Recommended** 2 GB RAM Fault tolerant disk for document storage. **Scaling Guide** For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."
Automation Service	**Minimum** Should be on a separate host from the portal component. If installed on the same host as the portal, schedule all jobs to run in off-peak hours. **Recommended** 1 GB RAM Dual processor, 1 Ghz or greater **Scaling Guide** If intensive use of identity service and content service jobs is anticipated, install multiple automation services and configure load balancing. Search performs document indexing and cannot be horizontally scaled; adding multiple automation services for the sole purpose of crawling content does not greatly improve system performance. For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."

Component	Host Requirements
Tagging Service	**Minimum** 1 GB RAM **Recommended** 2 GB RAM Fault tolerant disk for document storage. **Scaling Guide** For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."
Notification Service	**Minimum** 1 GB RAM **Recommended** 2 GB RAM Fault tolerant disk for document storage. **Scaling Guide** For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."
Directory Service	**Minimum** 1 GB RAM **Recommended** 2 GB RAM Fault tolerant disk for document storage. **Scaling Guide** For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."

Component	Host Requirements
Search	**Minimum** ■ **Small** (up to 250,000 documents): Dual CPU 2 GB RAM ■ **Medium** (up to 500,000 documents): Dual CPU, 4GB RAM Two Search Partitions ■ **Large** (more than 500,000 documents, or very high search query load): 4 or more Search Partitions with dedicated Dual CPU, 4GB RAM Servers Or 64-bit Solaris or AIX host (s), Dual CPU 1.3 Ghz or greater; 4-8 GB RAM, high performance I/O **Recommended** Two or more x86 Dual CPU Servers with 3GB RAM each configured as a cluster. 64-bit Solaris or AIX host, Dual CPU 1.2 Ghz or greater; 4-8 GB RAM, high performance I/O. **Scaling Guide** CPU requirements are directly proportional to the search request throughput the component can support. Indexing speed is proportional to the speed of an individual CPU, per Search Partition. RAM supports internal caching done by Search. RAM requirements are proportional to the size and number of documents indexed.
Oracle WebCenter Analytics	**Minimum** 2 GB RAM Dual processor, 2 Ghz **Recommended** Install on a separate host from the portal component. **Scaling Guide** No more than one Oracle WebCenter Analytics service should be installed. **Security Guide** Enable Unicast UDP on port 31314 for communication between Oracle WebCenter Analytics and the portal component. End-user access to Oracle WebCenter Analytics is gatewayed by the portal component, so the Oracle WebCenter Analytics host computer can reside behind a DMZ firewall.

Component	Host Requirements
Oracle WebCenter Collaboration	**Minimum** 2 GB RAM Dual processor, 2 Ghz Can reside on same host computer as other components that generate portlets, such as Oracle WebCenter Analytics. **Recommended** Install Oracle WebCenter Collaboration on a separate host computer from other components to preclude contention for the JVM. **Scaling Guide** For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."
Oracle WebCenter Interaction API Service	**Minimum** Can be on the same host as the portal component. **Recommended** Install on its own host. **Scaling Guide** No more than one Oracle WebCenter Interaction API service should be installed. **Security Guide** You should not expose the SOAP API through the extranet. To protect it, install the Oracle WebCenter Interaction API Service on a separate host from the portal component and locate the Oracle WebCenter Interaction API Service host behind a firewall. For details on security, see Chapter 5, "Securing Oracle WebCenter Interaction."

Component	Host Requirements
Database Server	**Minimum** 2 GB RAM 1 CPU, 2 Ghz **Recommended** 4 GB RAM 2-8 CPU Install on separate host computer. **Scaling Guide** Database Server Load Balancing The database server can be scaled using any database-compatible clustering technology. Currently, this means that scaling can only be provided by a larger machine. If necessary, each portal database can be placed on a separate computer and scaled separately. If running on Windows, failover of databases can be provided with Microsoft Cluster Services, and geographic load balancing and failover can be provided using SQL Server replication. However, this method is technically and administratively challenging and is not recommended unless availability requirements cannot be met otherwise. Oracle databases can be deployed for high availability. Oracle WebCenter Interaction supports both client-side connection and server-side connection failover with Oracle RAC. **Security Guide** Install the database server behind a firewall and restrict access so that only computers that host Oracle WebCenter Interaction components can access the database server host. End users do not need access to the database server host.
Remote Server - Identity Services (IDS)	**Minimum** 1 GB memory 2 GB disk space Dual processor, 1Ghz **Recommended** Install on a separate host from the portal component. To maximize performance, install in a network location that is in close proximity to back-end components. **Scaling Guide** Install additional Automation Services, as necessary, to accommodate a large number of IDS jobs. **Security Guide** End-user access to IDS portlets is gatewayed by the portal component, so the IDS host computer can reside behind a DMZ firewall.

Component	Host Requirements
Remote Server - Content Services	**Minimum** Install on a separate host from the portal component. **Recommended** To maximize performance, install in a network location that is in close proximity to back-end data sources. **Scaling Guide** Install additional automation services, as necessary, to accommodate a large number of Content Service jobs. **Security Guide** End-user access to Content Service portlets is gatewayed by the portal component, so the Content Service host computer can reside behind a DMZ firewall.
Remote Server - Portlets	**Minimum** Can share a host with other portlets and Web services. **Recommended** Install on a separate host from the portal component. To maximize performance, install in a network location that is in close proximity to back-end components. **Scaling Guide** In general, caching enables static portlets with minimal personalization to scale very well to any number of users. Dynamic portlets with more personalization cannot be as effectively cached and so require more processing power. If necessary, improve performance by installing dynamic portlets on hosts with premium hardware. **Remote Server Load Balancing** Remote servers can be load balanced using Parallel Portal Engine load balancing. For details on load balancing and failover, see Chapter 8, "Load Balancing." **Security Guide** End-user access to portlets is gatewayed by the portal component, so the remote server host computer for portlets can reside behind a DMZ firewall.

3.2 Optimization Strategies

The following table characterizes optimization strategies you might consider when you provision computer resources for your site.

Goal	Approach
Low initial hardware cost	Organizations optimizing for low initial hardware cost seek to buy the least expensive machines necessary to make the software work reliably. Given a choice between repurposing two existing single processor servers and spending $7,000 on a new multi-processor, multi-core server, they would choose the former.

Goal	Approach
Low hardware maintenance cost	Organizations optimizing for low hardware maintenance costs seek to reduce the number of machines needed to host the software. Because each additional computer incurs a minimum fixed cost in terms of administrative overhead, power consumption, space, and operating system license, these organizations would rather combine multiple Oracle WebCenter components on a single, more powerful computer than distribute those components over multiple, less expensive machines.
High availability	Organizations optimizing for high availability are willing to spend extra money and effort to ensure that the portal and other Oracle WebCenter components are available reliably to their users at all times. Such organizations typically purchase more computers and load balance them where possible, creating redundant configurations.
Low software maintenance cost	Organizations optimizing for low software maintenance cost assume that at some point in the life of the system, some part of the software will malfunction, and they seek both to lessen the chance that malfunctions will occur and lessen their impact when they do occur. Such organizations would typically purchase more individual computers to ensure that system components do not interfere with one another, and to reduce the risk that taking a computer out of the system to install new software will impact multiple system functions.
Scalability	Organizations optimizing for scalability assume that their deployments will be required to handle a large number of users. Such organizations would typically purchase extra hardware, and more expensive hardware, in order to create excess capacity in the system.
Performance	Organizations optimizing for performance seek to make their systems operate as fast as possible, especially in their ability to render pages quickly for end-users. Like organizations seeking to lower software maintenance costs, these organizations would distribute system components across a larger number of computers to ensure that each component has unrestricted access to the computing power it needs to perform its tasks the moment those tasks are called for.
Network Security	Organizations optimizing for network security seek to ensure that end-users touch only machines hosting the smallest amount of code and data. Such organizations also typically install firewalls between layers of their deployment, to ensure that if an intruder compromises one layer, the potential damage is limited. Such organizations tend to purchase more computers in order to isolate the portal component, which end-users touch directly, from other components.

3.3 Evaluating Hardware Requirements for the Portal

Complete the steps in the following worksheet to evaluate hardware options.

1. Estimate peak load using the following calculation:

```
Pages/sec = ((Power user pages/hr * #power users + Normal user pages/hr *
#normal users + Infrequent user pages/hr * #infrequent users pages/hr) / (3600
sec/hr) * fraction of users who could log on who are actually connected
```

> **Note:** Base your calculations on historical data for existing Web sites that serve a similar function. Use the following conventions to identify users:

- Power users. A power user is one who routinely adds or deletes portal content.
- Normal users. A normal user is one who routinely reads content.
- Infrequent users. An infrequent user is one who does not routinely use the portal.

Record your estimated peak load here: ____________ pages/sec

2. Review the benchmark charts on Section 3.4, "Portal Performance on Various Hardware Hosts," and choose a configuration that supports the peak load calculation from Step 1.

   In general, you want to provision a number of portal components that support a total of 2 to 3 times the estimated peak load from Step 1. For example, if you estimate peak load to be 15 pages/sec, you want to provision either:

   - One (1) portal component that can support 30-45 pages/sec
   - Two (2) or three (3) portal components that each support 15 pages/sec.

   Record the benchmark capacity here: ____________ pages/sec

   Follow the steps described in Steps 3-10 to adjust this benchmark capacity to a real-life estimate of expected use.

3. If users use My Pages more than communities, revise the number upward by approximately 5%.
4. If users use the Knowledge Directory more than 20% of the time, revise the number downward by approximately 10%.
5. If the deployment runs under SSL (security mode 2) on the portal component, without an SSL accelerator, subtract 10%.
6. IF the deployment will use SSL to communicate to the majority of Portlets and Web Services, subtract 10%.
7. If this portal also serves the administrative portal, revise the number downward by 5%.
8. If you use a virus scanner on the portal, subtract 0-10%, depending on the virus scanner settings.
9. If you use Tomcat as the Application Server and do not use the non-blocking Java connector (org.apache.coyote.http11.Http11NioProtocol), subtract 20%.
10. If the system is deployed as a VMWare Virtual Machine, subtract 15%.
11. After you have made the adjustments in Steps 3-10, does the configuration you selected in Step 2 still meet your capacity requirements?

3.4 Portal Performance on Various Hardware Hosts

Portal performance demonstrates the following general trends:

- Performance varies significantly on different types of server hardware.

- Performance is not dependent on the operating system, where platforms are otherwise similar.
- Performance is dependent on the JVM or CLR used and how these are tuned.
- In general, .NET and Java show similar performance, being nearly equal on most two-processor servers. However these vary somewhat in the sensitivity to processor frequency and system memory performance:
  - Java tends to be more sensitive to system memory performance.
  - .NET is more sensitive to processor cache size and processor frequency.

    These differences run approximately within a plus or minus 20% performance range at the very extreme.
- Overall performance is highly dependent on memory subsystem performance, which tends to be the most important performance-related property of a server. Memory subsystem performance can be characterized by the total aggregate system bandwidth to memory as well as the latency of memory access. For Intel Xeon-based systems, this is correlated with the processor bus speed. Systems with a 800Mhz bus significantly outperform those with a 400Mhz bus. Pentium III Xeon-based systems are also limited by their memory subsystem and scale poorly with extra CPUs.

The performance data in the table that follows is indicative of these general trends. This table provides benchmark data for the current version of the Oracle WebCenter Interaction portal component. For each representative system, the load shown is the maximum sustainable load on the server with an average mix of page views on an uncustomized system. Various factors will influence the maximum sustainable load of individual deployments such as UI customizations, effective use of portlet caching, and different mixes of page types.

3.4.1 Pages per Second on Oracle WebCenter Interaction 10.3.0

It is important that the performance measurements in the following table not be compared directly with the performance data for releases earlier than Oracle WebCenter Interaction 10.3.0. A new benchmark was created for Oracle WebCenter Interaction 10.3.0 that does more work per request and serves more sophisticated content than the previous benchmarks. In addition to richer content and more data in the system, HTTP compression is enabled and approximately 25% of the portlet request occur via HTTPS. Adaptive Layout mode is enabled for the benchmark.

The page distribution in the benchmark is approximately:

- 10% My Pages
- 30% Communities
- 10% Knowledge Directory
- 10% Searches
- 5% User Profiles
- 30% Gateway
- 5% other

The following table provides performance data for Oracle WebCenter Interaction 10.3.0.

System	System Details	Pages/Second
Xeon 2.4Ghz to 3.06Ghz, 533Mhz system bus, HyperThreading enabled (Dell PowerEdge 1750)	2 x 2.8Ghz Processors 512K L2	41
Xeon 3.2Ghz, 800Mhz system bus, HyperThreading enabled (Dell PowerEdge 1850)	2 x 3.2Ghz Processors 1M L2	67
Xeon MP 2.7Ghz, 400Mhz system bus, HyperThreading enabled (Dell PowerEdge 6650)	4 x 2.7Ghz Processor 512K L2 2M L3	67
Xeon 2.66Ghz, 1333Mhz system bus (Dell PowerEdge 1950)	4x2.66 Ghz Core 2 Xeon Dual Core	125
Opteron 2.2Ghz, 1000 MHz	2x2.2 Ghz Opteron Dual Core	105
UltraSparc IV 1.5Ghz Sun Fire V490	2 x 1.5 Ghz CPU	71
UltraSPARC-T1 1 GHz Sun Fire T1000	8 cores 32 threads 1GHz	74

4

Migration and Staging

This chapter summarizes migration capabilities for Oracle WebCenter deployments. The purpose of this chapter is to assist in planning development, QA, and production environments. By utilizing its migration capabilities you can stage the Oracle WebCenter deployment in a testing environment where you can test quality and gain acceptance prior to pushing it to production.

The following table summarizes migration capabilities.

Component	Migration Guidelines
Portal and Image Service	Follow the guidelines in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.
Search	Search should not be migrated. The Search Update Agent job indexes new portal objects and documents.
Identity Services, Content Services, and Portlet Suites	Do not migrate these services. Import the original product .pte package and complete configuration as described in the installation guide for the specific product.
Oracle-BEA AquaLogic Interaction Publisher	Follow the guidelines in the *Administrator Guide for AquaLogic Interaction Publisher*.
Oracle WebCenter Collaboration	Follow the guidelines in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Collaboration*.
Oracle-BEA AquaLogic Interaction Studio	Follow the guidelines in the *Administrator Guide for AquaLogic Interaction Studio*. **Notes:** ■ Migration is only relevant when the source and destination portals have distinct Oracle-BEA AquaLogic Interaction Studio installations. ■ Portlets must be created with a compatible version of Oracle-BEA AquaLogic Interaction Studio. ■ Do not include dependencies when creating the migration package. ■ Data in the source Oracle-BEA AquaLogic Interaction Studio portlet database is not migrated. Use the Oracle-BEA AquaLogic Interaction Studio data export/import functionality to move data. ■ If multiple Oracle-BEA AquaLogic Interaction Studio portlets share and underlying database, migrate these portlets in batch. This maintains the relationship between the portlets and their shared database.

Component	Migration Guidelines
Oracle WebCenter Analytics	Do not migrate Oracle WebCenter Analytics. Install and configure Oracle WebCenter Analytics in the production environment.

5 Securing Oracle WebCenter Interaction

This chapter summarizes security concerns for Oracle WebCenter Interaction deployments. While this chapter provides a summary of security needs, it is not intended to replace the services of a qualified security professional. The purpose of this chapter is assist in developing a security plan and should not be considered a replacement for the services of qualified security professionals. Oracle does not advocate the use of any specific security configuration. Oracle does provide professional consulting services to assist in securing an Oracle WebCenter deployment. To engage Oracle professional services, contact your Oracle representative.

This chapter is divided into the following sections:

- Section 5.1, "Determining Your Security Needs" describes best practices for determining the security needs of your Oracle WebCenter deployment.
- Section 5.2, "Security Architecture," provides an overview of the Oracle WebCenter component security architecture, including intra-component communication, firewalls, and the DMZ.
- Section 5.3, "Ensuring the Security of Your Production Environment" provides high-level descriptions of the security measures that can be employed to secure your Oracle WebCenter environment.
- Section 5.4, "Configuring SSL," provides an overview of SSL in the Oracle WebCenter deployment, including how and where CA certificates should be imported into the various Oracle WebCenter services.

5.1 Determining Your Security Needs

This section describes best practices for determining the security needs of your Oracle WebCenter deployment. It is divided into the following sections:

- Section 5.1.1, "Understand Your Environment"
- Section 5.1.2, "Hire Security Consultants or Use Diagnostic Software"
- Section 5.1.3, "Read Security Publications"

5.1.1 Understand Your Environment

To better understand your security needs, ask yourself the following questions:

- Which resources am I protecting?

  Many resources in the production environment can be protected, including information in databases accessed by Oracle WebCenter Interaction and the availability, performance, applications, and the integrity of the website. Consider the resources you want to protect when deciding the level of security you must provide.

- From whom am I protecting the resources?

  For most websites, resources must be protected from everyone on the Internet. But should the website be protected from the employees on the intranet in your enterprise? Should your employees have access to all resources within the Oracle WebCenter environment? Should the system administrators have access to all Oracle WebCenter resources? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators. Perhaps it would be best to allow no system administrators access to the data or resources.

- What will happen if the protections on strategic resources fail?

  In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the website. Understanding the security ramifications of each resource will help you protect it properly.

5.1.2 Hire Security Consultants or Use Diagnostic Software

Whether you deploy Oracle WebCenter on the Internet or on an intranet, it is a good idea to hire an independent security expert to go over your security plan and procedures, audit your installed systems, and recommend improvements. Oracle partners offer services and products that can help you to secure a Oracle WebCenter production environment. For details, visit the Oracle Support site at `http://www.oracle.com/support/index.html`.

5.1.3 Read Security Publications

For the latest information about securing web servers, Oracle recommends the "Security Practices & Evaluations" information available from the CERT™ Coordination Center operated by Carnegie Mellon University.

Report possible security issues in Oracle WebCenter products in the following ways by contacting Oracle technical support.

5.2 Security Architecture

This section describes Oracle WebCenter component architecture from a network security perspective. This includes how various components communicate with each other and which components need to be exposed to the end consumer.

5.2.1 Component Communication

With the exception of the database and Search, all requests from the Oracle WebCenter Interaction portal component are made using HTTP 1.1. This provides the following security advantages:

- There are third party tools to help monitor and audit HTTP 1.1 traffic.
- Each component web service uses a single, configurable port number, which eases firewall configuration.
- The Oracle WebCenter Interaction portal component implements the full range of HTTP security, including SSL/TLS certificates and basic authentication.

- Single Sign-On (SSO) third party products that are designed to protect HTTP traffic can be used to protect web services residing in the internal network. For details on SSO and Oracle WebCenter, see Section 5.5, "Authentication and SSO"

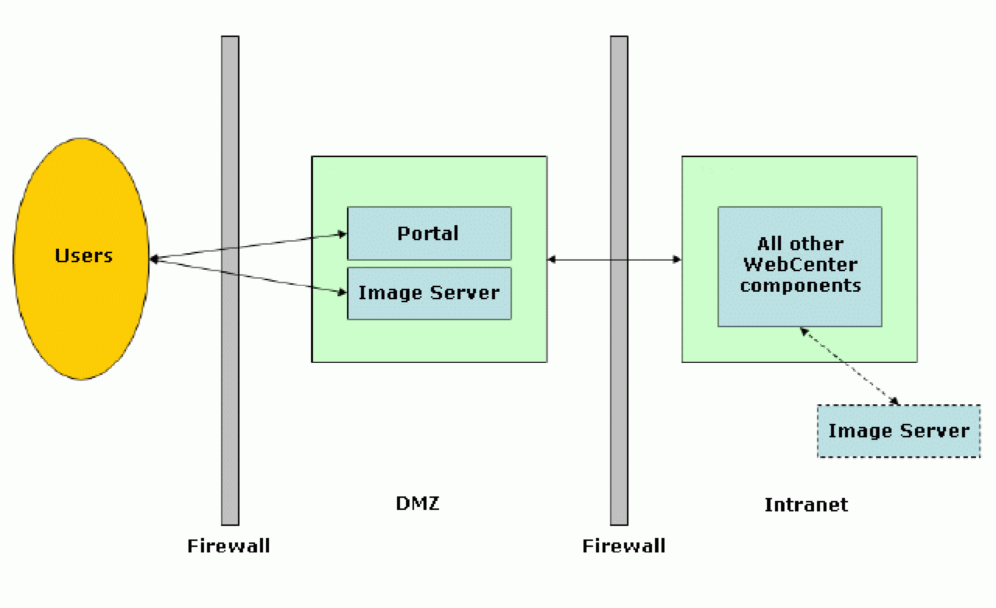
Communication between the Oracle WebCenter components can be further secured by:

- Using a separate network or subnet for the Oracle WebCenter components and the DB.
- Using technologies such as IPSec, VPN, or SSL.

5.2.2 Oracle WebCenter and the DMZ

A basic security architecture that limits external exposure to Oracle WebCenter products and other back-end systems is illustrated below.

Figure 5–1 Basic Security Architecture



In this configuration, only the Oracle WebCenter Interaction portal component and Image Service are placed within the DMZ. The Oracle WebCenter Interaction portal component and Image Service should be the only Oracle WebCenter components installed in the DMZ. When the portal is separate from other Oracle WebCenter components, persistent data in the search and database components and back-end tasks in the automation service are isolated from the external network.

The portal gateways requests to all other Oracle WebCenter components and back-end services, communicating with HTTP 1.1 across the firewall and into the internal network. The server housing the Oracle WebCenter Interaction portal should be hardened by a security professional, as it receives direct user requests. All communication should be SSL-encrypted.

To avoid traffic across the firewall between non-portal Oracle WebCenter components and the Image Service, another Image Service can be placed within the internal network.

Note: This is one potential network topology. For topologies involving software and hardware load balancing, see Chapter 8, "Load Balancing."

5.3 Ensuring the Security of Your Production Environment

This section provides high-level descriptions of the security measures that can be employed to secure your Oracle WebCenter environment. It is divided into the following sections:

- Section 5.3.1, "Securing the Oracle WebCenter Hosts"
- Section 5.3.2, "Securing Your Database"

5.3.1 Securing the Oracle WebCenter Hosts

An Oracle WebCenter production environment is only as secure as the security of the machines on which it is running. It is important that you secure the physical machine, the operating system, and all other software that is installed on the host machine. The following are suggestions for securing your Oracle WebCenter Interaction host in a production environment. Also check with the manufacturer of the machine and operating system for recommended security measures.

Table 5–1 Securing Oracle WebCenter Hosts

Security Action	Description
Physically secure the hardware.	Keep your hardware in a secured area to prevent unauthorized operating system users from tampering with the deployment machine ore its network connections.
Secure networking services that the operating system provides	Have an expert review network services such as e-mail programs or directory services to ensure that a malicious attacker cannot access the operating system or system-level commands. The way you do this depends on the operating system you use. Sharing a file system with other machines in the enterprise network imposes risks of a remote attack on the file system. Be certain that the remote machines and the network are secure before sharing the file systems from the machine that hosts Oracle WebCenter components.
Use a file system that can prevent unauthorized access.	Make sure the file system on each Oracle WebCenter component host can prevent unauthorized access to protected resources. For example, on a Windows computer, use only NTFS.
Set file access permissions for data stored on disk.	Set operating system file access permissions to restrict access to data stored on disk. This data includes, but is not limited to, the following: ▪ Third-party authentication directories. ▪ Portal configuration files. For example, operating systems such as Unix and Linux provide utilities such as umask and chmod to set the file access permissions. At a minimum, consider using "umask 066", which denies read and write permissions to Group and Others.
Set file access permissions for data stored in the portal database.	Set operating system file access permissions to restrict access to data stored in the portal database.

Table 5–1 (Cont.) Securing Oracle WebCenter Hosts

Security Action	Description
Safeguard passwords.	The passwords for user accounts on production machines should be difficult to guess and should be guarded carefully. Set a policy to expire passwords periodically. Never code passwords in client applications.
Do not develop on a production machine.	Develop first on a development machine and then move code to the production machine when it is completed and tested. This process prevents bugs in the development environment from affecting the security of the production environment.
Do not install development and sample software on a production machine.	Do not install development tools on production machines. Keeping development tools off the production machine reduces the leverage intruders have should they get partial access to an Oracle WebCenter production machine. Do not install the Oracle WebCenter sample applications on production machines.
Enable security auditing.	Configure security auditing to enable monitoring of sensitive portal functions using the Audit Manager function.
Consider using additional software to secure your operating system.	Most operating system can run additional software to secure a production environment. For example, an Intrusion Detection System (IDS) can detect attempts to modify the production environment. Refer to the vendor of your operating system for information about available software.
Apply operation-system service packs and security patches.	Refer to the vendor of your operating system for a list of recommended service packs and security-related patches.
Apply the latest Oracle WebCenter maintenance packs and implement the latest security advisories.	If you are responsible for security related issues on your site, review the alerts and patches available on the Oracle Support site at `http://www.oracle.com/support/index.html`. In addition, you are advised to apply each maintenance pack as it is released. Maintenance packs are a roll-up of all bug fixes for each version of the product.

5.3.2 Securing Your Database

Most web applications use a database to store their data. Common databases used with Oracle WebCenter are Oracle 10G and Microsoft SQL Server. The databases frequently hold sensitive data. When creating your web application you must consider what data is going to be in the database and how secure you need to make that data. You also need to understand the security mechanisms provided by the manufacturer of the database and decide whether they are sufficient for your needs. If the mechanisms are not sufficient, you can use other security techniques to improve the security of the database, such as encrypting sensitive data before writing it to the database. For example, leave all customer data in the database in plain text except for the encrypted credit card information.

5.4 Configuring SSL

Configuring Oracle WebCenter Interaction to use SSL is a relatively complex procedure that requires knowledge of SSL and CA certificates. This section provides an overview of the procedure. For more details, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

In the general case, the Oracle WebCenter Interaction portal Image Service would be secured with SSL, while another, unsecured Image Service would reside in the internal network for other Oracle WebCenter components. In this case Oracle WebCenter applications such as Oracle WebCenter Collaboration would use the unsecured Image Service and would only need to be configured for SSL communication with the portal.

The following sections explain how to configure the various Oracle WebCenter components for SSL:

1. Section 5.4.1, "Security Modes"
2. Section 5.4.2, "Configuring Oracle WebCenter for SSL"
3. Section 5.4.3, "Importing CA Certificates"
4. Section 5.4.4, "Configuring Oracle WebCenter Applications to Use a Secure Portal or Image Service"

5.4.1 Security Modes

After Oracle WebCenter components are installed, the security mode for the portal can be set. The security mode specifies how SSL is incorporated into your Oracle WebCenter deployment. Security mode options are described in the following table:

Security Mode	Description
0	Portal pages remain in whatever security mode—http or https—that the user initially uses to access the portal. For example, if a user accesses the portal via http, all the portal pages will remain http; if a user accesses the portal via https, all the portal pages will remain https. This is the default setting. **Note:** This mode is not recommended for production deployments or deployments that are exposed to the external network.
1	Certain portal pages are always secured via SSL and other pages are not. For example, the login page might always be secured but a directory browsing page might not. The page types that are secured are configurable. **Note:** This mode is not generally recommended.
2	All portal pages are always secured via SSL. Use this mode if there is no SSL accelerator. In this mode, the Web server should provide an SSL endpoint. **Note:** Configuring the SSL endpoint directly on a Tomcat application server is not recommended. A Web server should be used in front of the application server, and the SSL certificate should be installed on the Web server.
3	The portal uses an SSL accelerator. This is the most common configuration for production deployments. As with Security Mode 2, users are not connecting to the application server directly, so the front-end application server and the channel between the accelerator and the application sever must be secured.

For detailed information on configuring these settings, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

5.4.2 Configuring Oracle WebCenter for SSL

Use the following steps to configure Oracle WebCenter for SSL:

1. Configure SSL on Web servers or SSL accelerators that front-end the Oracle WebCenter Interaction portal and Image Service components. Refer to your Web

server or SSL accelerator documentation for instructions on configuring SSL and creating, signing, and installing an SSL certificate.

2. Configure the Portal component:

   a. Open **PT_HOME/settings/config/portalconfig.xml**.

   b. Ensure that `HTTPSecurePort` and `HTTPPort` are set to the ports you want to use.

   c. Change `ApplicationURL0` from `*` to `http://host_name:port/portal/server.pt`

   Note: The port number is not necessary for .NET deployments.

   d. Change `SecureApplicationURL0` from `*` to `https://host_name:port/portal/server.pt`

   Note: The port number is not necessary for .NET deployments.

   e. If multiple URL mappings are configured, ensure that these entries are updated as in Steps c and d. Refer to the comments in the configuration file for more information on URL mapping.

   f. Change `SecurityMode` from `0` to `1`, `2`, or `3`.

   g. Change `ImageServerSecureBaseURL` from `http` to `https`. Ensure that the Image Service port is correct.

3. If the Image Service is secured with SSL, set `ImageServerConnectionURL` to the secure URL. The CA certificate used by the Image Service must be imported into the Portal application server. For details, see Section 5.4.3, "Importing CA Certificates."

   If any portlets or remote servers use JSControls or Adaptive Portlets, the image service CA certificate must be imported into their runtimes as well. The JSControls libraries are embedded in server and IDK products, but are identified by XML stored on the Image Service.

4. If any remote server — including portlet servers, authentication sources, profile sources, or content services — is secured with SSL, import the remote server CA certificate into the Portal application server. For details, see Section 5.4.3, "Importing CA Certificates."

5. Configure Oracle WebCenter Collaboration to use the SSL-secured Portal and Image Service. For details, see Section 5.4.4, "Configuring Oracle WebCenter Applications to Use a Secure Portal or Image Service."

5.4.3 Importing CA Certificates

For each application server that makes requests to an SSL-secured service, the CA certificate from the secured service must be imported. The following two sections detail the process for importing CA certificates into a Java Application Server or IIS and .NET.

5.4.3.1 Importing CA Certificates Into a Java Application Server or Standalone Oracle WebCenter Product

For Java application servers the CA certificate is imported into the cacerts keystore.

To import the CA certificate:

1. On the computer that makes requests to an SSL secured service, open a command prompt.
2. Copy the CA certificate to this computer.

   > **Note:** The CA certificate is in the CA of the secured service. Save the .der encoded certificate as a .cer file.

3. Import the certificate using keytool. For example:

   ```
   keytool -v -import -trustcacerts -alias CA_alias -file CA_certificate_path
   -keystore CA_keystore_path
   ```

   where

   - CA_alias is the alias for the CA. For example, verisign or the server hostname.
   - CA_certificate_path is the path and filename of the .cer file to be imported.
   - CA_keystore_path is the path to the cacerts keystore. The cacerts keystore is typically located under the home of the JVM being run by the application server, **JVM_HOME/lib/security/cacerts**.

4. When prompted, enter the password for the cacerts keystore. The default password is changeme.

5.4.3.2 Importing CA Certificates into IIS and .NET

For IIS and .NET, the CA certificate is imported into the MMC.

1. On the computer that makes requests to an SSL secured service, open a command prompt.
2. Copy the CA certificate to this computer.

   > **Note:** The CA certificate is in the CA of the secured service. Save the .der encoded certificate as a .cer file.

3. Run MMC from the command line,

   ```
   > mmc
   ```

4. Click **Console** > **Add/Remove Snap-in**.
5. Click **Add**.
6. Click **Certificates**.
7. Click **Computer Account** and then click **Next**.
8. Click **local computer** and then click **Finish**.
9. Close the Add Standalone Snap-in dialog box.
10. Close the Add/Remove Snap-in dialog box by clicking **OK**.

11. In the MMC tree, expand to **Console Root** > **Certificates** > **Trusted Root Certificate Authorities** > **Certificates**.
12. Right click **Certificates** and select **All Tasks** > **Import**. Click **Next**.
13. Select the CA certificate to import. Click **Next**.
14. Choose to place all certificates in the **Trusted Root Certification Authorities** store.
15. Click **Next** and then click **Finish**.
16. Restart IIS.

5.4.4 Configuring Oracle WebCenter Applications to Use a Secure Portal or Image Service

This section describes how to configure Oracle WebCenter Collaboration and Oracle WebCenter BPM Suite to use a secure Portal or Image Service.

5.4.4.1 Configuring Oracle WebCenter Collaboration to Use a Secure Portal or Image Service

Oracle WebCenter Collaboration does not require any changes to function in security modes 1 or 2, as it uses the Portal's Image Service settings. A certificate is not required.

If you are using Security Mode 3, import the certificate of the CA that signed the Image Service and/or Portal certificate into Oracle WebCenter Collaboration. For details, see Section 5.4.3, "Importing CA Certificates."

Enable firewall access on port 28282 for communication between Oracle WebCenter Collaboration and the CNS. This is a UDP heartbeat port that Oracle WebCenter Collaboration uses to determine the CNS is alive without incurring a TCP handshake delay. You must add this port to the firewall.

If the host/port of the normal Image Service URL used by browsing users is not accessible from Oracle WebCenter Collaboration (for example, the Image Service is on a different machine than Oracle WebCenter Collaboration), you must change the jscontrols component that Oracle WebCenter Collaboration uses. This problem generates error messages that are displayed in the Calendar portlets. To avoid these errors:

1. Open the Oracle WebCenter Collaboration **config.xml** configuration file, located in **PT_HOME/ptcollab/*version*/settings/config**.
2. In the following line, set the URL to the value of **ImageServerConnectionURL** set in the portal **portalconfig.xml** configuration file.

```
<jscontrols>
<imageServerConnectionURL>[URL]</imageServerConnectionURL>
```

5.4.4.2 Configuring Oracle BPM Suite to Use a Secure Portal or Image Service

Import the CA certificate from the Image Service and Portal into Oracle BPM Suite. For details, see Section 5.4.3, "Importing CA Certificates."

5.5 Authentication and SSO

This section describes the various authentication options for an Oracle WebCenter deployment. It provides details on the following topics:

- Section 5.5.1, "Delegating Authentication,": By default, Oracle WebCenter performs authentication using credentials stored in the Oracle WebCenter Interaction portal database. Beyond basic portal authentication, Oracle WebCenter can delegate authentication to other back-end systems, such as:

  - A remote authentication tier, such as an LDAP service. For details, see Section 5.5.1.1, "Delegating to a Remote Authentication Tier."
  - An SSO Provider such as Oracle Access Manager. For details, see Section 5.5.1.2, "Delegating to an SSO Provider."
  - Windows Integrated Authentication. For details, see Section 5.5.1.3, "Delegating to Windows Integrated Authentication."

- Section 5.5.2, "Access Control Lists and Profile Sources,": Access control lists allow permissions to be granted to users and groups, and user and group properties can be pulled from back-end services and mapped to portal users and groups.
- Section 5.5.3, "Brokering Credentials,": Authenticated users can have their credential information brokered to other back-end services, allowing a single login to the portal to enable access to various systems.

5.5.1 Delegating Authentication

The portal can be configured to delegate authentication to various other systems, including remote authentication tiers such as LDAP servers and Active Directory, SSO providers such as Oracle Access Manager or Netegrity, and Windows Integrated Authentication (WIA). The following sections describe delegating authentication to these systems.

5.5.1.1 Delegating to a Remote Authentication Tier

Authentication can be delegated to a remote authentication tier by implementing an Oracle WebCenter authentication service. The authentication service serves two roles: synchronization and authentication.

Synchronization against a back-end authentication source imports users and groups into the Oracle WebCenter Interaction portal database. This must be done before the portal user can authenticate against the back-end authentication source. Passwords are not imported. This allows portal object permissions to be mapped to external users and groups, while maintaining authentication solely by the back-end authentication source.

Authentication allows the portal to query a back-end authentication source using a user's credentials. The sequence of events in the process is as follows:

1. The user browses to the main portal page and is presented the login screen. User enters credentials.
2. Oracle WebCenter Interaction sends a request to the back-end authentication source using the configured Oracle WebCenter authentication service.
3. The back-end authentication source returns validity of user credentials.
4. If the user is authenticated, access to their profile in the portal is granted. If the user is not authenticated, they are presented with the login screen.
5. Oracle WebCenter Interaction stores credentials in memory, and the user is identified by a browser cookie, if configured to do so. This allows the user to be logged in automatically next time he visits the portal.

Oracle provides pre-made authentication services supporting LDAP and Active Directory back-end systems. In addition, you can develop custom authentication services to authenticate against any back-end system.

5.5.1.1.1 Additional resources For details on configuring a pre-made authentication service, see *the Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

For details on creating a custom authentication service, start with *the Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

5.5.1.2 Delegating to an SSO Provider

Delegating authentication to an SSO provider can circumvent the Oracle WebCenter Interaction login screen and present the user with the login method of the SSO provider. This allows authentication by non-Web form mechanisms, such as keycards or biometric authentication.

The sequence of events of this process as follows:

1. The user browses to the main portal page address.
2. The portal forwards this request to the SSO provider.
3. The SSO provider determines whether the user is already authenticated or needs to be authenticated. This might be done by checking the user's browser cookies or by another method.
4. If the user is not authenticated, the SSO provider does what is necessary to gather credentials and authenticate the user.
5. The SSO provider returns the user to the portal and instructs Oracle WebCenter Interaction to grant the user access to his profile.

5.5.1.2.1 Additional resources For details on configuring an authentication source for an SSO provider, configuring the portal to use an SSO provider, or configuring the portal and SSO, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

5.5.1.3 Delegating to Windows Integrated Authentication

Delegating to Windows Integrated Authentication (WIA) is similar to delegating to an SSO source. With WIA, the user's credentials are the same as their Windows network credentials. When the user browses to the portal page, the portal uses Windows to authenticate the user.

Prior to authenticating with WIA, user information must be crawled into the portal database using an Active Directory authentication source.

The sequence of events in the WIA authentication process is as follows:

1. The user logged into a Windows network browses to the main portal page.
2. The Portal returns a 401 Unauthorized message to the user browser.
3. The browser and portal perform the WIA handshake to validate the user.
4. The portal accepts the authentication and grants access to the user's profile.

For WIA to work, the user must be logged into a Windows network and be using a browser, such as Internet Explorer, that supports the WIA handshake. WIA will fail over an HTTP proxy.

5.5.1.3.1 Additional resources For details on configuring an authentication source for WIA, configuring the portal to use WIA, or configuring the portal and SSO, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

5.5.2 Access Control Lists and Profile Sources

Access Control Lists (ACLs) allow users and groups to be granted permission to use and modify objects in the portal. Portal users who authenticate with any of the methods described in the section Section 5.5.1, "Delegating Authentication," can be identified within the portal database and added to object ACLs.

A *profile service* uses an authentication service to pull user properties from back-end systems such as LDAP services. Properties in the back-end system are mapped to Oracle WebCenter Interaction portal properties and synchronized with the authentication service.

5.5.2.1 Additional Resources

For details on configuring ACLs or configuring profile services, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

For details on developing profile services, start with the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

5.5.3 Brokering Credentials

The credentials of a logged in user can be made available to other systems being accessed via the Oracle WebCenter Interaction portal. This allows applications in the portal to display information from systems such as email or other enterprise applications without requiring for the user to log into each of these systems separately.

There are various ways Oracle WebCenter Interaction can pass credentials to back-end systems:

- PassThrough: The credentials the user supplied at login can be sent to the remote tier as a Basic Authentication header. This is useful if both the portal login and the back-end system login are based on the same authentication source, such as an LDAP service.
- Preferences: Preferences can be created to hold the user's credential, to be set individually by the end user. Preferences are stored encrypted in the portal database and controlled by the end-user.
- UserInfo: User properties are mapped to credential information stored in an LDAP service or other back-end source. Credentials are automatically populated for each user.
- SSO: An SSO token can be forwarded to the remote tier. This only works if the remote tier application can accept an SSO token. In cases where an SSO token is not accepted, some SSO Providers provide an API to convert the SSO token to name and password. This is dependent on the SSO vendor and the configuration of the SSO provider.
- Lockbox: User credentials can be stored in a lockbox in the Oracle WebCenter Interaction credential vault. The credential vault provides a central repository that securely stores and manages credentials. Portlets that need credentials to access back-end systems can securely retrieve appropriate user credentials.

5.5.3.1 Additional resources

For details on brokering credentials to existing applications, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

For details on developing portlets that use brokered credentials, start with *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter WSRP Producer for .NET*.

6

Defining Administrative Roles

This chapter provides a high level overview of administrative roles. The purpose of this chapter is to assist in developing a plan to assign administrative responsibility for managing portal objects.

6.1 Access Control Lists and Activity Rights

What users read, select, and modify in the portal is controlled by *access control lists* and *activity rights*.

6.1.1 Access Control Lists

An access control list (ACL) is a list of privileges associated with each folder or object in the portal. You can add users and groups to the ACL of an object in order to grant permission to perform certain tasks, such as viewing or modifying the object.

For details on using ACLs in the portal, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

6.1.2 Activity Rights

You can associate activity rights with users and groups to allow users to perform specific tasks within the portal. For example, the *Access Administration* activity right allows a user to see the Administration tab in the portal and to access the administrative object hierarchy. There are a number of activity rights built into the portal. You can also create custom activity rights.

For more information on activity rights, including a full list of activity rights built into the portal, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

6.2 Creating a Group Hierarchy

When creating a group hierarchy, begin with the users with the least rights and work towards the most powerful users. A group inherits the rights of its parent group, so the broadest groups with the least rights should be parent to more specific groups with greater rights.

For example, the engineering department creates an Engineer group (for all members of the department). The QA subset of the engineering department requires special access to certain bug tracking software, so a QA group should be created with the Engineer group as a parent. Administrative tasks on the bug tracking software is restricted to QA managers, so a group inheriting from the QA group is created for QA managers.

The Everyone group is the parent of all groups. All members of the Everyone group have the right to read and access their own profile.

The Administrator group is a child of all groups and has access to everything.

6.3 Assigning Activity Rights

The following table provides suggested activity rights for common roles found in an Oracle WebCenter deployment:

Role	Suggested Activity Rights
Content/Document Administrator	▪ Access Administration – to access the administration hierarchy ▪ Edit Knowledge Directory – to create new document folders ▪ Create Content Services – to create new Content Services ▪ Create Data Sources – to access secured documents ▪ Create Document Types – to force metadata onto documents ▪ Create Filters – to automatically manage folders ▪ Create Jobs – to create and run Crawler Web Service Synchronization jobs ▪ Access Utilities – to approve documents ▪ Access Smart Sort– to re-sort entire folders of already categorized documents
Community Creator	▪ Access Administration ▪ Create Communities – to create communities ▪ Create Community Infrastructure – to create community and page templates
Portlet Creator	▪ Access Administration ▪ Create Portlets – to create portlets ▪ Create Web Service Infrastructure – to create the remote server and web service to create truly custom portlets

Role	Suggested Activity Rights
Group/User Creator	■ Access Administration ■ Create Admin Folders – to make new admin folders to store users ■ Create Experience Definitions – to modify the user experience of users ■ Access Utilities – to create default profiles to apply initial layouts to users ■ Create Authentication Sources – to create authentication sources ■ Create Jobs – to run all Identity Service Synchronization Jobs ■ Create Profile Sources – to apply user information to synchronized users ■ Create Groups – to create groups ■ Create Users – to create users ■ Delegate Rights – to delegate rights to users (create activity groups)

6.4 Defining an Administrative Object Hierarchy

The Administrative Object Directory is a hierarchical folder structure that stores administrative objects.

Administrative objects include such objects as content services, portlets, and users. Each folder groups objects by object type. Each object's permissions default to the ACL of the folder.

For details on the Administrative Object Directory, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

The following guidelines can assist you in planning an administrative object hierarchy:

- Start with the end-user hierarchy rather than an organizational or management structure. End-users can see the administrative hierarchy in a few places in the portal. For example, by default, the Add Portlets and Join Communities pages search the administrative hierarchy for available portlets and communities and display a list of objects without showing their parent folders.

  Start by creating the hierarchy for communities and portlets (including portlet bundles) only and hide the administrative objects created during installation. For example, move all objects meant for administrators to a particular folder and restrict access to the folder so that end-users will not see it if they browse the hierarchy.

  The organization of the objects meant for administrators should be based on administrative structure or topic.

- Organize objects by topic rather than by object type. Objects are automatically grouped by type within each folder.
- Set ACLs for folders as early as possible. Objects created in a folder inherit the ACL of the folder. By planning access control early, you simplify managing object security.

- Manage user access by managing groups. Assigning a user to a group with permissions to a set of objects is easier than assigning each user to each object in the set.

6.5 Managing Quality through Object Migration

Creating a staging system for development and testing allows the Oracle WebCenter administrator to test object security. For information on object migration, see Chapter 4, "Migration and Staging."

7 Localization

This chapter provides an overview of localization options for an Oracle WebCenter deployment.

7.1 About Localization in Oracle WebCenter

All Oracle WebCenter products are fully Unicode-compliant and use UTF-8 encoding.

For additional details on localization and Oracle WebCenter, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

For developer documentation on localizing custom Web services and portlets, see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*.

7.1.1 Localization and the Oracle WebCenter Interaction User Interface

Out of the box, the Oracle WebCenter Interaction user interface is localized into eleven languages: Dutch, English, French, German, Italian, Portuguese, Spanish, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

Each portal user can choose her preferred language by changing her locale under **My Account** > **Edit Locale Settings**. For example, if a portal user changes her locale setting to any of the German locales (Austria, Germany, Luxembourg, or Switzerland), the user interface language will change to German.

You can create additional languages for the Oracle WebCenter Interaction user interface. For details, see Section 7.3, "Adding Custom Languages."

7.1.2 Localization and Oracle WebCenter Collaboration and Oracle BPM Suite

Oracle WebCenter Collaboration is localized to the same eleven languages as the Oracle WebCenter Interaction user interface. Oracle BPM Suite is localized to a subset of those languages.

It is possible to add custom languages to these applications; however, these customizations are not recommended unless done by Oracle professional services. To engage Oracle professional services, contact your Oracle representative.

7.1.3 Localization and Search

The Search index is stored in UTF-8 Unicode and supports 62 languages.

The Search engine supports advanced stemming and tokenization for the following 23 languages:

- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- French
- Finnish
- German
- Greek
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian (Bokmål)
- Norwegian (Nynorsk)
- Polish
- Portuguese
- Romanian
- Russian
- Spanish
- Swedish
- Turkish

In addition to those 23 languages, the Search engine provides basic tokenization support for an additional 39 languages.

The Search engine languages are hard-coded and cannot be customized.

7.2 Localizing Portal Objects

You can localize the names and descriptions of portal objects. For example, if you create a portlet with the name "Travel Portlet," it is possible to associate the name "Dienstreise Portlet" with the portlet for display to German locales.

Names and descriptions are added or modified using the administrative user interface for each object. When the object is opened in the administrative editor, the **Properties and Names** page allows you to specify a name and description for any available language.

For details on editing object properties, see the Oracle WebCenter Interaction online help.

7.2.1 The Localization Manager

You can export and import localized names and descriptions in bulk with the **Localization Manager**. Names and descriptions of objects are exported from the Oracle WebCenter Interaction database into an XML file. The XML file contains name and description strings and their translations. Translations are added or edited in the XML file, and then the names and descriptions imported into the Oracle WebCenter Interaction database using the Localization Manager.

This is a small sample of exported names and descriptions:

```
<localizationtable>
  <languages count='9'>
    <language>de</language>
    <language>en</language>
    <language>es</language>
    <language>fr</language>
    <language>it</language>
    ...
  </languages>
  <segments count='554'>
    <segment stringid='0' itemid='1' classid='2'>
      <source language='en'>Administrators Group</source>
      <target language='de'>Administratorengruppe</target>
      <target language='en'></target>
      <target language='es'>Grupo Administradores</target>
      <target language='fr'>Groupe d'administrateurs</target>
      <target language='it'>Gruppo Amministratori</target>
    ...
    </segment>
    <segment stringid='1' itemid='1' classid='2'>
      <source language='en'>WCI Administrators Group</source>
      <target language='de'>WCI-Administratorengruppe</target>
      <target language='en'></target>
      <target language='es'>Grupo Administradores de WCI</target>
      <target language='fr'>Groupe d'administrateurs WCI</target>
      <target language='it'>Gruppo Amministratori WCI</target>
    ...
    </segment>
    ...
  </segments>
</localizationtable>
```

In the exported XML:

- `<languages>` contains all of the user interface languages supported in the portal.
- `<segments>` contains one or more `<segment>` nodes. The `count` element shows the total number of name or description strings in the portal.
- `<segment>` contains a single name or description string and its translations. The contained `<source>` node is the original, to be translated text. The `<target>` nodes are the translations of the `<source>` node text.

The `<language>` element of each node is the ISO 639-1 two letter identifier for the given language.

7.3 Adding Custom Languages

This section covers adding custom languages to the Oracle WebCenter Interaction portal user interface. Adding custom languages to other Oracle WebCenter products, such as Oracle WebCenter Collaboration must be done by Oracle professional services.

Adding a custom language to the Oracle WebCenter Interaction portal user interface is a four step process:

1. Create a directory for the new language. For details, see Section 7.3.1, "Adding the Language Directory."
2. Add style sheets.
3. Translate online help
4. Translate Javascript language files.

Caution: Customizing OpenFoundation language resources is currently not supported.

7.3.1 Adding the Language Directory

The portal component loads supported languages based on the contents of the directory **PT_HOME/ptportal/*version*/i18n**. This directory contains one subdirectory for each supported language, each named with the ISO-639-1 language code.

The first step in adding a new language to the portal is to add a directory for that language to **PT_HOME/ptportal/*version*/i18n**. To do this:

1. Create a new directory under **PT_HOME/ptportal/*version*/i18n**. The directory must be named the ISO-639-1 language code of the language you intend to add.
2. Copy the contents of the **i18n/en** directory to the new directory.
3. Restart the portal. The new language is now available on the **My Account** > **Edit Locale Settings** page.

7.3.2 Adding Language Style Sheets

The second step in adding a new language to the portal is to add style sheets for that language.

Each language file in the **\ptimages\tools\cssmill\prop-text** folder has language-specific values for font style, font size, text style, etc. This design makes it easy to change the default font for each language. For example, if you want the default font for the Japanese user interface to be Tahoma, add Tahoma to the "ja" language file in the prop-text folder.

After adding a language file, you must also edit the **build.xml** file to generate the new language style sheets.

For more information, see the *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Interaction*.

7.3.3 Adding an Online Help Language

Online help is located on the Image Service under each product's private/help directory. For example, the Oracle WebCenter Interaction online help files are located in **imageserver/plumtree/portal/private/help**. Under this directory are two directories,

std for standard online help and **508** for Section 508-compliant help. Under those directories are directories for each supported language.

For example, the standard English online help for Oracle WebCenter Interaction is located in **imageserver/plumtree/portal/private/help/std/en**.

Online help is compiled using RoboHelp X5 for European languages and RoboHelp 2002 for Asian languages. RoboHelp projects are made available upon request. Contact Oracle Support at `http://www.oracle.com/support/index.html` for details.

7.3.4 Adding Javascript Language Files

You must localize string files for various Javascript user interface components when adding a language to the portal. The following Javascript components require you to add a string file with each added language:

- jscontrols
- jsdatepicker
- jsutil

These components are located on the Image Service, under **imageserver/plumtree/common/private/js**. The string files are located under each component's directory, in **LATEST/strings**.

To add a string file for the new language:

1. Copy the English file to a file in the strings file suffixed with the **ISO-639-1 code of the language to be added. For example, to add a Czech string file to jscontrols, copy LATEST/strings/PTControls-en.js** and save it as **LATEST/strings/PTControls-cz.js**.
2. Translate the copied string file to the language being added.

8 Load Balancing

This chapter provides an overview of load balancing and failover options for an Oracle WebCenter deployment. The purpose of this chapter is to assist in incorporating load balancing and redundancy into your network topology planning. Load balancing and redundancy options require third-party software or hardware and should be implemented with the aid of experts familiar with those third-party products. Oracle provides professional consulting services to assist in planning an Oracle WebCenter deployment. To engage Oracle professional services, contact your Oracle representative.

This chapter is divided into two sections:

- Section 8.1, "Load Balancing Oracle WebCenter," covers load balancing and failover strategies for the portal and other Oracle WebCenter components.
- Section 8.2, "Load Balancing Oracle WebCenter Applications," covers load balancing Oracle WebCenter applications such as Oracle WebCenter Collaboration and Oracle BPM Suite, and clustering for Oracle WebCenter Collaboration.

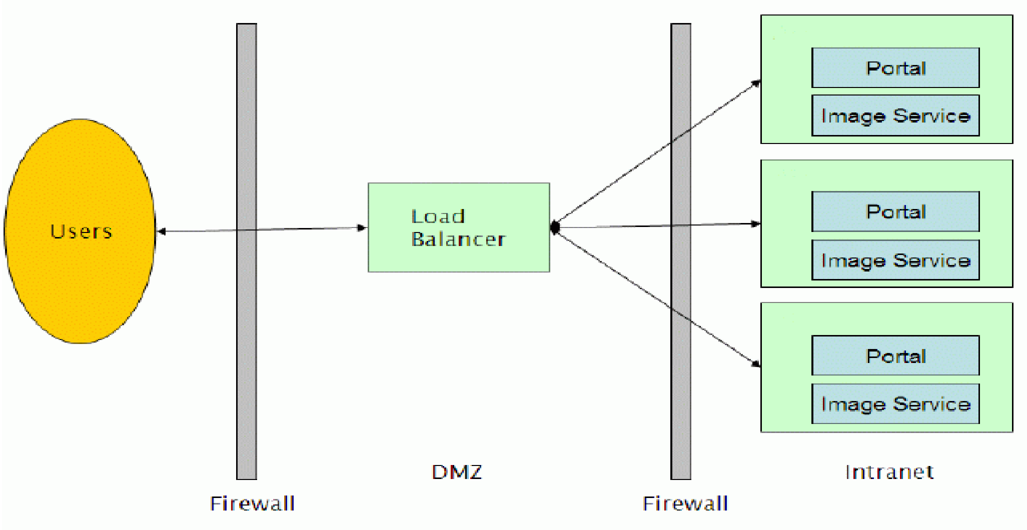
8.1 Load Balancing Oracle WebCenter

The following sections provide examples of load balancing strategies for Oracle WebCenter components.

8.1.1 Load Balancing the Oracle WebCenter Interaction Portal Component

A typical configuration for hardware load balancing is to put the load balancer network appliance in the DMZ and have it route requests to an Oracle WebCenter Interaction portal server farm, as illustrated in Figure 8–1.

Figure 8–1 Hardware Load Balancing Oracle WebCenter Interaction



The Oracle WebCenter Interaction portal can be used with any load balancing system that supports sticky IPs, including Cisco LocalDirector, F5 Big-IP, and Windows NLB, as well as the Apache Web server. Oracle does not advocate any specific load balancer.

Session states are maintained by the portal Web servers themselves. If a portal server is taken out of the server farm, user sessions on that server are lost and users will need to log back into the portal.

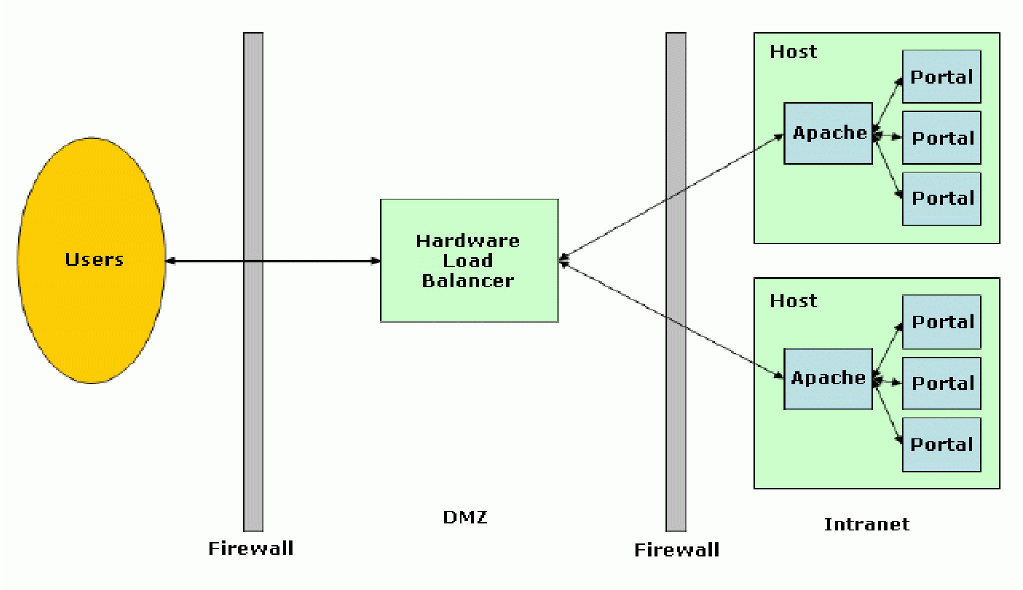
It is possible for the portal to become unresponsive while the portal Web server is still operational. In this case, the load balancer will assume that the portal is still alive. The load balancer should perform content verification to ensure that the portal is actually available.

The load balancer should send requests to the host with the most available resources instead of performing round-robin distribution of requests. Users use the portal component in different ways, and some users will tax the portal server more heavily than others.

For maximum fault tolerance, load balancers should be clustered.

Another potential load balancing topology is illustrated in Figure 8–2.

Figure 8–2 Multiple Oracle WebCenter Interaction Instances on One Server



In this example, multiple instances of Oracle WebCenter Interaction are running on a single host, with each portal server listening to a different port. On each host, an instance of Apache balances the load between the instances of Oracle WebCenter Interaction. There are multiple hosts running this configuration, and these hosts are load-balanced by a hardware load balancer in the DMZ. Sticky IPs must be maintained throughout.

On hardware that supports a large number of users, this configuration minimizes the number of user sessions lost in the event of a portal failure.

8.1.2 Load Balancing the Image Service

The Image Service serves static content and does not require sticky IPs. Any number of Image Services can be load balanced.

8.1.3 Load Balancing the Document Repository Service

The document repository service can be load balanced using IP load balancing. This provides partial failover; however, all document repository hosts must share a single, writable file system backing store.

The backing store cannot be load balanced, but failover can be achieved by using a shared local disk with MSCS for failover or a network share implemented with NAS or MSCS.

8.1.4 Load Balancing the Automation Service

The Automation Service requires no additional technology for load balancing or failover. Install multiple Automation Services in the Oracle WebCenter system and designate jobs to run on any set of available servers.

If a server fails mid-job, the job will not complete on another server; however, if the job is scheduled to run periodically, another Automation Service will pick up and run the job.

8.2 Load Balancing Oracle WebCenter Applications

The following sections describe how to load balance Oracle WebCenter applications such as Oracle WebCenter Collaboration and Oracle BPM Suite.

The following Oracle WebCenter products should not be load balanced:

- Oracle WebCenter Interaction Administrative Portal
- Oracle WebCenter Interaction API Service
- Oracle WebCenter Analytics

8.2.1 PPE-LB Load Balancing Oracle WebCenter Applications

The Oracle WebCenter Interaction portal component provides the Parallel Portal Engine Load Balancer (PPE-LB) to facilitate load balancing and failover services to Oracle WebCenter Collaboration, Oracle BPM Suite, and other portlet Web service providers utilizing HTTP messaging. This eliminates the need for third-party load balancers for middle-tier messaging.

To configure Oracle WebCenter Collaboration for clustering, see Section 8.2.2, "Clustering Oracle WebCenter Collaboration."

> **Caution:** Not all portlets can be load balanced. If the portlet caches data in memory with the assumption that the underlying database will not be modified, load balancing will cause issues. Consult the portlet documentation or portlet developer to determine if specific portlets can be load balanced.

8.2.1.1 Configuring the PPE-LB

The PPE-LB is configured by editing DNS so that one server name (the cluster name) resolves to each IP address in the cluster. Each remote server in the cluster must have a unique IP address and must have the same software installed.

Use nslookup from the portal server to verify that the cluster name resolves to all intended remote server addresses.

> **Caution:** Editing the **hosts** file on a Windows host is not equivalent to configuring DNS. Windows caches and returns only the first IP address instead of returning all IP addresses associated with the cluster.

Note: If the DNS server cannot be configured, edit the openhttp component section of the configuration.xml file to provide this information. Here is an example for configuring Oracle WebCenter Interaction to use clustered Oracle WebCenter Collaboration instances:

```
<setting name="openhttp:LoadBalancedHost0">
<value xsi:type="xsd:string">collab:11930</value>
</setting>
<setting name="openhttp:LoadBalancedIPs0">
<value
xsi:type="xsd:string">###.###.###.###:11930;###.###.###.###:11930</
value>
```

8.2.1.2 PPE-LB and SSL

When using SSL between the Oracle WebCenter Interaction portal and the remote servers, create a single SSL certificate by name and add it to each machine in the remote server cluster.

8.2.1.3 PPE Configuration Settings

The PPE is implemented with the OpenHTTP standard. OpenHTTP settings are configured in the Oracle WebCenter Interaction portal component by editing **PT_HOME/settings/configuration.xml** and modifying the openhttp component node.

The following settings are configurable:

Setting	Description
ProxyURL	Specifies the URL for a proxy host.
ProxyUser	Specifies an authentication user name for the proxy connection.
ProxyPassword	Specifies an authentication password for the proxy connection.
ProxyBypass	Contains a list of hosts accessed directly instead of through the proxy.
ProxyBypassLocal	Boolean flag specifies that hosts in the same domain should not be accessed through the proxy. If a hostname has no "." (dots) in its name it is considered local and in the same DNS domain.

The following settings can be added:

Setting	Description
ForceHttp10	Sends HTTP/1.0 requests instead of HTTP/1.1. The sockets are closed after sending a single request.
TraceBodyAndHeaders	For debugging only. Traces the values of headers and some parts of the body of the requests/responses to Oracle WebCenter Logging Utilities. Turned off by default because headers might contain passwords in cleartext.
HttpCacheSizeMb	Defines maximum size of the cached data. Cache uses an LRU algorithm to decide which old entry should be kicked out in order to accommodate newer data.
ConnectionCacheTimeoutSec	Defines the time that the socket remains unused in the cache before being closed by OpenHTTP.

Setting	Description
MinimumDNSThreads	Specifies the minimum number of threads that are used to perform DNS lookups.
MaximumDNSThreads	Specifies the maximum number of threads that are used to perform DNS lookups.

8.2.2 Clustering Oracle WebCenter Collaboration

Oracle WebCenter Collaboration supports clustering to provide load balancing and fail over. In clustering mode, multiple instances of Oracle WebCenter Collaboration communicate with each other to maintain a single, consistent logical image.

Configuring the Portal for Oracle WebCenter Collaboration Clustering

The portal provides load balancing through mapping one domain name to multiple IP addresses. A single domain name that contains the IP addresses of each Oracle WebCenter Collaboration server to be clustered must be provided. Use this name as the portlet remote server name.

Configuring Oracle WebCenter Collaboration for Clustering

You configure Oracle WebCenter Collaboration by editing two files, **config.xml** and **cluster.xml**. The files are located in **PT_HOME/ptcollab/*version*/settings/config**

To enable clustering, perform the following steps on each Oracle WebCenter Collaboration server to be clustered:

1. In **config.xml**, change the following:

   ```
   <cluster enabled="no">cluster.xml</cluster>
   ```

   to

   ```
   <cluster enabled="yes">cluster.xml</cluster>
   ```

2. Save **config.xml** and restart the Oracle WebCenter Collaboration server.

By default, Oracle WebCenter Collaboration uses UDP multicasting for communicating between servers. This is the most efficient option and is appropriate for most deployments. In environments where UDP multicasting is not allowed, configure Oracle WebCenter Collaboration to use UDP unicasting.

To configure Oracle WebCenter Collaboration to use UDP unicasting, perform the following steps on each Oracle WebCenter Collaboration server to be clustered:

1. In **cluster.xml**, nominate one of the machines in the cluster to be the coordinator:

   ```
   <coordinator-host>machine.name</coordinator-host>
   <coordinator-port>9990</coordinator-port>
   ```

   > **Note:** The port number can be any free port number.

2. Change the cluster profile to lan-cluster:

   ```
   <profiles profile='lan-multicast-cluster'>
   ```

   to

   ```
   <profiles profile='lan-cluster'>
   ```

3. Save **cluster.xml** and restart the Oracle WebCenter Collaboration server.

Another optional configuration is to use the **wan-cluster** profile. The **wan-cluster** profile uses TCP to communicate directly with specific Oracle WebCenter Collaboration instances.

To enable **wan-cluster**, perform the following steps on each Oracle WebCenter Collaboration server to be clustered:

1. In **cluster.xml**, add one or more Oracle WebCenter Collaboration instances to the `<hosts>` node. For example, if there are three Oracle WebCenter Collaboration instances, collab01, collab02, and collab03, edit the collab01 **cluster.xml** to include the other two instances:

   ```
   <hosts>collab02[$port],collab03[$port]</hosts>
   ```

   > **Note:** The $port string will be automatically replaced with the <port> setting already configured in cluster.xml.

2. In **cluster.xml**, change the cluster profile to wan-cluster:

   ```
   <profiles profile='lan-multicast-cluster'>
   ```

   to

   ```
   <profiles profile='wan-cluster'>
   ```

3. Save **cluster.xml** and restart the Oracle WebCenter Collaboration server.

9

Performance Tuning

This chapter details the process of tuning application servers and standalone Oracle WebCenter components to the needs of your Oracle WebCenter deployment.

The standalone Oracle WebCenter components are:

- Oracle WebCenter Analytics
- Oracle WebCenter Collaboration
- Oracle Business Process Management

The standalone components installed with Oracle WebCenter Interaction are:

- Automation Service
- Document Repository Service
- Notification Service
- Content Upload Service
- Tagging Engine Service
- Directory Service
- Remote Portlet Service

9.1 Tuning a Java Application Server or Standalone Oracle WebCenter Product

For Java application servers and standalone Oracle WebCenter products, tuning is a matter of adjusting various Java Virtual Machine (JVM) settings to optimize garbage collection. Oracle provides a comprehensive document on this subject, *Tuning Garbage Collection with the 1.4.2 Java[tm] Virtual Machine*, which you can find at `http://www.oracle.com/technetwork/java/javase/tech/vmoptions-jsp-140102.html`.

The following provides a brief background on the garbage collection process and a detailed, Oracle WebCenter focused process for tuning JVM garbage collection.

9.1.1 Garbage Collection Concepts

Garbage collection is the process the JVM undergoes to remove unused objects from memory. The following description of the garbage collection process is simplified for the purpose of this guide.

The JVM stores objects in two sections of the heap: the *young generation* and the *tenured generation*. The young generation is where objects are first created and provides the quickest, least CPU intensive access to objects. When the young generation fills, older active objects are transferred to the larger tenured generation. Objects in the tenured generation are more CPU intensive to access than those in the young generation.

The JVM undertakes two types of garbage collection. The *minor collection* runs when the young generation fills. It clears garbage objects and copies surviving objects to the tenured generation. The *major collection* runs when the tenured generation fills. The minor collection is significantly less CPU-intensive than the major collection.

9.1.2 Garbage Collection Logs

In order to analyze garbage collection impact on application server performance, a garbage collection log needs to be collected. The process is:

1. Enable garbage collection logging in the JVM. This is done in different places for each of the supported application servers and standalone Oracle WebCenter products. For details on enabling garbage collection logging, see Appendix A, "Java Virtual Machine Configuration."
2. Restart the application service to start logging garbage collection memory usage.
3. Run logging garbage collection until the problem occurs. If the problem is continuous, collect a sample of approximately 24 hours of data.

> **Note:** Every time the application server is restarted, the garbage collection log is overwritten. It is important to turn off automatic restarting of services, especially if you are investigating an issue that yields a server crash.

9.1.3 Analyzing the Garbage Collection Log

Tagtraum industries (`http://tagtraum.com`) provides a free utility, *gcviewer*, for analyzing garbage collection logs generated by the JVM. Load the garbage collection log into gcviewer and determine which issue is occurring based on the descriptions in Table 9–1.

Table 9–1 Garbage Collection Performance Issues

Issue	Symptoms in Garbage Collection Log	Impact of the Issue
Insufficient total (heap) memory allocated	Memory usage trends upwards and reaches the top of the total memory allocated.	Reduces the performance or potentially crashes the Oracle WebCenter product.
Excessive total (heap) memory allocated	Memory usage peaks much lower than total memory allocated.	Can cause a slowdown across all applications on the server. The application server or Oracle WebCenter product is taking up too much of the system memory.
Insufficient young generation memory allocated	Sawtoothed memory usage.	Reduces the performance of the Oracle WebCenter product. This represents excessive minor garbage collector runs, which increases the number of objects in the tenured generation. Objects in the tenured generation are more resource intensive when called.

9.1.4 Resolving Garbage Collection Performance Issues

Resolving the issues described in Section 9.1.3, "Analyzing the Garbage Collection Log," is a matter of adjusting the JVM memory settings and reanalyzing the garbage collection log. Table 9–1 shows what memory settings to adjust for each issue. For details on how to adjust these settings for each supported application server and standalone Oracle WebCenter product, see Appendix A, "Java Virtual Machine Configuration."

Table 9–2 Garbage Collection Performance Issue Resolution

Issue	Resolution	JVM Memory Parameter
Insufficient total (heap) memory allocated	Increase total heap memory allocation until memory usage stays reasonably below total memory.	Increase `-Xmx`
Excessive total (heap) memory allocated	Decrease total heap memory allocation until memory usage is reasonably, but not excessively, below total memory.	Decrease `-Xmx`
Insufficient young generation memory allocated	Increase young generation memory allocation until the memory usage trend is horizontal.	Adjust `-XX:NewRatio`

10

Developing a Production Maintenance Plan

This chapter provides an overview of Oracle WebCenter maintenance tasks and tools. The purpose of this chapter is to help you scope administrative responsibilities for the Oracle WebCenter so that you can develop a maintenance plan.

This chapter includes the following topics:

- Section 10.1, "Periodic Tasks"
- Section 10.2, "Monitoring Oracle WebCenter Services"
- Section 10.3, "Monitoring Databases and Java Application Servers"
- Section 10.4, "Monitoring Usage"
- Section 10.5, "Troubleshooting Tools"

10.1 Periodic Tasks

The following table provides suggestions for periodic tasks that you should consider as part of your production system maintenance plan.

Frequency	Task
Daily	Modify security of portlets, communities, and other objects in the portal. Modify permission roles for users. Publish new and existing applications/portlets to remote servers. Monitor portal, database, and remote servers alerts for CPU, memory, and hard disk usage to ensure availability.
Weekly	Install releases to one or more software components.
Monthly	Add new hardware to the environment (for example, new remote servers, new hard disk, and so on).
Ad Hoc	Install Oracle WebCenter patches. Install server patches from critical third-party software providers, such as operating system and anti-virus software.

10.2 Monitoring Oracle WebCenter Services

The Counter Monitoring System collects information from various performance counters for portal applications and exposes them for diagnosis and review. This system can be used to examine counters from any Oracle WebCenter application that resides on a remote host, provided the both the remote host and the counter monitoring system are on a network in which they can reach each other via UDP.

With the Counter Monitoring System you can:

- Set up counter logging files in your desired format to view counter information.
- Use the Counter Monitoring console to request specific counter data in real time.
- Use the Windows Perfmon utility to view portal counter data, if you use a Windows system.

For detailed information on the Counter Monitoring System, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

10.3 Monitoring Databases and Java Application Servers

Databases support Performance Monitor counters on Windows. WebLogic, Tomcat, and WebSphere do not. For information on performance monitoring for application servers, refer to the related application server documentation.

10.4 Monitoring Usage

Oracle WebCenter Analytics is an advanced usage tracking and analytics tool designed exclusively for Oracle WebCenter. This portal add-on enables you to assess portal ROI and define future opportunities with usage trends in mind. Oracle WebCenter Analytics delivers the following features out of the box:

- Usage Tracking Metrics: Tracks metrics for common portal functions, including community, portlet, collaboration project, and document hits, as well as search queries, logins, and more.
- Behavior tracking: Tracks usage patterns, such as number and duration of visits.
- User Profile Correlation: Correlates metrics with user profile information. In this way, usage tracking reports can be viewed and filtered by profile data, such as country, company and department.

Oracle WebCenter Analytics includes the following reports that you can customize by setting filtering, grouping, and presentation options.

Report	Description	Features
Community Traffic	Displays traffic information for each community in the portal.	Displays traffic in three ways: ■ Hits: Count of page views within the community. ■ Visits: Count of visits to the community, each visit can consist of several hits. ■ Users: Count of unique users who have visited the community. Users can select to see the most active, least active, or a select list of communities.
Community Response Time	Displays average, maximum and minimum response time for each community within the portal.	Calculates response time as the time between the portal receiving a community page request until the time an HTML response is sent to the client. Users can select to see the slowest response times, fastest response times, or response times for a select list of communities.

Report	Description	Features
Portlet Usage	Shows usage statistics within gatewayed portlets.	Displays traffic in two ways: ■ Activity: Count of hits on an object (for example, a button or link) within a portlet. ■ Users: Count of unique users who have performed an activity within the portlet. Users can select to see the most active, least active, or a select list of portlets.
Portal Traffic	Shows an aggregate of all portal page views within the portal.	
Portal Users	Displays statistics regarding portal user accounts.	Displays the following four figures to help explain user inception and activity. ■ Total user accounts in the portal. ■ Added (new) user accounts created in the portal during a given date range. ■ Active users defined by activity during a given date range. ■ Inactive users defined by inactivity during a given date range
Portal Logins	Shows an aggregate of all portal logins.	
Portal Duration	Displays the length of visits to the portal.	Calculate visit durations as the time between login and logoff or the time between login and inactivity for a configurable length of time. This report shows both average and maximum visit duration.
Search Keywords	Shows the top search keywords entered in searches within the portal.	See the top 5, 10, 25, 50 or 100 search keyword phrases entered within the portal.
Document Views	Shows statistics for document views in the portal.	Can display these statistics in two ways: ■ Top Documents: List of top documents viewed with view count. ■ Folders: Count of all document views by folders in the knowledge directory.

10.5 Troubleshooting Tools

This section describes logging and troubleshooting tools. It includes the following topics:

- Section 10.5.1, "Oracle WebCenter Logging Utilities"
- Section 10.5.2, "View Source"

For details on portlet debugging, see the *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction.*

10.5.1 Oracle WebCenter Logging Utilities

Oracle WebCenter Logging Utilities includes three *log message receivers* that allow for a wide variety of logging solutions. In the OpenLog Framework, log message receivers act to display or store log messages generated by *log message senders*, such as the portal or Oracle WebCenter Collaboration. Oracle WebCenter Logging Utilities include:

- Logging Spy. Previously called PTSpy, this utility is the primary log message receiver for the OpenLog Framework. In addition to displaying log messages from the portal and other Oracle WebCenter products and services, Logging Spy provides fine-grained filtering, viewing of saved log files, highlighting of errors, and the searching and sorting of log messages.
- Logger. Logger runs as an unattended background process that receives log messages from the OpenLog Framework and writes the messages to the file system. In addition to this primary use, the Logger can be configured to provide output in other ways, such as sending log messages to an e-mail system.
- Console Logger. The Console Logger runs in a console window, writing log messages to the console standard output. The Console Logger has limited use; in most cases, it is preferable to use Logging Spy.

For information on using these utilities, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction for Windows* or the *Oracle Fusion Middleware Upgrade Guide for Oracle WebCenter Interaction for Unix and Linux*.

10.5.2 View Source

HTML code creates Web pages. In turn, Oracle WebCenter Activity Spaces generate HTML code. Along with HTML from the View and Display pages, the underlying framework inserts some general information for each page. If there is an error on the page, the Error framework might insert additional debugging information. You can review the HTML source for any given Web page to gather this information. Often the HTML for a given error page contains detailed information about the error.

10.5.2.1 When to Use View Source

Use View Source to gather more information when you receive an error on a portal page or when you want some general information about the page. For example, use View Source if you receive the following error message on a portal page: "An unexpected error occurred when trying to start the Editor." The message itself gives no clues to the source of the error, but when you view the HTML source code for the page, you might be able to determine the source of the error.

10.5.2.2 How to Use View Source

While viewing the Web page, in the browser menu, click **View** > **Source**. This displays the HTML for that page. If the browser menu is unavailable, sometimes it is possible to view source by right-clicking the page and then clicking **View Source**. With this approach, be aware that if there are frames, only the source for the frame in which you right-clicked will display. When the source displays, you can search for specific pieces of information as described in the next section.

10.5.2.3 What Is Available in View Source

Each portal page contains several pieces of general information:

- To determine the server hosting the portal, search for "Hostname:". The hostname of the server is commented in the source: "<!--Hostname: My Server-->".
- To find information about the build of the portal, search for "Portal Version:", "Clingiest:", and "Build Date:".

- To find information about general timing data points, search for "Total Request Time:", "Control Time:", "Page Construction Time:", and "Page Display Time:".

If there is an error on the page, View Source might provide extended information. There are three items that you can search for:

- To view the error, search for "alert Error Title". You might have to repeat the search because several error related Tanglements might use that text.
- To view extended information, search for "Extended Error Message:". The extended error is wrapped in an HTMLComment and thus does not show up on the page, "<!--Extended Error Message: Sample Extended Error message.-->". The extended information, controlled by the developer and Activity Space, is frequently the same as the error message that displays in the user interface.
- You might also need to search for "unexpected error". When the portal encounters an unexpected error, the stack trace for the error is often inserted into an HTMLComment. The following example informs the user where the error originates from. The user then has a starting point from which to perform further debugging:

  ```
  <!--An unexpected error occurred when trying to start the Editor.:
  com.plumtree.openfoundation.util.XPException: An unexpected error occurred when
  trying to start the Editor.
  at
  com.plumtree.portalpages.admin.editors.group.GroupModel.DoTaskOnStartEditor(Gro
  upModel.java:411)
  ```

A

Java Virtual Machine Configuration

This appendix describes how to adjust JVM memory parameters and turn garbage collection logging on and off. Instructions below cover applications supported by Oracle WebCenter and those standalone Oracle WebCenter components.

The standalone Oracle WebCenter components are:

- Oracle WebCenter Analytics
- Automation Server
- Oracle WebCenter Collaboration
- Document Repository
- Notification
- PTUpload
- Oracle BPM Suite
- Tagging Service

A.1 Java Memory Switches

The following are Java memory switches used to tune JVM garbage collection. Use these switches in conjunction with the instructions specific to your application server or Oracle WebCenter product.

- `-Xloggc:`path/filename

  This switch turns on garbage collection logging for the JVM. Replace path/filename with the location where the garbage collection log should be generated.

- `-Xms` and `-Xmx`

  These switches set the minimum (`-Xms`) and maximum (`-Xmx`) heap size for the JVM. The JVM adjusts heap size based on object usage and bounded by these two switches. Setting these switches to the same value increases predictability by removing the ability of the JVM to adjust the heap size.

  > **Caution:** Fixing the heap size to a specific value requires special attention to memory tuning.

- `-XX:NewRatio`

This switch sets the ratio of the young generation to the tenured generation. For example

```
-XX:NewRatio=3
```

would mean that the tenured generation is 3x the size of the young generation, or, in other words, the young generation is one quarter of the heap and the tenured generation is three-quarters of the heap.

A.2 Application Servers

This section describes how to configure your application server. Refer to the section that applies to your type of application server.

A.2.1 Tomcat 6.x

To update Java options for Tomcat 6.x on Windows:

1. Run TOMCAT_HOME\tomcat6w.exe
2. Click the Java tab.
3. Update the Java memory switches in the Java Options: box.
4. Click OK. Restart the Tomcat service.

A.2.2 Oracle WebLogic Portal 10.3.0

To update Java options for Oracle WebLogic Portal 10.3.0:

1. Edit setDomainEnv.cmd in BEA_HOME/user/projects/domains/domain_name.
2. Add arguments to the line:

   ```
   set MEM_ARGS=-Xms256m -Xmx512m
   ```

3. Run setDomainEnv.cmd.

> **Note:** The `MEM_ARGS` parameter can also be updated in the startup script for the WebLogic domain.

A.2.3 IBM Websphere

To update Java options for IBM Websphere, use the IBM Websphere Admin Console. For instructions, refer to your IBM Websphere documentation.

A.3 Oracle WebCenter Standalone Components

The following sections describe how to configure Oracle WebCenter standalone components.

A.3.1 Oracle WebCenter Analytics

To update Java options for the Oracle WebCenter Analytics JVM:

1. Edit wrapper.conf in PT_HOME/ptanalytics/version/settings/config.
2. Add or modify parameters in the section Additional -D Java Properties.

> **Note:** Java parameter numbers must be continuous and incremental, and are set in both wrapper_base.conf and wrapper.conf. Check both files to ensure added parameters use the next number in sequence.

Restart the Analytics service.

A.3.2 Automation Service

To update Java options for the Automation Service JVM:

1. Edit wrapper.conf in PT_HOME/ptportal/version/settings/config.
2. Add or modify parameters in the section Additional -D Java Properties.

> **Note:** Java parameter numbers must be continuous and incremental, and are set in both wrapper_base.conf and wrapper.conf. Check both files to ensure added parameters use the next number in sequence.

Restart the Automation service.

A.3.3 Oracle WebCenter Collaboration

To update Java options for the Oracle WebCenter Collaboration JVM:

1. Edit wrapper.conf in PT_HOME/ptcollab/*version*/bin/ptcollaborationserverd.bat.
2. Add or modify parameters in the section Additional -D Java Properties.

   > **Note:** Java parameter numbers must be continuous and incremental, and are set in both wrapper_base.conf and wrapper.conf. Check both files to ensure added parameters use the next number in sequence.

3. Restart the Collaboration service.

A.3.4 Document Repository

To update Java options for the Document Repository JVM:

1. Edit wrapper.conf in PT_HOME/ptdr/version/settings/config.
2. Add or modify parameters in the section Additional -D Java Properties.

> **Note:** Java parameter numbers must be continuous and incremental, and are set in both wrapper_base.conf and wrapper.conf. Check both files to ensure added parameters use the next number in sequence.

Restart the Document Repository service.

A.3.5 Notification

To update Java options for the Notification JVM:

1. Edit wrapper.conf in PT_HOME/ptnotification/*version*/settings/config.

2. Add or modify parameters in the section Additional -D Java Properties.

> **Note:** Java parameter numbers must be continuous and incremental, and are set in both wrapper_base.conf and wrapper.conf. Check both files to ensure added parameters use the next number in sequence.

3. Restart the Notification service.

A.3.6 PTUpload

To update Java options for the PTUpload JVM:

1. Edit wrapper.conf in PT_HOME/ptupload/*version*/settings/config.
2. Add or modify parameters in the section Additional -D Java Properties.

> **Note:** Java parameter numbers must be continuous and incremental, and are set in both wrapper_base.conf and wrapper.conf. Check both files to ensure added parameters use the next number in sequence.

3. Restart the PTUpload service.

A.3.7 Oracle BPM Suite

To update Java options for the Publisher JVM:

1. Edit service.conf in PT_HOME/ptcs/*version*/settings/config.
2. Add a new parameter or modify existing parameters in the section Java Additional Parameters.

   For example, locate

   ```
   # Java Additional Parameters
   wrapper.java.additional.1=-Dprogram.name=cswfserver
   wrapper.java.additional.2=-Djava.awt.headless=true
   wrapper.java.additional.3=-Dplumtree.container.home=./../../../../../ptcs/6.2/c
   ontainer
   wrapper.java.additional.4=-Dplumtree.container.logs=./../../../../../ptcs/6.2/l
   ogs
   wrapper.java.additional.5=-Dorg.jboss.net.protocol.file.decodeFilePaths=true
   ```

   and add the garbage collection logging parameter

   ```
   # Java Additional Parameters
   wrapper.java.additional.1=-Dprogram.name=cswfserver
   wrapper.java.additional.2=-Djava.awt.headless=true
   wrapper.java.additional.3=-Dplumtree.container.home=./../../../../../ptcs/6.2/c
   ontainer
   wrapper.java.additional.4=-Dplumtree.container.logs=./../../../../../ptcs/6.2/l
   ogs
   wrapper.java.additional.5=-Dorg.jboss.net.protocol.file.decodeFilePaths=true
   wrapper.java.additional.6=-Xloggc:c:\publishergclog
   ```

3. Restart the Publisher service.

A.3.8 Tagging Service

To update Java options for the Tagging Service JVM:

1. Edit wrapper.conf in PT_HOME/pathways/*version*/settings/config.
2. Add or modify parameters in the section Additional -D Java Properties.

> **Note:** Java parameter numbers must be continuous and incremental, and are set in both wrapper_base.conf and wrapper.conf. Check both files to ensure added parameters use the next number in sequence.

3. Restart the Tagging Service.

Index

A

ACL. See access control lists (ACL)
Administrative Portal
  host requirements, 3-1
  scaling, 3-1
  security, 3-1
Analytics
  host requirements, 3-4
  monitoring usage with, 10-2
  scaling, 3-4
  security, 3-4
API Service
  host requirements, 3-5
  scaling, 3-5
  security, 3-5
Automation Service
  host requirements, 3-2
  scaling, 3-2
  security, 3-2

C

Collaboration
  host requirements, 3-5
  scaling, 3-5
  security, 3-5
Community Creator activity rights suggestions, 6-2
ConnectionCacheTimeoutSec setting, 8-5
Content Services (CS)
  host requirements, 3-7
  scaling, 3-7
  security, 3-7
Content/Document Administrator activity rights suggestions, 6-2
Counter Monitoring System, 10-1
CPU requirements, 3-1
CS. See Content Services (CS)

D

database server
  host requirements, 3-6
  scaling, 3-6
  security, 3-6
Document Repository Service
  host requirements, 3-2
  scaling, 3-2
  security, 3-2

F

failover
  Search, 3-4
ForceHttp10 setting, 8-5

G

Group/User Creator activity rights suggestions, 6-3

H

hardware requirements, 3-1
host requirements, 3-1
  Administrative Portal, 3-1
  Analytics, 3-4
  API Service, 3-5
  Automation Service, 3-2
  Collaboration, 3-5
  Content Services, 3-7
  database server, 3-6
  Document Repository Service, 3-2
  Image Service, 3-2
  Portal Service, 3-1
  portlets, 3-7
  Search, 3-4
HttpCacheSizeMb setting, 8-5

I

Identity Services (IDS)
  host requirements, 3-6
  scaling, 3-6
  securityhost requirements
    Identity Services, 3-6
IDS. See Identity Services (IDS)
Image Service
  host requirements, 3-2
  scaling, 3-2
internationalization, 7-1

J

Javascript, adding language files, 7-5

L

localization, 7-1
Logger, about, 10-4

M

MaximumDNSThreads setting, 8-6
memory requirements, 3-1
MinimumDNSThreads setting, 8-6
monitoring performance, 10-1
monitoring usage, 10-2

P

performance monitoring, 10-1
Portal Service
- host requirements, 3-1
- scaling, 3-1
- security, 3-1

Portlet Creator activity rights suggestions, 6-2
portlets
- host requirements, 3-7
- scaling, 3-7
- security, 3-7

ProxyBypass setting, 8-5
ProxyBypassLocal setting, 8-5
ProxyPassword setting, 8-5
ProxyURL setting, 8-5
ProxyUser setting, 8-5

R

RAM requirements, 3-1
reports, 10-2

S

scaling
- Administrative Portal, 3-1
- Analytics, 3-4
- API Service, 3-5
- Automation Service, 3-2
- Collaboration, 3-5
- Content Services, 3-7
- database server, 3-6
- Document Repository Service, 3-2
- host requirements, 3-2
- Identity Services, 3-6
- Portal Service, 3-1
- portlets, 3-7
- Search, 3-4

scaling your solution, 3-1
Search
- failover, 3-4
- host requirements, 3-4
- scaling, 3-4
- security, 3-4

Search administrator
- about, 2-7

security
- Administrative Portal, 3-1
- Analytics, 3-4
- API Service, 3-5
- Automation Service, 3-2
- Collaboration, 3-5
- Content Services, 3-7
- database server, 3-6
- Document Repository Service, 3-2
- host requirements for, 3-1
- Identity Services, 3-6
- Portal Service, 3-1
- portlets, 3-7
- Search, 3-4

T

TraceBodyAndHeaders setting, 8-5
troubleshooting tools, 10-3

U

usage monitoring, 10-2