

Oracle® Content Database

Administrator's Guide for Oracle WebCenter Suite

10g (10.1.3.2)

B32191-01

November 2006

Oracle Content Database Administrator's Guide for Oracle WebCenter Suite, 10g (10.1.3.2)

B32191-01

Copyright © 2002, 2006, Oracle. All rights reserved.

Primary Author: Marla Azriel

Contributors: Simon Azriel, Sudhanshu Garg, Mei Hong, Vasant Kumar, Charles Liuson, Diep Maser, Liju Nair, Alejandro Paredes, Karthik Raju, Alan Wiersba

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

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

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

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

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

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

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

Contents

Preface	xi
Audience	xi
Documentation Accessibility	xi
Related Documents	xii
Conventions	xiii
1 Oracle Content DB Administration Concepts	
About Oracle Content DB System Administration	1-1
Skills Required to Administer Oracle Content DB	1-1
Administrative Accounts	1-2
Oracle Content DB Administration Tools	1-2
Application Server Control	1-3
Accessing the Oracle Content DB Home Page	1-3
Oracle Content DB Administration Mode	1-5
Other Oracle Application Server Tools	1-5
Oracle Content DB System Administration Tasks Not Covered in This Guide	1-6
Oracle Content DB Architecture	1-6
Oracle Content DB Web Services	1-6
Oracle Content DB Application Architecture	1-7
Oracle Content DB Domain	1-7
Oracle Content DB Nodes	1-8
Services, Servers, and Agents	1-9
Oracle Content DB User Repository	1-10
Oracle Content DB Site	1-10
About the Oracle Content DB Protocol Servers	1-10
Using WebDAV with Oracle Content DB	1-11
Integration with Key Oracle Technologies	1-11
Integration with Oracle Database	1-11
Oracle Database and the Oracle Content DB Schema	1-11
Oracle Text	1-12
Oracle Streams Advanced Queueing	1-12
Oracle Real Application Clusters (Oracle RAC)	1-12
Integration with Oracle Application Server	1-12
Oracle Containers for J2EE (OC4J)	1-13
Oracle Process Manager and Notification Server (OPMN)	1-13

Oracle Enterprise Manager.....	1-13
Oracle BPEL Process Manager	1-14
About BPEL	1-14
Oracle Workflow	1-14
A Note for Windows Platforms	1-14

2 Planning for Oracle Content DB Deployment

Oracle Content DB Deployment Configurations.....	2-1
Single-Computer Deployment	2-1
Multiple-Computer Deployment.....	2-2
High Availability Considerations.....	2-3
Best Practices for High Availability of Agents in a Multiple Middle Tier Environment	2-3
Oracle Content DB Sizing Guidelines	2-4
Hardware Requirements.....	2-4
Sizing Formulas for Each Middle-Tier Computer.....	2-5
Number of CPUs.....	2-6
Required Usable Disk Space.....	2-6
Total Computer Memory, HTTP as the Primary Protocol.....	2-6
Total Computer Memory, Primary Protocol Other Than HTTP.....	2-7
Sizing Formulas for the Database Computer	2-8
Number of CPUs.....	2-8
Required Usable Disk Space.....	2-8
Total Computer Memory.....	2-9
Memory Requirements: Sample Deployment.....	2-9
Oracle Content DB Tablespaces	2-9
Data Types and Storage Requirements.....	2-10
Storing Files in an Oracle Database	2-11
Oracle Content DB Metadata and Infrastructure	2-13
Oracle Text	2-13
Disk Space Requirements: Sample Deployment	2-14

3 Oracle Content DB Security

SSL Configuration for Oracle Content DB.....	3-1
Setting Up SSL for Client Connections to Oracle Content DB.....	3-1
Setting Up SSL Between Oracle Content DB and the User Repository	3-2
Setting Up Server Only SSL Between Oracle Content DB and Your LDAP Server	3-2
Setting Up Anonymous SSL Between Oracle Content DB and Your LDAP Server	3-5
About User Authentication in Oracle Content DB.....	3-6
Authenticating as a Trusted Application Over Web Services	3-7
Setting Up a Server Keystore for WS-Security.....	3-7
About Oracle Content DB Access to the Server Keystore	3-7
Configuring a Server Keystore.....	3-7
Importing Client Public Keys Into the Server Keystore	3-9
Changing the Private Server Key and Keystore Passwords.....	3-9
Changing the Private Server Key Password	3-9
Changing the Keystore Password for WS-Security.....	3-10
Changing the LDAP Keystore Password.....	3-10

Changing the Oracle Content DB Schema Password.....	3-10
Security Considerations for HTTP/WebDAV	3-11
Network Channel Encryption	3-11
Preventing Malicious Uploads	3-11
Changing the Client Session Timeout Period	3-12
Applying the Latest Critical Patch Updates to Oracle Content DB.....	3-12

4 Choosing Oracle Content DB Options

Enabling Oracle Content DB Error Reporting and Site Quota Warning Notifications.....	4-1
Setting Up Antivirus Integration	4-2
Setting Up SAVSE	4-3
Enabling Antivirus Functionality in Oracle Content DB	4-3
Enabling Antivirus Functionality and Setting the Maximum Number of Repair Attempts ...	4-3
Configuring the Virus Repair Agent.....	4-4
Excluding Formats from Being Scanned.....	4-4
Performance Implications of Scanning for Viruses.....	4-4
Managing Storage Options.....	4-5
Data Aging and Archiving.....	4-5
Setting Up Data Aging	4-5
Setting Up Data Archiving	4-6
Specifying Storage Management Options	4-7
Changing the Oracle Content DB Port Number.....	4-8
Changing the Port Number in Oracle HTTP Server	4-8
Changing the Port Number in Oracle Content DB	4-8
Allowing Access to Oracle Content DB from Outside the Firewall.....	4-8
Changing a Middle-Tier Host Name or IP Address	4-9
Changing the Oracle Database URL.....	4-10
Using Oracle Drive with Oracle Content DB	4-10
Setting Up an Administrator-Configured Installation of Oracle Drive	4-11
Configuring Oracle Drive Service Details For Your Users	4-11
Setting Up config.xml.....	4-11
Setting Up update.xml	4-14
Setting Up odrive.ini	4-14
Preparing for Deployment Using Active Directory	4-15
Deploying Oracle Drive Using Active Directory	4-15
Redeploying Oracle Drive	4-16
Removing Oracle Drive from User Workstations	4-17
Packaging Service Information with the Oracle Drive Executable.....	4-17
Installing Oracle Drive	4-18
Customizing the New User Orientation	4-19

5 Managing Oracle Content DB Users

Using Oracle Internet Directory with Oracle Content DB.....	5-1
Logging In to Oracle Content DB for the First Time.....	5-1
Managing Users in Oracle Internet Directory	5-2

Using a Third-Party LDAP Server with Oracle Content DB	5-2
Logging In to Oracle Content DB for the First Time.....	5-2
Managing Users in a Third-Party LDAP Solution	5-3
Using a File-Based User Repository with Oracle Content DB	5-3
Logging In to Oracle Content DB for the First Time.....	5-3
Using a File-Based User Repository with Multiple Oracle Content DB Middle Tiers.....	5-3
Managing Users in a File-Based User Repository	5-4
Using the Application Server Control to Manage Users.....	5-4
Using the OracleAS JAAS Provider Admintool to Manage Users	5-4
User Provisioning in Oracle Content DB	5-5
Deleting Users in Oracle Content DB	5-5
Running the deleteuser Script.....	5-5
What Happens to User Content When a User Is Deleted?.....	5-6
Updating User Information in the Oracle Content DB Web Client.....	5-6
User Profile Information	5-6
User Preferences Information.....	5-6
Setting the First Name, Last Name, and E-mail Address Attributes.....	5-7

6 Using Custom BPEL Workflows in Oracle Content DB

About Custom Workflows	6-1
About BPEL.....	6-2
Creating Custom Workflows in Oracle BPEL Process Manager	6-2
Registering Custom Workflows with Oracle Content DB	6-2
Deleting Custom Workflows from Oracle Content DB.....	6-4

7 Managing Oracle Content DB Processes

About the Oracle Content DB Domain	7-1
Starting and Stopping the Oracle Content DB Domain	7-1
Starting the Domain.....	7-2
Restarting the Domain.....	7-2
Stopping the Domain.....	7-2
Managing Nodes at Run Time	7-3
Starting, Stopping, and Restarting OC4J_Content Instances.....	7-3
Modifying Nodes at Run Time	7-4
Managing Services at Run Time.....	7-4
Creating Services	7-5
Creating Services at Run Time	7-5
Permanently Adding Services to a Node	7-5
Modifying Run-Time Service Parameters	7-5
Changing the Service Configuration Used by the Service.....	7-6
Managing the Committed Data Cache.....	7-6
Making Run-Time Changes to Committed Data Cache Properties	7-7
Managing the Connection Pools	7-8
About the Statement Cache	7-8
Making Run-Time Changes to Connection Pool Properties.....	7-8
Deleting Services	7-11
Deleting Services at Run Time	7-11

Permanently Removing Services from a Node.....	7-11
Managing Servers at Run Time	7-11
Creating Servers	7-12
Creating Servers at Run Time	7-12
Permanently Adding Servers to a Node.....	7-12
Starting, Stopping, Restarting, Suspending, and Resuming Servers.....	7-13
Ensuring Servers Are Started When the Node Is Started	7-14
Modifying Run-Time Server Parameters.....	7-14
Changing the Server Configuration Used by the Server.....	7-15
Reloading Servers.....	7-15
Deleting Servers.....	7-16
Deleting Servers at Run Time.....	7-16
Permanently Removing Servers from a Node	7-16
Managing Oracle Content DB from the Command Line.....	7-16

8 Changing Oracle Content DB Configuration Settings

Managing Domain Properties.....	8-1
Changing Domain Properties.....	8-1
Managing Node Configurations	8-4
Modifying Node Configurations	8-5
Adjusting Java Parameters for Nodes.....	8-7
Managing Service Configurations	8-8
About Service Configurations	8-8
Creating Service Configurations.....	8-9
Modifying Service Configurations	8-10
Deleting Service Configurations	8-11
Managing Server Configurations.....	8-11
About Server Configurations	8-12
Changing Values of Inherited Properties	8-13
Viewing Inherited Properties.....	8-13
Creating Server Configurations	8-13
Modifying Server Configurations.....	8-15
Deleting Server Configurations	8-16

9 Monitoring Domain, Node, Service, and Server Performance

Monitoring Node Performance.....	9-1
Monitoring Service Performance	9-2
Logging Service Performance Information	9-4
Monitoring Server Performance	9-4
Viewing Logs.....	9-4
Oracle Content DB Logs.....	9-4
Viewing Oracle Content DB Logs from the Application Server Control.....	9-5
Changing the Log Level for Oracle Content DB Processes.....	9-5

10 Managing Oracle Content DB Formats

About Formats.....	10-1
---------------------------	-------------

Adding Formats	10-1
Modifying Formats	10-2
Deleting Formats	10-3
Default Formats	10-4
11 Managing the Oracle Content DB Site	
About the Oracle Content DB Site	11-1
Modifying Site Settings	11-1
Granting the Security Administrator Role	11-3
12 Oracle Content DB Maintenance and Tuning	
Backup and Recovery	12-1
Service Configurations and Java Memory Sizing	12-1
Calculating Xmx Settings	12-2
Adjusting Service Configuration Settings	12-3
Performance Tuning	12-3
Running the Oracle Content DB analyze.sql Script	12-3
Restoring Prior Statistics	12-4
Analyzing Performance Problems	12-4
If the Database Is Causing the Problem	12-4
If the Java Processes Are Causing the Problem	12-5
Viewing Cache Statistics and Changing Cache Settings	12-5
Viewing Connection Pool Statistics and Changing Connection Pool Settings	12-6
A Troubleshooting Oracle Content DB	
Solving General Administration Problems	A-1
Solving Performance Problems	A-4
B Migrating Content to Oracle Content DB	
Migration Tasks	B-1
Migrating Oracle Content DB Users	B-1
Creating Oracle Content DB Libraries	B-2
Scripted Library Creation	B-2
Migrating Oracle Content DB Content	B-2
How to Copy the Data	B-2
C Managing the Oracle Text Index	
Oracle Text Tablespaces and Disk Utilization	C-1
Creating and Maintaining the Oracle Text Index	C-2
Maintaining the IFS_TEXT Index by Using the Oracle Text PL/SQL Packages	C-2
Sync Job	C-3
Optimize Job	C-3
Monitoring DBMS_JOBS	C-3
Changing or Removing the Default DBMS_JOBS	C-3
Manually Synchronizing and Optimizing IFS_TEXT	C-4

Monitoring Oracle Text Indexing of Oracle Content DB Documents	C-4
Indexing Non-Standard Content Types.....	C-4
Modifying the Search Timeout Parameter	C-5
Troubleshooting Oracle Text Problems.....	C-5

D Service Configuration Properties

E Server Configuration Properties

Shared Properties	E-2
Background Request Agent.....	E-2
Cleanup Agent	E-3
Content Agent	E-4
Content Garbage Collection Agent.....	E-5
Dangling Object AV Cleanup Agent.....	E-5
Event Exchanger Agent	E-6
Expiration Agent.....	E-6
Folder Index Agent.....	E-6
Folder Index Analyzer Agent	E-7
Garbage Collection Agent	E-7
HTTP Server	E-7
Inbound Queue Listener Agent.....	E-9
Lock Expiration Agent.....	E-9
Most Recent Doc Agent.....	E-9
Quota Agent	E-9
Read Document Agent	E-10
Reassign Quota Agent.....	E-10
Refresh Security Agent	E-11
Service Warmup Agent.....	E-11
Service Watchdog Agent	E-11
Statistics Agent	E-12
User Connect Agent	E-12
Version Purge Agent	E-13
Virus Repair Agent.....	E-13

F Oracle Content DB Globalization Support

How to Choose the Database Character Set for Oracle Content DB	F-1
How to Ensure Documents Are Properly Indexed in Oracle Content DB	F-2
Character Set.....	F-2
Language	F-2
Globalization and the Oracle Content DB Protocols	F-3
Character Sets Supported in Oracle Content DB	F-4
Document Languages Supported in Oracle Content DB	F-6

Glossary

Index

Preface

Oracle Content Database (Oracle Content DB) is a consolidated, database-centric content management application that provides a comprehensive, integrated solution for file and document lifecycle management. Oracle Content DB provides both Windows and Web interfaces. This release of Oracle Content DB ships with Oracle WebCenter Suite, a set of tools and services that you can use to build applications that are transactional, analytical, and dynamic in a product context.

Oracle Content DB runs on Oracle Application Server and Oracle Database, and provides a scalable content management repository. Oracle Content DB also offers a comprehensive set of Web services that developers can use to build and enhance content management applications.

Audience

This document is intended for system administrators, or anyone involved in configuring, running, and maintaining an Oracle Content DB instance. Oracle Content DB application administrators, such as Quota or Content Administrators, should refer to *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite* for information about application administration tasks.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

For more information, see the following documents:

Oracle Content DB

- *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite*
- Oracle Content Database developer documentation, available on Oracle Technology Network (OTN) at:

<http://www.oracle.com/technology/products/contentdb/>

Oracle WebCenter Framework

- *Oracle WebCenter Framework Developer's Guide*
- *Oracle WebCenter Framework Error Messages Guide*
- *Oracle WebCenter Framework Tutorial*

Oracle Application Server

- *Oracle Application Server Concepts*
- *Oracle Application Server Installation Guide* for your platform
- *Oracle Application Server Release Notes* for your platform
- *Oracle Application Server Administrator's Guide*
- *Oracle Application Server Performance Guide*
- *Oracle HTTP Server Administrator's Guide*
- *Oracle BPEL Process Manager Developer's Guide*
- *Oracle Internet Directory Administrator's Guide*

Oracle Database

- *Oracle Database Administrator's Guide*
- *Oracle Database Concepts*
- *Oracle Database Advanced Security Administrator's Guide*
- *Oracle Database Performance Tuning Guide*
- *Oracle Database Backup and Recovery User's Guide*
- *Oracle Database Net Services Administrator's Guide*
- *Oracle Database Globalization Support Guide*

- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*
- *Oracle Text Reference*

Conventions

The following text conventions are used in this document:

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

Oracle Content DB Administration Concepts

This chapter explains key architectural and administration concepts related to Oracle Content DB.

This chapter provides information about the following topics:

- [About Oracle Content DB System Administration](#)
- [Oracle Content DB Architecture](#)
- [About the Oracle Content DB Protocol Servers](#)
- [Integration with Key Oracle Technologies](#)

About Oracle Content DB System Administration

Typically, Oracle Content DB **system administrators** are responsible for the following tasks:

- Planning for Oracle Content DB deployment
- Installing and configuring Oracle Content DB
- Optionally customizing their Oracle Content DB deployment by enabling an antivirus solution, **BFILE** archiving or aging, and other options
- Managing the Oracle Content DB **domain**, **nodes**, **services**, and **servers**
- Performing system tuning and troubleshooting
- Managing the Oracle Content DB **Site**
- Managing custom **BPEL** workflows

Note: Oracle Content DB **application administrators** are responsible for tasks such as managing users, quotas, categories, and content. There are a variety of application administration roles, such as the Category Administrator, Configuration Administrator, and Security Administrator. Users with one or more application administration roles should refer to *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite* for information about application administration tasks.

Skills Required to Administer Oracle Content DB

System administrators need to have the following skills:

- **Basic Oracle Database administration experience.** Because the file system is stored in an Oracle database, administrators need to understand the basics of how to administer the database, including knowledge of [Oracle Text](#).
- **Knowledge of Internet and intranet protocols.** Administrators need to understand how [HTTP](#), [WebDAV](#), and the other networking protocols work.
- **Oracle Application Server administration experience.** Administrators need to understand how to administer the various components of Oracle Application Server, such as [Oracle HTTP Server](#) and Oracle Containers for J2EE ([OC4J](#)), using administrative tools such as the [Application Server Control](#) and `opmnctl`.

Administrative Accounts

[Table 1–1](#) is a summary of the administrative accounts used by system administrators.

Table 1–1 Administrative Accounts

Account Name	Purpose	Notes
oc4jadmin	Used to access the Application Server Control.	The password is set during Oracle Content DB middle-tier installation.
contentadmin	Used to access Oracle Content DB after installation. You only use this account if you are using a file-based user repository.	This user has all the application administrator roles for Oracle Content DB. The initial password is the same as the Oracle Content DB schema password. You can use this account to create new users for a file-based user repository using the OracleAS JAAS Provider Admintool. See " Managing Users in a File-Based User Repository " on page 5-4 for more information.
orcladmin	Used to access Oracle Content DB after installation. You only use this account if you are using Oracle Internet Directory as your user repository.	This user has all the application administrator roles for Oracle Content DB. The password was entered during OracleAS Infrastructure installation. You can use this account to create new users for an Oracle Internet Directory user repository using the Oracle Internet Directory Self-Service Console (<code>oiddas</code>). See <i>Oracle Identity Management Guide to Delegated Administration</i> for more information.
Third-party LDAP server administrator user	Used to access Oracle Content DB after installation. You only use this account if you are using a third-party LDAP server as your user repository.	This user has all the application administrator roles for Oracle Content DB. You provided the name and password of this user during Oracle Content DB installation. You can use this account to create new users for a third-party LDAP user repository using the administration tools provided with your LDAP server. Refer to the documentation for your LDAP server for more information.

Oracle Content DB Administration Tools

Several administration tools are provided with Oracle Content DB, including browser-based management tools and command-line tools. Using these administration tools, you can:

- Start and stop domains and nodes

- Manage service and server objects
- Work from the command line
- Monitor domain, service, and node performance

The following sections describe the administration tools available to Oracle Content DB administrators:

- [Application Server Control](#)
- [Oracle Content DB Administration Mode](#)
- [Other Oracle Application Server Tools](#)

Application Server Control

Oracle Enterprise Manager 10g Application Server Control (Application Server Control) provides access to basic Oracle Content DB process management and monitoring functions, such as monitoring and dynamically tuning the domain, nodes, services, and servers. You can also use the Application Server Control to create users for a file-based user repository.

Typically, you can access the Application Server Control at the following URL:

`http://host:port/em`

Use the `oc4jadmin` account to log in.

See *Oracle Application Server Administrator's Guide* for more information about how to access the Application Server Control.

Note: Oracle HTTP Server and the "home" instance must both be started before you can access the Application Server Control.

Accessing the Oracle Content DB Home Page Most Oracle Content DB tasks in the Application Server Control can be performed from the Content DB Home page. The steps to access the Content DB Home page can vary, depending on whether you want to perform general Oracle Content DB tasks, such as configuring domain properties, modifying Site settings, or managing server configurations, or whether you want to perform tasks related to a particular node, service, or server.

To access the Content DB Home page for administration tasks related to a particular node, service, or server:

1. Connect to the Application Server Control on the middle tier where you want to manage Oracle Content DB processes.
2. On the Cluster Topology page, in the Members table, click the **plus** icon next to the node (OC4J_Content instance) that relates to the particular task you want to perform.

You cannot expand the OC4J_Content instance unless it is running. To start the OC4J_Content instance, select it and click **Start**.

3. Under the OC4J_Content heading, click **content**.
4. On the Application:content page, in the Related Links section, click **Content DB Extension**. The Content DB Home page appears and displays information about the particular node (OC4J_Content instance) you expanded in Step 2.


[Figure 1–1](#) shows the Content DB Home page.

Figure 1–1 Content DB Home Page

Content DB: content Page Refreshed Aug 29, 2006 5:54:29 PM CDT

Home [Performance](#) [Administration](#)

General



Status **Up**
 Version **10.1.3.2.0**
 Database Service **orcl**
[▶ Show Database Connect Descriptor](#)
 Schema **CONTENT**
 Node Configuration **Aug29basoid.stbec05.us.oracle.com_HTTP_Node**

Services

Delete | Create

Select	Name ▲	JDBC Driver	Accepting New Sessions	Auto Disposed	Connected Sessions	Max Concurrent Sessions
<input checked="" type="radio"/>	IfsDefaultService	oci8	✓		19	40

Servers

Status Legend: ▶ Started ■ Stopped ▶ Starting □ Stopping ■ Suspended

Start Stop Restart Suspend Resume Reload Delete | Create ◀ Previous 1-10 of 24 Next 10 ▶

Select	Name ▲	Type	Status	Last Start Time	Last Stop Time	Service	Priority
<input checked="" type="radio"/>	BackgroundRequestAgent	AGENT	▶	Aug 29, 2006 5:36:57 PM CDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	CleanupAgent	AGENT	▶	Aug 29, 2006 5:37:03 PM CDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	ContentAgent	AGENT	■	Unavailable	Unavailable	IfsDefaultService	5

To access the Content DB Home page for general Oracle Content DB administration tasks:











1. Connect to the Application Server Control.
2. On the Cluster Topology page, in the Members table, click the **plus** icon next to one of the OC4J_Content instances. It does not matter which OC4J_Content instance you choose to expand.

You cannot expand the OC4J_Content instance unless it is running. To start the OC4J_Content instance, select it and click **Start**.
3. Under the OC4J_Content heading, click **content**.
4. On the Application:content page, in the Related Links section, click **Content DB Extension**. The Content DB Home page appears. Most general administration tasks can be performed from the **Administration** tab.

Figure 1–2 shows the Administration tab of the Content DB Home page.

Figure 1–2 Administration Tab of the Content DB Home Page

Content DB: content Page Refreshed Aug 29, 2006 5:58:38 PM CDT

Home Performance Administration		
Task Name	Go to Task	Description
Domain Properties		Configure domain properties.
Node Configurations		Manage node configurations in the domain.
Service Configurations		Manage service configurations in the domain.
Server Configurations		Manage server configurations in the domain.
Site Management		Configure Site settings.
Site Security		Grant the security role for the Site.
Custom Workflows		Manage custom BPEL workflows.
Formats		Configure formats in the domain.
Retention Hardware		Set connection credentials for a retention storage device.
Storage Management		Configure BFILE storage settings.

Home Performance Administration

Oracle Content DB Administration Mode

Oracle Content DB **Administration Mode** provides access to application administration functions such as allocating quota and assigning roles. To access Administration Mode, log in to the Oracle Content DB Web client as a user with one or more application administration roles, then click **Switch to Administration Mode**. See *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite* for more information.

Other Oracle Application Server Tools

The following Oracle Application Server tools can be used to perform some Oracle Content DB tasks:

- You can use the `opmnctl` utility to start and stop Oracle Content DB, the Application Server Control, OC4J processes, and Oracle HTTP Server. You can access `opmnctl` from `ORACLE_HOME/opmn/bin/`.
See *Oracle Process Manager and Notification Server Administrator's Guide* for more information about using the `opmnctl` tool.
- If you are using a file-based user repository with Oracle Content DB, you can use the OracleAS JAAS Provider Admintool to manage users. The Admintool is a lightweight Java application that provides administration for users, roles, policies, and login modules for a file-based user repository. However, you must restart `OC4J_Content` for changes made by the Admintool to take effect.
- If you are using Oracle Internet Directory as your Oracle Content DB user repository, you can use a variety of Oracle Internet Directory administration tools to manage users. For example, you can use Oracle Internet Directory command-line tools like `ldapadd` and `ldapmodify`, you can use the Oracle Internet Directory Self-Service Console (`oiddas`), or you can use Oracle Directory Manager.

See *Oracle Identity Management Guide to Delegated Administration* for information about how to use the Oracle Internet Directory Self-Service Console; *Oracle Identity Management User Reference* for information about how to use Oracle Internet Directory command-line tools; and *Oracle Internet Directory Administrator's Guide* for information about how to use Oracle Directory Manager.

Oracle Content DB System Administration Tasks Not Covered in This Guide

Some Oracle Content DB system administration tasks are not covered in this guide. The following table explains what these tasks are, and where to go for more information.

Table 1–2 System Administration Tasks and Information Not Covered in This Guide

Task	Where to Go for More Information
Installing Oracle Content DB	<i>Oracle Application Server Installation Guide</i> for your platform
Setting up a load balancer	<i>Oracle Application Server Enterprise Deployment Guide</i>
Getting started after installing Oracle Content DB	<i>Oracle Application Server Installation Guide</i> for your platform
Accessing shared administrative tools, such as the Application Server Control	<i>Oracle Application Server Administrator's Guide</i>
Setting up the Oracle Content DB JCR Adapter	<i>Oracle WebCenter Framework Developer's Guide</i>
Client and other certification information	OracleMetaLink (http://metalink.oracle.com) <i>Oracle Application Server Certification Information</i>

Oracle Content DB Architecture

The following sections describe the underlying technology for Oracle Content DB, and explain how the Oracle Content DB nodes and other processes interact. Information is also provided about user repositories and the Oracle Content DB Site.

This section contains the following topics:

- [Oracle Content DB Web Services](#)
- [Oracle Content DB Application Architecture](#)
- [Oracle Content DB Domain](#)
- [Oracle Content DB User Repository](#)
- [Oracle Content DB Site](#)

Oracle Content DB Web Services

Oracle Content DB offers a comprehensive set of Web services that developers can use to build and enhance applications to provide sophisticated content management capabilities.

These Web services provide a large number of API calls for content and records management. The Web services also support the extensive business process automation capabilities provided by Oracle BPEL Process Manager.

Developers can use the Oracle Content DB Web services to:

- Build custom applications that leverage Oracle Content DB to manage unstructured data
- Script and automate content-based operations
- Build custom BPEL-based workflows and use them to drive and respond to Web service invocations

To see a list of available services descriptions, open a Web browser and go to the following URL:

`http://host_name:port/content/ws/wsdl`

To download developer documentation and sample code, see the Oracle Content DB product page on the Oracle Technology Network (OTN) at:

<http://www.oracle.com/technology/products/contentdb/index.html>

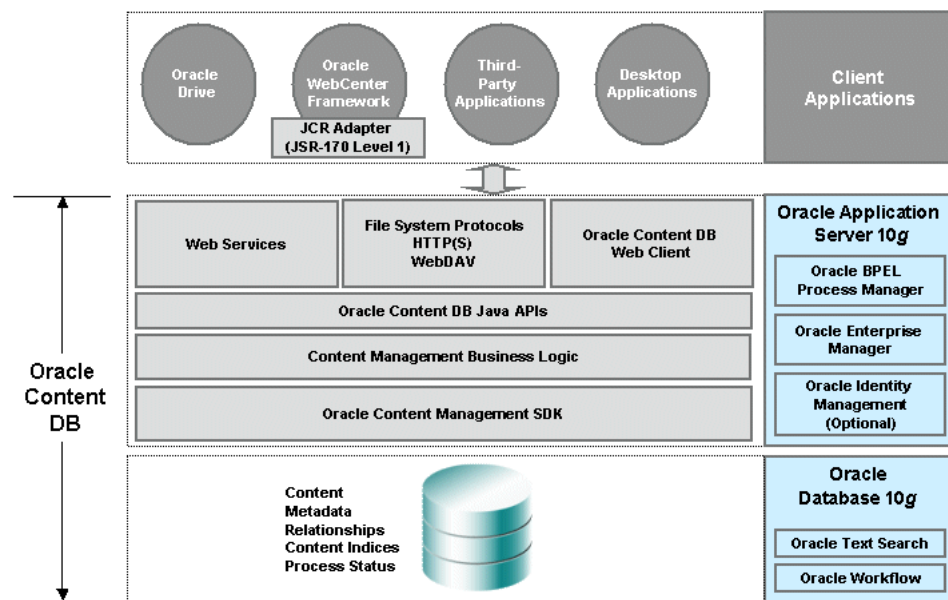
Note: The Oracle Content DB Web services use the Axis framework, not the Oracle Application Server Web Services framework. Because of this, in the Application Server Control, the Oracle Content DB Web services do not appear in the Web Services tab for OC4J_Content.

Oracle Content DB Application Architecture

A Java API layer provides a uniform interface that encompasses content management business logic. This layer is the foundation for the Oracle Content DB Web application, protocol servers, and Web services. The Java API layer ensures that all components interfacing to Oracle Content DB do so at an abstraction level that respects the application business logic.

Oracle WebCenter Framework comes with an Oracle Content DB JCR Adapter that provides JSR-170 Level 1 support. You can use Oracle WebCenter Framework to configure this adapter so that you can access content stored in Oracle Content DB with the Oracle Content DB Data Control. See *Oracle WebCenter Framework Developer's Guide* for more information.

Figure 1–3 Oracle Content DB Application Architecture



Oracle Content DB Domain

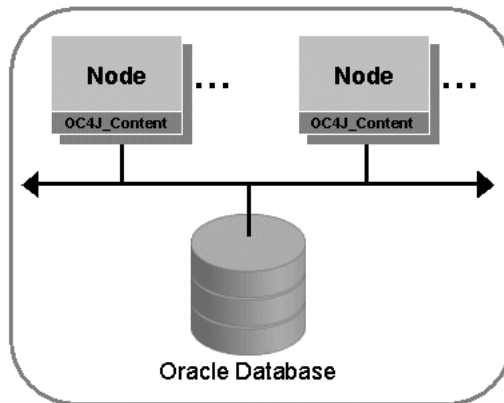
An Oracle Content DB **domain** is a logical grouping of Oracle Content DB **nodes** and an Oracle Database instance that contains the Oracle Content DB data. The nodes run on Oracle Application Server. The Oracle Content DB node processes and the database

can be physically configured on a single computer or across several, separate computers.

The Oracle Content DB **schema** is created in the Oracle Database during the configuration process. The schema owns all database objects, including metadata about Oracle Content DB and configuration information. You cannot have more than one Oracle Content DB schema in the same database.

Figure 1–4 shows the Oracle Content DB domain.

Figure 1–4 The Oracle Content DB Domain



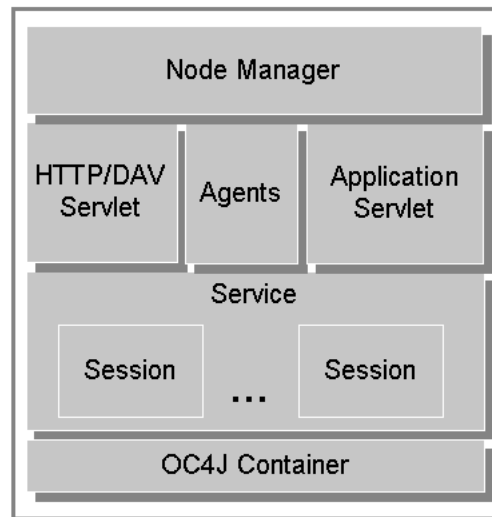
Oracle Content DB Nodes

An Oracle Content DB **node** is the application software that comprises the product, along with the underlying Java Virtual Machine (JVM) required to support the software at run time.

Important concepts to understand about nodes include:

- After installation, each Oracle Content DB middle tier includes one node by default that supports the Oracle Content DB application.
- Each node supports protocol servers, such as HTTP, and agents, such as the Garbage Collection Agent.
- Nodes support the Oracle Content DB application, WebDAV, Oracle Drive, and the Web services using servlets that are configured to work with OC4J.
- The OC4J process for each node is guarded by OPMN, which restarts the OC4J process if it is stopped unexpectedly.
- Each node has a node manager. It is responsible for starting the default services and servers for the node. It also provides an administrative API for the node that lets you find information about node log levels, locale information, available free memory, and the Oracle home for the node.

Figure 1–5 shows an Oracle Content DB node.

Figure 1–5 An Oracle Content DB Node

Services, Servers, and Agents

Each node supports a **service** that has specific configuration parameters, such as credential managers, connections to the database, and cache sizes. By default, a single service starts on each node, and that service supports all protocol servers and agents for that node.

The **servers** supported by the service can be either protocol servers or agents. The protocol servers listen for requests from clients on a specific port and respond to requests according to the rules of the protocol specification. By default, each protocol server listens on the industry standard well-known port and adheres to the specification of the protocol server.

Agents perform operations periodically (time-based) or in response to events generated by other Oracle Content DB servers or processes (event-based). For example, the Content Garbage Collection Agent deletes content no longer associated with any document in Oracle Content DB. It does this based on an activation period parameter specified in the server configuration object.

Although different agents can run on different nodes, each agent must run only on a single node, except the Service Warmup Agent and the Statistics Agent. These agents must be running on all nodes. Typically, most of the shipped agents must be run to ensure a stable system. See [Appendix E, "Server Configuration Properties"](#) for more information about particular agents.

The Oracle Content DB architecture is flexible: services and servers are not coupled so that you can configure services, protocol servers, and agents across a wide array of hardware. For example, you can run all protocol servers on one node, and run all agents on another node; or, they can all run on the same node.

An initial domain and node configuration is set up for you during Oracle Content DB configuration, but you can change this later. You can configure the protocol servers and other processes at any point using the Application Server Control.

See [Appendix D, "Service Configuration Properties"](#) for information about service configuration parameters. See [Appendix E, "Server Configuration Properties"](#) for information about server configuration parameters.

Oracle Content DB User Repository

Oracle Content DB supports three options for its user repository:

- Oracle Internet Directory, a component of Oracle Identity Management
- A third-party LDAP solution, such as Open LDAP or Microsoft Active Directory
- File-based user repository

See [Chapter 5, "Managing Oracle Content DB Users"](#) for more information about choosing a user repository for Oracle Content DB.

Oracle Content DB Site

The Oracle Content DB Site is an organizational entity that is used to manage settings for all Oracle Content DB users. There are a designated set of application administrators for the Site who can manage quota, specify Site settings, and perform other tasks. See *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite* for more information.

The Oracle Content DB Site is created during Oracle Content DB installation and configuration. See [Chapter 11, "Managing the Oracle Content DB Site"](#) on page 11-1 for information about managing Site settings at the system administration level.

About the Oracle Content DB Protocol Servers

Users can connect to Oracle Content DB using protocols appropriate to their platform. For example, Windows users can use the Oracle Drive client or connect using Web Folders, and Macintosh users can connect through WebDAV. Users on all platforms can connect using HTTP for browser-based access.

Oracle Content DB supports the following protocols:

- **HTTP** is used for browser-based access. Use the following URL to access Oracle Content DB with HTTP, using the Oracle Content DB Web client:

```
http://server_name:port/content
```

- **WebDAV**, Web-based Distributed Authoring and Versioning, is an HTTP-related protocol that is designed for wide area networks such as the Internet. Currently, the most widespread WebDAV client is the Web Folders extension to Windows Explorer, also known as Network Places in Windows 2000 and Windows XP. Oracle Content DB also provides WebDAV support for Macintosh users.

The Oracle Drive client provides Windows users with SMB-like drive mapping capabilities, while using WebDAV as the actual file protocol. See ["Using Oracle Drive with Oracle Content DB"](#) on page 4-10 for more information about Oracle Drive.

[Table 1–3](#) lists some of the client platforms, protocols, and access methods supported by Oracle Content DB. See *Oracle MetaLink* at <http://metalink.oracle.com> for complete client certification information.

Table 1–3 Client Platforms and Protocol Support

Client Platform	Protocols Supported	Access Using ¹
Windows	HTTP, WebDAV	Browser, Oracle Drive, Windows Explorer
Macintosh (Mac OS 10.3)	HTTP, WebDAV	Browser, WebDAV client

Table 1–3 (Cont.) Client Platforms and Protocol Support

Client Platform	Protocols Supported	Access Using ¹
UNIX	HTTP	Browser
Red Hat Linux Adv. Server 3.0 (Kernel 2.4.9-e.16)	HTTP	Browser

¹ For all protocols, if the server to which you are connecting uses DHCP, then you must use the current IP address of the host in the connection syntax instead of the host name.

Using WebDAV with Oracle Content DB

The WebDAV protocol is enabled, by default, after Oracle Content DB is installed and configured.

Note that if you define a policy on a folder or Library that requires users to enter data associated with uploaded content, users will not be able to place content in that folder or Library using WebDAV. This limitation is because the WebDAV protocol does not provide a facility to enter metadata.

Use the following URL to access Oracle Content DB with WebDAV:

```
http://server_name:port/content/dav
```

The value for *port* varies depending on your platform. On UNIX systems, the port number is typically 7778. On Windows systems, the port number is typically 80, unless 80 is in use when the middle tier is configured.

To check the port number, use the following `opmnctl` command:

```
opmnctl status -l
```

You can run the `opmnctl` command-line tool from `ORACLE_HOME/opmn/bin`.

Note that users with multibyte user names cannot sign on to Oracle Content DB using WebDAV. For this reason, you should not create Oracle Content DB user names that contain multibyte characters.

Integration with Key Oracle Technologies

Oracle Content DB uses the capabilities of both the Oracle Database and Oracle Application Server.

This section contains the following topics:

- [Integration with Oracle Database](#)
- [Integration with Oracle Application Server](#)

Integration with Oracle Database

Oracle Content DB uses Oracle Database to store all content and metadata.

Oracle Database and the Oracle Content DB Schema

All content and metadata about the Oracle Content DB instance is stored in an Oracle database. These objects, including tablespaces, tables, indexes, views, sequences, and procedures owned by the schema, provide the underpinnings of a fully functioning system.

There is an additional schema created to ensure secure connectivity to other systems. The name for the additional schema is derived from the Oracle Content DB schema name. For example, if the Oracle Content DB schema name is `CONTENT`, the additional schema is `CONTENT$CM`.

User content, such as word processing files, spreadsheets, sound files, and presentations, is stored by Oracle Content DB in the database as large objects (LOBs).

LOBs enable fast access and optimized storage for large bits of content, often binary, stored in the database. Otherwise, all content in the Oracle Content DB schema is stored as standard data types in various tables.

Oracle Text

Oracle Text is full-text retrieval technology built into Oracle Database for indexing and searching text and documents. Oracle Text supports mixed languages and character sets in the same index. Oracle Content DB uses the text indexing and retrieval features of Oracle Text.

Oracle Streams Advanced Queueing

Oracle Streams Advanced Queueing provides an infrastructure for distributed applications to communicate asynchronously using messages. Oracle Streams Advanced Queueing is built into Oracle Database.

Oracle Content DB uses Oracle Streams Advanced Queueing to integrate with Oracle Workflow and Oracle BPEL Process Manager.

Oracle Real Application Clusters (Oracle RAC)

A cluster is a group of computers that work together and behave as a single system. Clustering requires both hardware (interconnect) and software (clusterware) support. In the past, clusters were used in high availability read-only applications, such as data warehouses. Now, clusters are increasingly becoming a lower-cost approach for computing applications that require high availability and scalability.

An Oracle Real Application Cluster consists of two or more computers configured to interact and provide the appearance of a single Oracle database. These Oracle RAC nodes are linked by an interconnect. The interconnect serves as the communication path between each node in the cluster database. Each Oracle Database instance uses the interconnect for the messaging that synchronizes each instance's use of shared resources. Oracle also uses the interconnect to transmit data blocks that are shared by the multiple instances. The data files accessed by all the nodes are the primary type of shared resource.

Oracle RAC requires that all nodes have simultaneous access to the shared disks to give the instances concurrent access to the database. The implementation of the shared disk subsystem is based on your operating system: you can use either a cluster file system, or place the files on raw devices. Cluster file systems simplify the installation and administration of Oracle Real Application Clusters.

For more information about Oracle RAC, see *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*.

Integration with Oracle Application Server

Oracle Content DB is designed to integrate with several components from the Oracle Application Server product family, including OC4J and the Application Server Control.

Oracle Containers for J2EE (OC4J)

OC4J is a J2EE-compliant application server that supports Java Server Pages (JSP), Java servlets, and many other APIs from the Java 2 Platform, Enterprise Edition (J2EE). Services are deployed to an OC4J instance using XML-based configuration files as standard Web Application Archive (.WAR), Enterprise Application Archive (.EAR), Resource Adapter Archive (.RAR), and Java Archive (.JAR) files. Oracle Content DB uses the Java Servlet and the run-time environment of OC4J to support the HTTP/WebDAV servlet and Web services.

OC4J is automatically configured for Oracle Content DB nodes as part of the Oracle Content DB configuration process. You can manage OC4J through the Application Server Control.

Oracle Process Manager and Notification Server (OPMN)

OPMN manages all the components within an application server instance, including Oracle HTTP Server and OC4J processes. It channels all events from different components to all components interested in receiving them.

OPMN provides the following functionality:

- Provides a command-line interface for process control and monitoring for single or multiple Oracle Application Server components and instances.
- Provides an integrated way to manage Oracle Application Server components.
- Solves interdependency issues between Oracle Application Server components by enabling you to start and stop components in order.
- Provides automatic restart of Oracle Application Server processes when they become unresponsive, terminate unexpectedly, or become unreachable as determined by ping and notification operations.

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

Note: On the Microsoft Windows operating system, OPMN is installed as a Windows service (Oracle<OracleHomenam>ProcessManager). It starts up automatically when you start or restart your computer.

You can use the OPMN command-line tool, `opmnctl`, to manage Oracle Content DB. For complete information about `opmnctl` syntax and usage, see *Oracle Process Manager and Notification Server Administrator's Guide*.

Oracle Enterprise Manager

Oracle Enterprise Manager is a systems management software application that enables you to manage and monitor Oracle Application Server instances and other Oracle products.

You can use the Oracle Enterprise Manager 10g Application Server Control (Application Server Control) to manage Oracle Content DB middle-tier hosts. For example, you can use the Application Server Control to operate and monitor system processes associated with the Oracle Content DB domain and nodes.

You can access the Application Server Control using a Web browser from anywhere on the network. The first page you see is the Cluster Topology page, which lets you view the OC4J instances in your Oracle Application Server cluster. See "[Accessing the Oracle](#)

[Content DB Home Page](#)" on page 1-3 for information about how to get to the Oracle Content DB Home page from the Cluster Topology page.

Oracle BPEL Process Manager

Oracle BPEL Process Manager provides a framework to design, deploy, monitor, and administer processes based on BPEL standards. You can define custom BPEL workflows in Oracle BPEL Process Manager, and then register them for use in Oracle Content DB. Custom workflows are only available to the default Site in Oracle Content DB; additional Sites cannot use the custom workflows. See [Chapter 6, "Using Custom BPEL Workflows in Oracle Content DB"](#) for detailed information.

About BPEL The Business Process Execution Language (BPEL) is an XML-based language for enabling task-sharing across multiple enterprises using a combination of Web services. BPEL is based on the XML schema, Simple Object Access Protocol (SOAP), and Web Services Description Language (WSDL). Using BPEL, you can design a business process that integrates a series of discrete services into an end-to-end process flow. For more information about BPEL and Oracle BPEL Process Manager, see *Oracle BPEL Process Manager Developer's Guide*.

Oracle Workflow

Oracle Workflow is business-process automation software. You can use Oracle Workflow to automate the process of routing and approving information, according to business rules you specify. Oracle Content DB integrates with Oracle Workflow to support the default workflow processes shipped with Oracle Content DB.

You can view workflow notifications by accessing the Oracle Content DB Reports feature.

A Note for Windows Platforms

This guide typically uses a forward slash (/) when documenting directory locations or commands. If you are running Oracle Content DB on Windows, make sure to change the slashes to back slashes (\) when typing the paths or commands. For example, this guide provides the following instructions:

At the command prompt, go to `ORACLE_HOME/content/bin` and run the following command:

```
./changepassword -p
```

If you are running Oracle Content DB on Windows, you should read these instructions as:

At the command prompt, go to `ORACLE_HOME\content\bin` and run the following command:

```
.\changepassword -p
```

Planning for Oracle Content DB Deployment

This chapter explains how to plan for an Oracle Content DB deployment.

This chapter provides information about the following topics:

- [Oracle Content DB Deployment Configurations](#)
- [Oracle Content DB Sizing Guidelines](#)
- [Oracle Content DB Tablespaces](#)

Oracle Content DB Deployment Configurations

This section describes the two types of Oracle Content DB deployment and provides information about high availability considerations.

This section contains the following topics:

- [Single-Computer Deployment](#)
- [Multiple-Computer Deployment](#)
- [High Availability Considerations](#)

See *Oracle Containers for J2EE Deployment Guide* for more information about OC4J application deployment options.

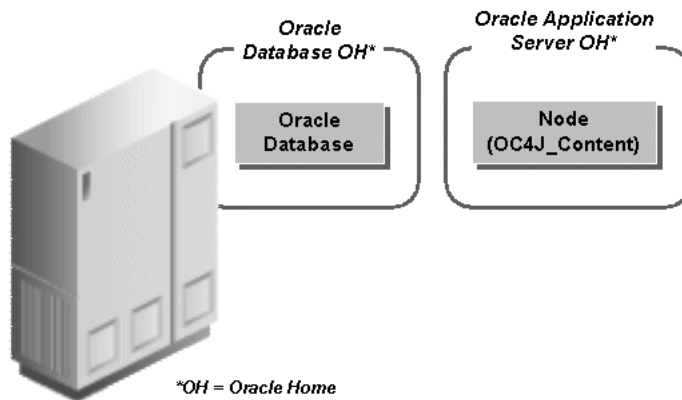
Single-Computer Deployment

Oracle Content DB can be installed on a single computer if the computer meets the recommended hardware and software requirements. If your computer does not meet the recommended requirements, the performance of this configuration might be less than satisfactory. See *Oracle Application Server Installation Guide* for your platform for more information about hardware and software requirements.

In a single-computer deployment, Oracle Content DB and all required components are installed on a single computer. These components include Oracle Application Server and Oracle Database. A single-computer deployment does not allow you to use load balancing or failover options.

[Figure 2-1](#) shows an Oracle Content DB domain running on a single computer.

Figure 2–1 A Single-Computer Oracle Content DB Deployment



See "[Oracle Content DB Nodes](#)" on page 1-8 for more information about the Oracle Content DB node process shown in [Figure 2–1](#).

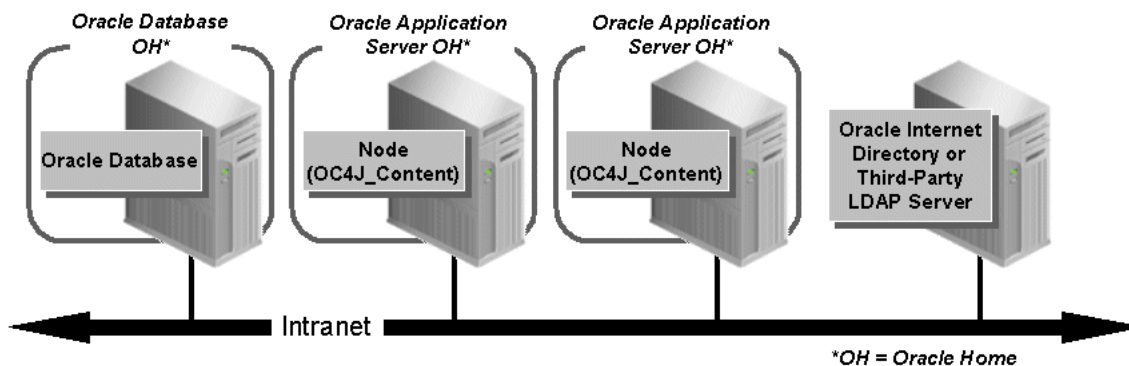
Multiple-Computer Deployment

Oracle Content DB can be deployed on multiple computers. This configuration enables you to separate the components, and configure failover, load balancers, and high availability options. With multiple-computer deployment, you can also use computers with lower hardware requirements than required for single-computer deployment. See *Oracle Application Server Installation Guide* for your platform for more information about hardware requirements.

With the appropriate network load balancers and computer configuration, users may not know whether the Oracle Content DB instance is running on one host or across several hosts. Users access content, such as folders and files, using the appropriate client application for a particular Oracle Content DB protocol server.

[Figure 2–2](#) is an example of a multiple-computer deployment, with Oracle Content DB components distributed across three computers.

Figure 2–2 A Multiple-Computer Oracle Content DB Deployment



See "[Oracle Content DB Nodes](#)" on page 1-8 for more information about the Oracle Content DB node processes shown in [Figure 2–2](#).

Most Oracle Content DB agents can only run on one middle tier at a time. However, agents can be deployed on multiple middle tiers in an inactive state, and activated if

the middle tier on which they were running fails. See the following section for more information.

High Availability Considerations

When you first configure Oracle Content DB, the first middle tier that you configure contains important configuration settings that are not stored in subsequent middle tiers. Because of this, if you choose to deinstall the first Oracle Content DB middle tier, or if the first middle tier goes down, you must ensure these configuration settings are restored on another middle tier.

The following list is a summary of these configuration settings:

- If you were running some or all of the Oracle Content DB agents on a particular middle tier that is deinstalled or becomes unavailable, you must configure these agents to run elsewhere. To do this, modify the node configuration of a node running on another Oracle Content DB middle tier. See ["Modifying Node Configurations"](#) on page 8-5 for more information. See also ["Best Practices for High Availability of Agents in a Multiple Middle Tier Environment"](#) in the following section.
- The `IFS.DOMAIN.APPLICATION.ApplicationHost` domain property points to a particular middle tier (typically the first that was configured). If that middle tier is deinstalled or becomes unavailable, you must update this domain property to point to another Oracle Content DB middle tier. See ["Changing Domain Properties"](#) on page 8-1 for more information.
- If you were using Oracle Mail as your SMTP server, and you were running Oracle Mail on a particular middle tier that is deinstalled or becomes unavailable, you must update the `IFS.DOMAIN.EMAIL.SmtpHost` and `IFS.DOMAIN.EMAIL.SmtpPort` domain properties to point to another SMTP server. See ["Changing Domain Properties"](#) on page 8-1 for more information.

Best Practices for High Availability of Agents in a Multiple Middle Tier Environment

By default, all the Oracle Content DB agents are running on the first middle tier that was configured. If you have multiple middle tiers, you should configure the agents to run separately from the Oracle Content DB Web application. Otherwise, if an agent goes down and you need to restart the OC4J_Content instance where the agents are running, the Oracle Content DB Web client, WebDAV access, and Web services will also go down.

Follow these steps to run your agents on a different node than your Web application:

1. Install and configure Oracle Content DB on the first middle tier. All the agents and the Web application (`EcmHttpServer`) run on this middle tier by default.
2. Leave the agents running, but disable the Web application (`EcmHttpServer`) on this middle tier. To do this, follow these steps:
 - a. Connect to the Application Server Control and go to the Content DB Home page. See ["Accessing the Oracle Content DB Home Page"](#) on page 1-3 for information about how to do this.
 - b. On the Content DB Home page, click the **Administration** tab.
 - c. In the Node Configurations table row, click the **Go to Task** icon.
 - d. On the Node Configurations page, click the name of the node configuration where the `EcmHttpServer` is running.

- e. On the Edit Node Configuration page, in the Servers section, click **Activate/Deactivate**.
 - f. Move **EcmHttpServer** from the Active Servers list to the Inactive Servers list and click **OK**.
 - g. Click **OK** on the Edit Node Configuration page.
 - h. Return to the Cluster Topology page, select the **OC4J_Content** instance, and click **Restart**.
3. Install and configure Oracle Content DB on the second middle tier. By default, all agents are disabled, but the Web application (`EcmHttpServer`) is running.
 4. Install and configure additional Oracle Content DB middle tiers, as needed. By default, all agents are disabled, but the Web application (`EcmHttpServer`) is running on these middle tiers.
 5. Optionally, configure a load balancer for the middle tiers running the Web application.

Oracle Content DB Sizing Guidelines

This section describes hardware requirements for a sample deployment of Oracle Content DB and formulas that allow you to determine the hardware configuration required to deploy Oracle Content DB in your organization.

This section includes the following topics:

- [Hardware Requirements](#)
- [Sizing Formulas for Each Middle-Tier Computer](#)
- [Sizing Formulas for the Database Computer](#)
- [Memory Requirements: Sample Deployment](#)

Hardware Requirements

Hardware requirements for Oracle Content DB are primarily determined by the factors described in [Table 2-1](#).

Table 2-1 Primary Factors Determining Oracle Content DB Hardware Requirements

Hardware Resource	Middle-tier computer requirement variables	Database computer requirement variables
CPU	<ul style="list-style-type: none"> ■ Peak number of operations performed each second 	<ul style="list-style-type: none"> ■ Peak number of operations performed each second ■ Whether using Oracle Text indexing
Memory	<ul style="list-style-type: none"> ■ Peak number of operations performed each second ■ Peak number of concurrent connected users ■ Average number of sessions used by each concurrent connected user ■ Number of files in each folder 	<ul style="list-style-type: none"> ■ Peak number of operations performed each second ■ Number of files

Table 2–1 (Cont.) Primary Factors Determining Oracle Content DB Hardware

Hardware Resource	Middle-tier computer requirement variables	Database computer requirement variables
Disk Size	Not applicable	<ul style="list-style-type: none"> ■ Number of files ■ Average content size of files, whether they can be indexed or not
Disk Throughput	Not applicable	<ul style="list-style-type: none"> ■ Peak number of files read and written each second ■ Average content size of files

In order to determine hardware requirements, assumptions must be made about the type of work that users are performing. The following measurements are averages extrapolated from a deployment within Oracle Corporation (40,000+ users), and are generally applicable for projecting Oracle Content DB usage.

Table 2–2 User Profiles

User Task	Number of Operations Each Connected User Performs Each Hour
Folder opens	8
Files read or written	10
Queries	0.1

These sizing guidelines are based on benchmarks of 10,000 concurrent connected users on Sun Microsystems hardware. The guidelines have been validated against measurements taken from an internal Oracle Corporation production usage by 55,000 Oracle employees, with 30 million files and 13TB of content. This system uses Intel Linux hardware for the middle-tier computers, and Sun hardware for the database.

Note: The sizing guidelines discussed in the following sections may be inaccurate if the desired user profile is significantly larger than the average measurements detailed in [Table 2–2](#).

Sizing Formulas for Each Middle-Tier Computer

This section provides formulas that you can use to determine specific hardware sizing for each middle-tier computer. [Table 2–3](#) summarizes the sizing formulas.

Table 2–3 Oracle Content DB Sizing Recommendations for Each Middle-Tier Computer

Component	Sizing Recommendations
Number of CPUs	$\text{roundup}(\text{peak concurrent connected users} / 250 + 33\% \text{ headroom})$
Required Usable Disk Space	At least 500MB for Oracle Content DB
Total Computer Memory, HTTP as the Primary Protocol	If HTTP is the primary protocol: $480\text{MB} + (3.6 \text{ MB} * \text{peak concurrent connected users})$

Table 2–3 (Cont.) Oracle Content DB Sizing Recommendations for Each Middle-Tier

Component	Sizing Recommendations
Total Computer Memory, Primary Protocol Other Than HTTP	If HTTP is not the primary protocol, or if the desired user profile is different than the average measurements described in Table 2–2: $480\text{MB} + (1\text{MB} * \text{peak concurrent connected users} * \text{average number of sessions in use by each concurrent connected user}) + (3\text{KB} * \text{number of objects desired in the java object cache}) + (8\text{MB} * \text{number of connections to the database})$

Number of CPUs

Use the following formula to determine the number of CPUs required:

$$\text{roundup}(\text{peak concurrent connected users} / 250 + 33\% \text{ headroom})$$

The *peak concurrent connected users* parameter is the number of users who are signed in to Oracle Content DB and have performed an operation during the peak hour of the day. If you do not know how many users that is likely to be, assume 10% of your entire Oracle Content DB named user population.

The *headroom* parameter represents the amount of CPU resources that should be left available. In order to ensure optimal efficiency, no more than 75% of the CPU should be allocated.

This formula is based on the following assumptions:

- The formula assumes Sun SPARC Solaris 400MHz UltraSPARC-II processors with 8MB secondary cache.
- Other RISC processors should perform roughly proportional to their MHz.
- Intel Pentium III (or later) processors on Windows and Linux computers should perform roughly proportional to half their MHz. For example, an 800MHz Pentium processor is approximately equivalent to a 400MHz RISC processor.

Required Usable Disk Space

Allocate at least 500MB for Oracle Content DB.

Total Computer Memory, HTTP as the Primary Protocol

If HTTP is the primary protocol, use the following formula to determine the total computer memory required:

$$480\text{MB} + (3.6\text{MB} * \text{peak concurrent connected users})$$

The 480MB is for the first Oracle Content DB middle-tier computer. The value of 3.6MB is calculated from the following assumptions:

- **1.6 sessions per concurrent connected user:** This assumes that the primary interface for Oracle Content DB is through the HTTP node. The additional 0.6 sessions are HTTP sessions which are started whenever a user of the Oracle Content DB Web client starts another Oracle Content DB Web client, or if the user accesses Web Folders or Oracle Drive.
- **0.1 connection pool connections per concurrent connected users:** This assumes the stated user profile.
- **400 objects in the Java data cache per concurrent connected user:** This assumes 50 files per folder and 8 folders opened per hour, assuming the stated user profile.

Total Computer Memory, Primary Protocol Other Than HTTP

If HTTP is not the primary protocol, or if the desired user profile is different than the average measurements described in [Table 2-2](#), use the following formula to determine the total computer memory required:

$$480\text{MB} + (1\text{MB} * \text{peak concurrent connected users} * \text{average number of sessions in use by each concurrent connected user}) + (3\text{KB} * \text{number of objects desired in the Java object cache}) + (8\text{MB} * \text{number of connections to the database})$$

The 480MB is for the first Oracle Content DB middle-tier computer. The other values are calculated from the following assumptions:

- The value of 1MB is high by design. Oracle Content DB has been optimized to reduce database CPU load by using middle-tier memory to cache items. This ensures a more scalable and less expensive system, because the database computer is less of a scalability bottleneck, and because memory on one- or two-processor middle-tier computers is typically less expensive than memory or CPU on high-end database computers (computers with large amounts of attached storage or with many processors).
- Oracle recommends limiting the number of peak concurrent user sessions through the `IFS.SERVICE.MaximumConcurrentSessions` parameter in the service configuration. Oracle has tested with Java heaps up to 2GB. With this constraint, this implies up to approximately 700 concurrent connected users per node and a total of 1986MB in size, if the following are true:
 - Each user uses 1.6 sessions
 - Each session is 1MB ($700 * 1.6 * 1\text{MB} = 1,120\text{MB}$)
 - Each user needs 400 Java data cache objects
 - Each object is 3KB in size ($700 * 400 * 3\text{KB} = 866\text{MB}$)

The HTTP/WebDAV memory overhead includes memory for 10 simultaneous guest user requests. Because of this, guest users should not be counted as connected users for HTTP/WebDAV access.

- For the average number of sessions in use by each concurrent connected user, use the value 1.6 for the HTTP node.
- Calculate the number of objects desired in the Java object cache by using the following formula:

$$(\text{number of folder opens in the peak hour}) * (\text{number of objects per folder}) * (\text{number peak concurrent connected users})$$

Use the result to set the value of the `IFS.SERVICE.DATACACHE.Size` parameter.

- The number of connections to the database depends on the number of simultaneous read or write operations being performed. Assume 0.1 database connections per user if using a standard user profile. This is a sum of the parameters `IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSize` and `IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSize` for each service.

See ["Service Configurations and Java Memory Sizing"](#) on page 12-1 for more information on middle-tier memory.

Sizing Formulas for the Database Computer

This section provides formulas that you can use to determine specific hardware sizing for each database computer to be used for Oracle Content DB users. [Table 2-4](#) summarizes the sizing formulas.

Table 2-4 Oracle Content DB Sizing Recommendations for the Database Computer

Component	Sizing Recommendations
Number of CPUs	$\text{roundup}(\text{peak concurrent connected users} / 250 + 33\% \text{ headroom})$
Required Usable Disk Space	$4.5\text{GB} + \text{total raw file size} + (\text{total raw file size} * 20\%)$
Total Computer Memory	$64\text{MB} + 128\text{MB} + \text{database buffer cache} + (1\text{MB} * \text{number of connections to the database}) + (500 \text{ bytes} * \text{number of files}) + (100\text{KB} * \text{peak concurrent connected users})$

Number of CPUs

Use the following formula to determine the number of CPUs required:

$$\text{roundup}(\text{peak concurrent connected users} / 250 + 33\% \text{ headroom})$$

The *peak concurrent connected users* parameter is the number of users who are signed in to Oracle Content DB and have performed an operation during the peak hour of the day. If you do not know how many users that is likely to be, assume 10% of your entire Oracle Content DB named user population.

The *headroom* parameter represents the amount of CPU resources that should be left available. In order to ensure optimal efficiency, no more than 75% of the CPU should be allocated. One additional CPU is used for the background Oracle Text indexing of new file content, if you are using Oracle Text indexing.

This formula is based on the following assumptions:

- The formula assumes Sun SPARC Solaris 400MHz UltraSPARC-II processors with 8MB secondary cache.
- Other RISC processors should perform roughly proportional to their MHz.
- Intel Pentium III (or later) processors on Windows and Linux computers should perform roughly proportional to half their MHz. For example, an 800MHz Pentium processor is approximately equivalent to a 400MHz RISC processor.

Required Usable Disk Space

Use the following formula to determine the usable disk space required:

$$4.5\text{GB} + \text{total raw file size} + (\text{total raw file size} * 20\%)$$

The 4.5GB represents the space required for Oracle software and the initial database configuration. If you are not using Oracle Text to index the content, multiply the total raw file size by 15% instead of 20%.

The following considerations can increase the amount of usable disk space required for the database computer:

- Mirroring for backup and reliability
- Redo log size, which should be determined by how many files are inserted and their size

- Unused portion of the last extent in each database, which occurs with pre-created database files or which can be large if the next extent setting is large

Total Computer Memory

Use the following formula to determine the total computer memory required:

$$64\text{MB} + 128\text{MB} + \text{database buffer cache} + (1\text{MB} * \text{number of connections to the database}) + (500 \text{ bytes} * \text{number of files}) + (100\text{KB} * \text{peak concurrent connected users})$$

This formula is based on the following assumptions:

- 128MB is the minimum amount of memory required to run a small Oracle Server.
- Number of files: The database buffer cache in the default Oracle database configuration is sufficient for approximately 50,000 files. For deployments with more than 50,000 files, allocate 500 bytes per file for optimal performance, including wildcard filename searches. Reduce this number if users do not perform wildcard filename searches.
- 100KB is calculated by assuming that 0.1 database connections are needed per concurrent connected user as in the stated user profile. Each database connection takes approximately 1MB of database memory.

Memory Requirements: Sample Deployment

Table 2–5 describes approximate minimum memory overhead on each middle-tier computer.

Table 2–5 Memory Overhead

Description	Approximate minimum memory (MB) for middle-tier computer
Memory used by the operating system upon booting the computer.	60
Overhead for first Java Virtual Computer (JVM).	30
Application Server Control. Must run on every middle tier.	150
Oracle HTTP Server, including the default HTTP daemons. Required for Oracle Content DB Web client, HTTP, Web Folders, and Oracle Drive access.	30
Oracle Content DB OC4J process. Required for Oracle Content DB Web client, HTTP, Web Folders, and Oracle Drive access. Must be paired with Oracle HTTP Server.	180
Total	450

Oracle Content DB Tablespaces

This section provides information about the Oracle Content DB tablespaces, and includes the following topics:

- [Data Types and Storage Requirements](#)
- [Storing Files in an Oracle Database](#)
- [Oracle Content DB Metadata and Infrastructure](#)
- [Oracle Text](#)

- [Disk Space Requirements: Sample Deployment](#)

Data Types and Storage Requirements

Table 2–6 shows the different types of data stored in Oracle Content DB and describes the purpose of each tablespace. Each of these tablespaces will be discussed in further detail in subsequent sections of this file.

Table 2–6 Tablespace Definitions

Tablespace Type	Tablespace Name	Description
File Storage	CONTENT_IFS_LOB_I	Stores the Large Object (LOB) data for files that are indexable by Oracle Text, such as text and word processing files.
File Storage	CONTENT_IFS_LOB_N	Stores the LOB data for files that are not indexed by Oracle Text, such as zip files.
File Storage	CONTENT_IFS_LOB_M	Stores the LOB data for files that are indexable by Oracle <i>interMedia</i> , such as image, audio, and video files.
Oracle Text	CONTENT_IFS_CTX_I	Stores words (tokens) extracted by Oracle Text from Oracle Content DB files (the Oracle table DR\$IFS_TEXT\$I).
Oracle Text	CONTENT_IFS_CTX_X	Stores the Oracle B*tree index on the Oracle Text tokens (the Oracle index DR\$IFS_TEXT\$X).
Oracle Text	CONTENT_IFS_CTX_K	Stores miscellaneous Oracle Text tables (the Oracle tables DR\$IFS_TEXT\$K, DR\$IFS_TEXT\$N, DR\$IFS_TEXT\$R).
Metadata	CONTENT_IFS_MAIN	Stores metadata for files, information about users and groups, and other Oracle Content DB object data.
Oracle Workflow	WORKFLOW_IFS_MAIN	Stores data for Oracle Workflow.
General Oracle Storage	Various	SYSTEM, ROLLBACK, TEMP, and other tablespaces that store the Oracle data dictionary, temporary data during transactions, and so on.

Typical tablespace storage space and disk I/O are detailed in [Table 2–7](#):

Table 2–7 Tablespace Storage Requirements and Disk I/O

Tablespace	% of Total I/O Throughput Requirements	% of Disk Space Requirements
CONTENT_IFS_MAIN	50%	2%
CONTENT_IFS_CTX_X	20%	1%
CONTENT_IFS_CTX_I	10%	1%
CONTENT_IFS_LOB_I	7%	34%
CONTENT_IFS_LOB_N	5%	55%
Various	5%	1%
CONTENT_IFS_LOB_M	1%	4%
CONTENT_IFS_CTX_K	1%	1%

Table 2-7 (Cont.) Tablespace Storage Requirements and Disk I/O

Tablespace	% of Total I/O Throughput Requirements	% of Disk Space Requirements
WORKFLOW_IFS_MAIN	1%	1%
Total	100%	100

Note the following issues regarding the information in [Table 2-7](#):

- I/O rates are highly dependent on the size of the `db_cache_size`. These measurements were taken on an Oracle-internal implementation, with 8GB `db_cache_size`, 17 million files, and 40,000 named users.
- The `CONTENT_IFS_MAIN` tablespace is the most important tablespace to spread across disks for maximum I/O capacity.
- Disk I/O for the `CONTENT_IFS_CTX_I`, `CONTENT_IFS_CTX_X` and `CONTENT_IFS_CTX_K` tablespaces is largely generated from Oracle Text batch processes (`ctx_ddl.sync_index`, and `ctx_ddl.optimize_index`), which are not critical to end-user performance. Therefore, these tablespaces can be on disks with lower I/O capacity, if necessary.

Storing Files in an Oracle Database

The largest consumption of disk space will occur on the disks that actually contain the files that reside within Oracle Content DB, namely the `CONTENT_IFS_LOB_I` tablespaces, `CONTENT_IFS_LOB_N` tablespaces, and `CONTENT_IFS_LOB_M` tablespaces. This section explains how the files are stored and how to calculate the amount of space those files will require.

As previously mentioned, files stored in Oracle Content DB are actually stored in database tablespaces. Oracle Content DB makes use of the Large Object (LOB) facility of the Oracle Database. All files are stored as Binary Large Objects (BLOBs), which is one type of LOB provided by the database. LOBs provide for transactional semantics much like the normal data stored in a database. In order to accomplish these semantics, LOBs must be broken down into smaller pieces which are individually modifiable and recoverable. These smaller pieces are referred to as chunks. Chunks are a group of one or more sequential database blocks from a tablespace that contains a LOB column.

Both database blocks and chunk information within those blocks (BlockOverhead) impose some amount of overhead for the stored data. BlockOverhead is presently 60 bytes per block, which consists of the block header, the LOB header, and the block checksum. Oracle Content DB configures its LOBs to have a 32K chunk size.

As an example, assume that the `DB_BLOCK_SIZE` parameter of the database is set to 8192(8K). A chunk would require four contiguous blocks and impose an overhead of 240 bytes. The usable space within a chunk would be $32768 - 240 = 32528$ bytes.

Each file stored in Oracle Content DB consists of an integral number of chunks. Using the previous example, for instance, a 500K file will actually use $512000 / 32528 = 15.74 = 16$ chunks. Sixteen chunks will take up $16 * 32K = 524288$ bytes. The chunking overhead for storing this file would then be $524288 - 512000 = 12288$ bytes which is 2.4 percent of the original file's size.

The chunk size used by Oracle Content DB is set to optimize access times for files. Note that small files, files less than one chunk, will incur a greater disk space percentage overhead since they must use at least a single chunk.

Another structure required for transactional semantics on LOBs is the LOB Index. Each LOB index entry can point to 8 chunks of a specific LOB object (`NumLobPerIndexEntry = 8`). In our continuing example, where a 500K file takes up 16 chunks, two index entries would be required for that object. Each entry takes 46 bytes (`LobIndexEntryOverhead`) and is then stored in an Oracle B*tree index, which in turn has its own overhead depending upon how fragmented that index becomes.

The last factor affecting LOB space utilization is the `PCTVERSION` parameter used when creating the LOB column. For information about how `PCTVERSION` works, please consult the *Oracle Database SQL Reference*.

Oracle Content DB uses the default `PCTVERSION` of 20 percent for the LOB columns it creates. This reduces the possibility of "ORA-22924 snapshot too old" errors occurring in read consistent views. So by default, a minimum of a 20 percent increase in chunking space must be added in to the expected disk usage to allow for persistent `PCTVERSION` chunks.

For large systems where disk space is an issue, Oracle recommends reducing `PCTVERSION` to 1, in order to reduce disk storage requirements. This may be done at any time in a running system using the following SQL commands:

```
alter table odmm_contentstore modify lob (globalindexedblob) (pctversion 1);
alter table odmm_contentstore modify lob (emailindexedblob) (pctversion 1);
alter table odmm_contentstore modify lob (emailindexedblob_t) (pctversion 1);
alter table odmm_contentstore modify lob (intermediablob) (pctversion 1);
alter table odmm_contentstore modify lob (intermediablob_t) (pctversion 1);
alter table odmm_nonindexedstore modify lob (nonindexedblob2) (pctversion 1);
```

The steps for calculating LOB tablespace usage are as follows:

1. Calculate the number of chunks a file will use by figuring the number of blocks per chunk, then subtracting the `BlockOverhead` (60 bytes) from the chunk size to get the available space per chunk.
2. Divide the file size by the available space per chunk to get the number of chunks, per the following formula:

$$\text{chunks} = \text{roundup}(\text{FileSize} / \text{ChunkSize} - ((\text{ChunkSize} / \text{BlockSize}) * \text{BlockOverhead}))$$

For example, if `FileSize = 100,000`, `ChunkSize = 32768`, `Blocksize = 8192`, and `BlockOverhead = 60`, then:

$$\text{roundup}(100000 / (32768 - ((32768 / 8192) * 60))) = 4 \text{ chunks}$$

3. Calculate the amount of disk space for a file by multiplying the number of chunks times the chunk size, multiplying that result by the `PCTVERSION` factor, and then adding the space for `NumLobPerIndexEntry` (8) and `LobIndexEntryOverhead` (46 bytes).

$$\text{FileDiskSpaceInBytes} = \text{roundup}(\text{chunks} * \text{ChunkSize} * \text{PCTVERSIONFactor}) + \text{roundup}(\text{chunks} / \text{NumLobPerIndexEntry} * \text{LobIndexEntryOverhead})$$

Hence, if `chunks = 4`, `ChunkSize = 32768`, `PCTVERSIONFactor = 1.1`, `NumLobPerIndexEntry = 8`, and `LobIndexEntryOverhead = 46`:

$$\text{roundup}(4 * 32768 * 1.1) + (\text{roundup}(4 / 8) * 46) = 144226 \text{ FileDiskSpaceInBytes}$$

4. Calculate the total disk space used for file storage by summing up the application of the preceding formulas for each file to be stored in the LOB, per the formula:

$$\text{TableSpaceUsage} = \text{sum}(\text{FileDiskSpaceInBytes})$$

for all files stored

Oracle Content DB creates multiple LOB columns. The space calculation must be made for each tablespace based upon the amount of content that will qualify for storage in that tablespace.

Oracle Content DB Metadata and Infrastructure

The Oracle Content DB server keeps persistent information about the file system and the contents of that file system in database tables. These tables and their associated structures are stored in the `CONTENT_IFS_MAIN` tablespace. This tablespace contains approximately 300 tables and 500 indexes. These structures are required to support both the file system and the various protocols and user interfaces that make use of that file system.

The administration and planning tasks of this space should be very similar to operations on a normal Oracle database installation. The administrator of the system should plan for approximately 6K of overhead per file to be used from this tablespace, or about 2% of the overall content. If there is a significant amount of custom metadata, such as categories, this overhead will be larger.

The initial disk space allocated for this tablespace is approximately 50MB for a default install. Of this 50MB, 16MB is actually used at the completion of installation. This includes instantiations for all required tables and indexes and the metadata required for the approximately 700 files that are loaded into Oracle Content DB as part of the install. Different tables and indexes within this tablespace will grow at different rates depending on which features of Oracle Content DB are used in a particular installation.

Oracle Text

When Oracle Content DB works in conjunction with Oracle Text, it allows users to access powerful search capabilities on the files stored within Oracle Content DB. Disk space for these capabilities is divided among three distinct tablespaces for optimal performance.

The `CONTENT_IFS_CTX_I` tablespace contains tables which hold the text tokens (separate words) that exist within the various indexed files. The storage for these text tokens is roughly proportional to the ASCII content of the file.

The ASCII content percentage varies depending on the format of the original file. Text files only have white space as their non-ASCII content and therefore incur a greater per file percentage overhead. File types such as Microsoft Word or PowerPoint contain large amounts of data required for formatting that does not qualify as text tokens. The per file percentage on these types of files is therefore lower. On a system with diverse content types the expected overhead is approximately 8% of the sum of the original sizes of the indexed files.

[Table 2–8](#) offers general guidelines for the amount of ASCII text in a file for several popular formats:

Table 2–8 Average ASCII Content Per File Type

Format	Plain ASCII Content as Percentage of File Size	Typical Percentage of all File Content ¹
Microsoft Excel ²	250%	4%
ASCII	100%	2%

Table 2–8 (Cont.) Average ASCII Content Per File Type

Format	Plain ASCII Content as Percentage of File Size	Typical Percentage of all File Content ¹
HTML	90%	10%
Rich Text Format	80%	2
Microsoft Word	70%	13%
Acrobat PDF	10%	18%
Microsoft PowerPoint	1%	3%
Images (JPEG, BMP), Compressed files (Zip, TAR), Binary files, and so on.	0%	50%
Total		100%

¹ From statistics of Oracle Corporation's internal usage of Oracle Content DB.

² By default, Oracle Text indexes each number in an Excel file as a separate word. Excel stores a number more efficiently than its ASCII equivalent, which is why the ASCII content as a percentage of the file size is greater than 100%.

The CONTENT_IFS_CTX_K tablespace contains the tables and indexes required to translate from the Oracle Content DB locator of a file (the Oracle Content DB DocID) to the Oracle Text locator of that same file (the Oracle Text DocID). The expected space utilization for this tablespace is approximately 70 bytes per indexed file.

The CONTENT_IFS_CTX_X tablespace contains the B*tree database index that is used against the text token information stored in the CONTENT_IFS_CTX_I tablespace. This will grow as a function of the ASCII content just as the CONTENT_IFS_CTX_I tablespace does. On a system with diverse content types the expected overhead is approximately 4% of the sum of the ASCII content of the files, or approximately 1% of the sum of the total sizes of the indexed files.

Disk Space Requirements: Sample Deployment

This section details various requirements for disk space, and offers guidance as to how necessary disk space will expand with the addition of files to the server.

Based on experience running Oracle Content DB for Oracle Corporation's internal usage, the disk overhead of Oracle Content DB for a large system (hundreds of gigabytes of file content) is approximately as detailed in [Table 2–9](#).

Table 2–9 Disk Space Requirements Summary

Tablespace Overhead Type	Overhead Versus Total Raw File Content ¹	Primarily Determined By
File Storage	12%	Size of files relative to chunk size (32KB by default)
Oracle Text	5%	Amount of ASCII content in all files
Metadata	2%	Number of folders, files, and so on.
General Oracle Storage	1%	Fixed, not configurable, database settings for TEMP, UNDO, and other tablespaces
Total	20%	Not applicable

¹ This does not include: mirroring for backup and reliability; Redo log size, which should be determined by how many files are inserted and their size; unused portion of the last extent in each database file (which will occur with pre-created database files or which may be large if the next extent setting is large).

See *Oracle Database Concepts* for explanations of the terms Large Object, tablespace, chunk size, and extents.

Given that a large percentage of the overhead is in LOB overhead, note that the overhead for your Oracle Content DB instance may vary depending on the average and median sizes of files.

Oracle Content DB Security

Oracle Content DB provides the basic infrastructure required by any shared, network-accessible system, including authentication and authorization. This section describes the architecture and configuration of security in Oracle Content DB.

This chapter provides information about the following topics:

- [SSL Configuration for Oracle Content DB](#)
- [About User Authentication in Oracle Content DB](#)
- [Setting Up a Server Keystore for WS-Security](#)
- [Changing the Private Server Key and Keystore Passwords](#)
- [Changing the Oracle Content DB Schema Password](#)
- [Security Considerations for HTTP/WebDAV](#)
- [Preventing Malicious Uploads](#)
- [Changing the Client Session Timeout Period](#)
- [Applying the Latest Critical Patch Updates to Oracle Content DB](#)

Note: Do not make any configuration changes to your Oracle Content DB deployment beyond those described in the documentation or required by the support team. Making undocumented changes to your system could have serious security implications.

SSL Configuration for Oracle Content DB

You can set up SSL for client connections to Oracle Content DB, including Web client, WebDAV, and Web services access. You can also set up SSL for the connection between Oracle Content DB and the user repository.

This section contains the following topics:

- [Setting Up SSL for Client Connections to Oracle Content DB](#)
- [Setting Up SSL Between Oracle Content DB and the User Repository](#)

Setting Up SSL for Client Connections to Oracle Content DB

You must configure Oracle HTTP Server to use SSL before configuring Oracle Content DB for SSL. Be sure to use a valid certificate when you configure Oracle HTTP Server for SSL. See *Oracle HTTP Server Administrator's Guide* for more information.

After configuring Oracle HTTP Server for SSL, follow these steps to configure Oracle Content DB for SSL:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Domain Properties table row, click the **Go to Task** icon.
4. Click **IFS.DOMAIN.APPLICATION.ApplicationPort**.
5. Update the value to the appropriate SSL port and click **OK**. This value may be the Oracle HTTP Server SSL port, a load balancer port, or some other port.
6. Click **IFS.DOMAIN.APPLICATION.ApplicationUseHttps**.
7. Set the value to **true** and click **OK**.
8. Return to the Cluster Topology page and restart the Oracle Content DB domain. See "[Starting and Stopping the Oracle Content DB Domain](#)" on page 7-1 for information about how to do this.

Setting Up SSL Between Oracle Content DB and the User Repository

If you are using an LDAP server as your Oracle Content DB user repository, you can use SSL for the connection between Oracle Content DB and the LDAP server. You cannot use SSL for the connection to a file-based user repository.

There are two supported authentication modes for an SSL connection between Oracle Content DB and the LDAP server: Server Only or Anonymous. You can only use Anonymous authentication mode if you are using Oracle Internet Directory.

This section contains the following topics:

- [Setting Up Server Only SSL Between Oracle Content DB and Your LDAP Server](#)
- [Setting Up Anonymous SSL Between Oracle Content DB and Your LDAP Server](#)

Setting Up Server Only SSL Between Oracle Content DB and Your LDAP Server

The following procedure explains how to set up Server Only SSL authentication between Oracle Content DB and your LDAP server. In Server Only authentication, also called SSL Server Authentication, the directory server authenticates itself to the client, then the directory server sends the client a certificate verifying that the server is authentic.

You must first configure your LDAP server for SSL before you perform the steps in the following procedure. If you are using Oracle Internet Directory, see *Oracle Internet Directory Administrator's Guide* for more information. If you are using a third-party LDAP server, refer to the documentation for your LDAP server for more information.

To set up Server Only SSL between Oracle Content DB and your LDAP server:

1. Ensure that the LDAP server certificate has been created on the LDAP host. Refer to the documentation for your LDAP server for more information.
2. On each Oracle Content DB middle tier, create a keystore for the LDAP server, as follows:
 - a. At the command prompt, go to `ORACLE_HOME/jdk/bin`.
 - b. Create an LDAP keystore by running the following keytool command:

```
./keytool -genkey -keystore keystore_file_name -keypass key_password
-storepass keystore_password
```

For example:

```
./keytool -genkey -keystore ORACLE_HOME/content/settings/ldap-keystore.jks
-keypass defaultkp -storepass ldapksp
```

The `-keypass` argument is required in order to create the keystore, but this key password is generic and is not used for anything.

- c. Repeat these steps for each Oracle Content DB middle tier.

Tip: If you want to avoid performing Step 2 and Step 3 on each middle tier, you can choose one of the following alternatives:

- Copy the keystore file onto each middle tier
- Create the keystore file in a common location, accessible by each middle tier

If you choose to copy the keystore file onto each middle tier, wait until after you have performed Step 3, importing the LDAP server certificate, to do so.

Even if you choose one of these options, other steps in this procedure must be performed on each middle tier. Choosing one of these options only enables you to avoid having to perform Step 2 and Step 3 on each middle tier.

3. On each Oracle Content DB middle tier, import the LDAP server certificate into the keystore, as follows:
 - a. At the command prompt, go to `ORACLE_HOME/jdk/bin`.
 - b. Import the LDAP server certificate into the keystore by running the following keytool command:

```
./keytool -import -file server_certificate -keystore keystore_file_name
-keypass key_password -storepass keystore_password
```

For example:

```
./keytool -import -file myldapserver.cer -keystore ORACLE_
HOME/content/settings/ldap-keystore.jks -keypass ldapkp -storepass ldapksp
```

- c. Repeat these steps for each Oracle Content DB middle tier, unless you chose one of the alternatives mentioned in Step 2.
4. On each Oracle Content DB middle tier, store the LDAP keystore password in a secure location so that Oracle Content DB can access the keystore. To do this, follow these steps:
 - a. At the command prompt, go to `ORACLE_HOME/content/bin`.
 - b. Run the following command:

```
./changepassword -l
```

Note: Do not use the option `-k`. The `-k` option is used to change the password for the WS-Security keystore, not the LDAP keystore.

- c. When prompted for the old password, just press Enter. Then, enter and confirm the LDAP keystore password that you provided in Step 2.
Be sure to follow the steps described in "[Changing the LDAP Keystore Password](#)" on page 3-10 if you need to change this password later.
- d. Repeat these steps for each Oracle Content DB middle tier.
5. On each Oracle Content DB middle tier, edit the `oc4j.properties` file, as follows:
 - a. Go to `ORACLE_HOME/j2ee/OC4J_Content/config` and open the `oc4j.properties` file for editing.
 - b. Add the following properties:


```
oracle.ifs.security.LdapSslEnabled=true
oracle.ifs.security.LdapSslAuthenticationMode=ServerOnly
```
 - c. The LDAP keystore location is also stored in the `oc4j.properties` file, in the property `oracle.ifs.security.LdapKeyStoreLocation`. Update the value of this property if needed.

Note: Do not update the value of `oracle.ifs.security.KeyStoreLocation`. This property stores the location of the keystore for WS-Security, not the LDAP keystore location.

- d. Save and close the `oc4j.properties` file.
- e. Repeat these steps for each Oracle Content DB middle tier.
6. If you are using a third-party LDAP server, you must edit the `system-jazn-data.xml` file on each Oracle Content DB middle tier. You do not need to perform this step if you are using Oracle Internet Directory as your user repository. To edit the `system-jazn-data.xml` file:
 - a. Go to `ORACLE_HOME/j2ee/OC4J_Content/config` and open the `system-jazn-data.xml` file for editing.
 - b. Go to the `oracle.security.jazn.login.module.LDAPLoginModule` for the **content** application, and change the `oracle.security.jaas.ldap.provider.url` option to the LDAP SSL URL, in the format:

```
ldaps://ldap_host:ldap_ssl_port
```

For example:

```
<application>
  <name>content</name>
  <login-modules>
    <login-module>
      <class>oracle.security.jazn.login.module.LDAPLoginModule</class>
      <control-flag>required</control-flag>
      <options>
        ...
        ...
        <option>
          <name>oracle.security.jaas.ldap.provider.url</name>
          <value>ldaps://myhost.mydomain.com:636</value>
        </option>
      </options>
    </login-module>
  </login-modules>
</application>
```



```

    </login-module>
  </login-modules>
</application>

```

- c. Save and close the `system-jazn-data.xml` file.
 - d. Repeat these steps for each Oracle Content DB middle tier.
7. Update Oracle Content DB domain properties with the new SSL port of your LDAP server. You only need to perform this step on one Oracle Content DB middle tier. To update Oracle Content DB domain properties:
- a. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
 - b. On the Content DB Home page, click the **Administration** tab.
 - c. In the Domain Properties table row, click the **Go to Task** icon.
 - d. Click **IFS.DOMAIN.CREDENTIALMANAGER.Idm**. You may need to move to the next page to find this property, or you can use the **Search** field.
 - e. Click **IFS.DOMAIN.CREDENTIALMANAGER.Idm.LdapSslEnabled**.
 - f. Set the value to **true** and click **OK**.
 - g. Click **IFS.DOMAIN.CREDENTIALMANAGER.Idm.LdapPort**.
 - h. Change the port number listed in the URL to be the SSL-enabled LDAP port, such as 636 or 4031, and click **OK**.
 - i. Click **OK** on the Edit Domain Property page.
8. On each Oracle Content DB middle tier, edit the `opmn.xml` file, as follows:
- a. Go to `ORACLE_HOME/opmn/conf` and open the `opmn.xml` file for editing.
 - b. In the **start-parameters** for `OC4J_Content`, add the java options **-Djavax.net.ssl.trustStore** and **-Djavax.net.ssl.trustStorePassword**.

For example:

```

<process-type id="OC4J_Content" module-id="OC4J" status="enabled">
  <module-data>
    <category id="start-parameters">
      <data id="java-options" value="-server -XX:MaxPermSize=128M -ms512M
-mx1024M -XX:AppendRatio=3 -Djava.security.policy=$ORACLE_HOME/j2ee/OC4J_
Content/config/java2.policy -Djava.awt.headless=true
-Dhttp.webdir.enable=false -Doc4j.userThreads=true
-Djavax.net.ssl.trustStore=your_keystore_location
-Djavax.net.ssl.trustStorePassword=your_keystore_password" />
    </category>
  </process-type>

```

- c. Save and close the `opmn.xml` file.
- d. Restart OPMN. Note that restarting OPMN will interrupt your OPMN-managed processes on this middle tier.
- e. Repeat these steps for each Oracle Content DB middle tier.

Setting Up Anonymous SSL Between Oracle Content DB and Your LDAP Server

The following procedure explains how to set up Anonymous SSL authentication between Oracle Content DB and your LDAP server. In Anonymous authentication,

also called No SSL Authentication, neither the client nor the server authenticates itself to the other. No certificates are sent or exchanged; only SSL encryption and decryption is used.

You can only use Anonymous SSL authentication if you are using Oracle Internet Directory as your user repository.

You must first configure Oracle Internet Directory for Anonymous SSL authentication (No SSL Authentication) before you perform the steps in the following procedure. See *Oracle Internet Directory Administrator's Guide* for more information.

To set up Anonymous SSL between Oracle Content DB and Oracle Internet Directory:

1. On each Oracle Content DB middle tier, edit the `oc4j.properties` file, as follows:
 - a. Go to `ORACLE_HOME/j2ee/OC4J_Content/config` and open the `oc4j.properties` file for editing.
 - b. Add the following properties:

```
oracle.ifs.security.LdapSslEnabled=true
oracle.ifs.security.LdapSslAuthenticationMode=ServerOnly
```
 - c. Save and close the `oc4j.properties` file.
 - d. Repeat these steps for each Oracle Content DB middle tier.
2. Update Oracle Content DB domain properties with the new Oracle Internet Directory SSL port. You only need to perform this step on one Oracle Content DB middle tier. To update Oracle Content DB domain properties:
 - a. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
 - b. On the Content DB Home page, click the **Administration** tab.
 - c. In the Domain Properties table row, click the **Go to Task** icon.
 - d. Click `IFS.DOMAIN.CREDENTIALMANAGER.Idm`. You may need to move to the next page to find this property, or you can use the **Search** field.
 - e. Click `IFS.DOMAIN.CREDENTIALMANAGER.Idm.LdapSslEnabled`.
 - f. Set the value to **true** and click **OK**.
 - g. Click `IFS.DOMAIN.CREDENTIALMANAGER.Idm.LdapPort`.
 - h. Change the port number listed in the URL to be the SSL-enabled Oracle Internet Directory port, such as 636 or 4031, and click **OK**.
 - i. Click **OK** on the Edit Domain Property page.
 - j. Return to the Cluster Topology page and restart the Oracle Content DB domain. See "[Starting and Stopping the Oracle Content DB Domain](#)" on page 7-1 for information about how to do this.

About User Authentication in Oracle Content DB

Authentication is a process in which a user provides some proof of identity (called a *credential*, which is often constructed from a user's password by means of a hashing or encryption algorithm) before that user can attempt to access objects in the system.

The user repository uses **JAZN** authentication to determine whether the user name and password are valid for the user. Because of JAZN limitations, to fully log out of Oracle Content DB, users must close all browser windows associated with the browser they used to log in to Oracle Content DB. For example, if users logged in using Microsoft Internet Explorer, they must close all Internet Explorer windows after they log out.

Note: Oracle Content DB does not support OC4J Java Single Sign-On (Java SSO), a single sign-on solution supplied with OC4J.

Authenticating as a Trusted Application Over Web Services

The Oracle Content DB JCR adapter, or any application using a Web Services client to connect to the Oracle Content DB server, can authenticate as a trusted application to the server. Under this model, the trusted client application does not need to provide a user credential. The server authenticates the trusted client application and assumes that the trusted client application has already verified the identity of the user.

You can use **WS-Security** to authenticate as a trusted application to Oracle Content DB. WS-Security is based on public key cryptography. A keystore must be configured for both the server and the client, and then the public keys of the client and server must be imported into the server and client keystores.

You can use commercially purchased secure certificates for these keys, or you can generate your own, as long as they are kept secure.

Setting Up a Server Keystore for WS-Security

To enable WS-Security trusted authentication for the Oracle Content DB server, you must first create a server keystore. You can use the `keytool` utility provided in `ORACLE_HOME/jdk/bin` to set up a server keystore and to import public keys.

See *Oracle WebCenter Framework Developer's Guide* for information about how to configure keystores for the client, and how to import server-side public keys into the client keystore.

About Oracle Content DB Access to the Server Keystore

When you create a server keystore for WS-Security, you also create a private server key. This private server key is protected by two passwords: one password for the server keystore, and one password for the private server key itself, called the private server key password.

After these passwords have been created, they must be stored in a secure location so that Oracle Content DB can access the private server key at run time. The Oracle Content DB `changepassword` utility is used to store these passwords in a secure location that can be accessed by Oracle Content DB.

Configuring a Server Keystore

To configure a keystore at the server side, follow these steps:

1. At the command prompt, go to `ORACLE_HOME/jdk/bin`.
2. Create the server keystore by running the following `keytool` command:

```
./keytool -genkey -keyalg RSA -validity number_of_days_certificate_is_valid
-alias server_public_key_alias -keystore keystore_file_name -dname
```

```
distinguished_name -keypass private_server_key_password -storepass keystore_password
```

For example:

```
./keytool -genkey -keyalg RSA -validity 5000 -alias server -keystore server-keystore.jks -dname "cn=server" -keypass serverprivkeypass -storepass serverksp
```

3. You can list the keys in the keystore by running the following keytool command:

```
./keytool -list -keystore keystore_file_name -keypass private_server_key_password -storepass keystore_password
```

For example:

```
./keytool -list -keystore server-keystore.jks -keypass serverprivkeypass -storepass serverksp
```

4. To use the key, sign it by running the following keytool command:

```
./keytool -selfcert -validity number_of_days_certificate_is_valid -alias server_public_key_alias -keystore keystore_file_name -keypass private_server_key_password -storepass keystore_password
```

For example:

```
./keytool -selfcert -validity 5000 -alias server -keystore server-keystore.jks -keypass serverprivkeypass -storepass serverksp
```

5. Export the server public key from the server keystore to a file by running the following keytool command:

```
./keytool -export -alias server_public_key_alias -keystore keystore_file_name -file server.pubkey -keypass private_server_key_password -storepass keystore_password
```

For example:

```
./keytool -export -alias server -keystore server-keystore.jks -file server.pubkey -keypass serverprivkeypass -storepass serverksp
```

6. Store the keystore password and the private server key password in a secure location so that Oracle Content DB can access the keystore and the private key. To do this, follow these steps:

- a. At the command prompt, go to `ORACLE_HOME/content/bin`.

- b. Run the following command:

```
./changepassword -k
```

- c. When prompted for the old password, just press Enter. Then, enter and confirm the keystore password that you provided in Step 2.

Be sure to follow the steps described in "[Changing the Keystore Password for WS-Security](#)" on page 3-10 if you need to change this password later.

- d. Run the following command:

```
./changepassword -p
```

- e. When prompted for the old password, just press Enter. Then, enter and confirm the private server key password that you provided in Step 2.

Be sure to follow the steps described in "[Changing the Private Server Key Password](#)" on page 3-9 if you need to change this password later.

Importing Client Public Keys Into the Server Keystore

To verify the signature of trusted clients, you must import the client public key into the server keystore.

To import a client public key into the server keystore, follow these steps:

1. At the command prompt, go to `ORACLE_HOME/jdk/bin`.
2. Run the following keytool command:

```
./keytool -import -alias client_private_key_alias -file client.pubkey -keystore
keystore_file_name -keypass private_server_key_password -storepass keystore_
password
```

For example:

```
./keytool -import -alias client -file client.pubkey -keystore
server-keystore.jks -keypass serverprivkeypass -storepass serverksp
```

Changing the Private Server Key and Keystore Passwords

If you created a server keystore for Oracle Content DB for WS-Security, you specified a password for both the private server key and for the keystore itself when you created the keystore. If you are using SSL for the connection between Oracle Content DB and the LDAP server, you also specified an LDAP keystore password when you created the LDAP keystore.

If you need to change any of these passwords, you must first change the passwords in the appropriate keystore by running a keytool command. Then, you must run the Oracle Content DB `changepassword` utility. This utility updates the passwords in the secure location where they are stored for use by Oracle Content DB.

This section contains the following topics:

- [Changing the Private Server Key Password](#)
- [Changing the Keystore Password for WS-Security](#)
- [Changing the LDAP Keystore Password](#)

Changing the Private Server Key Password

To change the private server key password:

1. First, change the private server key password in the keystore by running the appropriate keytool command.
2. On each Oracle Content DB middle tier, store the private server key password in a secure location so that Oracle Content DB can access it. To do this, follow these steps:
 - a. At the command prompt, go to `ORACLE_HOME/content/bin`.
 - b. Run the following command:


```
./changepassword -p
```
 - c. When prompted, enter the old password, new password, and confirm the new password.

- d. Repeat these steps for each Oracle Content DB middle tier.

Changing the Keystore Password for WS-Security

To change the WS-Security keystore password:

1. First, change the WS-Security keystore password in the keystore by running the appropriate keytool command.
2. On each Oracle Content DB middle tier, store the WS-Security keystore password in a secure location so that Oracle Content DB can access the keystore. To do this, follow these steps:
 - a. At the command prompt, go to `ORACLE_HOME/content/bin`.
 - b. Run the following command:

```
./changepassword -k
```
 - c. When prompted, enter the old password, new password, and confirm the new password.
 - d. Repeat these steps for each Oracle Content DB middle tier.

Changing the LDAP Keystore Password

To change the LDAP keystore password:

1. First, change the LDAP keystore password in the keystore by running the appropriate keytool command.
2. On each Oracle Content DB middle tier, store the LDAP keystore password in a secure location so that Oracle Content DB can access the keystore. To do this, follow these steps:
 - a. At the command prompt, go to `ORACLE_HOME/content/bin`.
 - b. Run the following command:

```
./changepassword -l
```
 - c. When prompted, enter the old password, new password, and confirm the new password.
 - d. Repeat these steps for each Oracle Content DB middle tier.

Changing the Oracle Content DB Schema Password

To change the Oracle Content DB schema password, first change the password in Oracle Database. Then, you need to run a script to change the password on each Oracle Content DB middle tier.

To change the Oracle Content DB schema password:

1. Stop the Oracle Content DB domain. See ["Starting and Stopping the Oracle Content DB Domain"](#) on page 7-1 for information about how to do this.
2. Change the Oracle Content DB schema password in Oracle Database, as follows:
 - a. Log in to SQL*Plus. For example, on UNIX systems:

```
cd $ORACLE_HOME/bin
./sqlplus /nolog
```

- b. Connect as the SYSDBA user. For example:


```
SQL>conn / as sysdba
```
- c. Change the password for the CONTENT schema, as follows:


```
SQL>alter user CONTENT identifiedby new_password;
```
3. Change the Oracle Content DB schema password on each middle tier, as follows:
 - a. At the command prompt, go to `ORACLE_HOME/content/bin`.
 - b. Run the following command:


```
./changepassword -s
```
 - c. When prompted, enter the old password, new password, and confirm the new password.
 - d. Repeat these steps for each Oracle Content DB middle tier.
4. Start the Oracle Content DB domain. See ["Starting and Stopping the Oracle Content DB Domain"](#) on page 7-1 for information about how to do this.

Security Considerations for HTTP/WebDAV

The HTTP and WebDAV protocol allows *digest* (hashed challenge/response) authentication. Whether HTTP and WebDAV use SSL depends on the configuration of Oracle HTTP Server, and on whether Oracle Content DB has been configured for SSL.

Note: You can only use digest authentication with Oracle Internet Directory or file-based user repositories. You cannot use digest authentication with third-party LDAP servers due to limitations in JAZN support.

Oracle Drive is a desktop client that uses the WebDAV protocol to access Oracle Content DB. After it is installed, Oracle Drive appears as a mapped drive in Windows Explorer. Oracle Drive also provides file synchronization capabilities between your local computer and Oracle Content DB.

Network Channel Encryption

The HTTP and WebDAV protocols do not encrypt the network channel by default. This means that files transferred using these protocols are susceptible to interception. If you are unwilling to accept this behavior, then you should disable these protocols or configure them to use SSL.

See ["SSL Configuration for Oracle Content DB"](#) on page 3-1 for more information.

Preventing Malicious Uploads

Because user quota is managed asynchronously through the Quota Agent, it is possible for a malicious user to upload a very large file for filling up disk space. To prevent such attacks, you can limit the size of any single file uploaded to Oracle Content DB by setting the `IFS.DOMAIN.MEDIA.CONTENTTRANSFER.ContentLimit` domain property. If you try to upload a file beyond the specified limit, then the upload fails. This limit does not apply to administrators.

When this property is set to 0, the default value, the content limit is disabled. You will be able to upload any file whose size is within the last calculated available quota, as of the beginning of the upload.

See "[Changing Domain Properties](#)" on page 8-1 for information about how to set the `IFS.DOMAIN.MEDIA.CONTENTTRANSFER.ContentLimit` property.

Changing the Client Session Timeout Period

The *client session timeout period* is the number of minutes of idle time after which a Web user interface session expires. By default, the client session timeout for Oracle Content DB is set to 30 minutes.

To change the client session timeout period:

1. Connect to the Application Server Control.
2. On the Cluster Topology page, in the Members table, click the **plus** icon next to one of the OC4J_Content instances. It does not matter which OC4J_Content instance you choose to expand.

You cannot expand the OC4J instance unless it is running. To start the OC4J instance, select it and click **Start**.
3. Under the OC4J_Content heading, click **content**.
4. On the Application: content page, in the Modules table, click **content**.
5. On the Web Module: content page, click the **Administration** tab.
6. In the Configuration Properties table row, click the **Go to Task** icon.
7. Change the value for **Session Timeout (seconds)**. The default is 1800 seconds (30 minutes).
8. Click **OK**.
9. Under the Confirmation heading, click **Restart** to restart the Oracle Content DB (content) application.

Applying the Latest Critical Patch Updates to Oracle Content DB

For greater security, apply any necessary Critical Patch Updates to your Oracle Content DB deployment. For more information on Critical Patch Updates and Security Alerts, go to the Oracle Technology Network (OTN) at:

<http://www.oracle.com/technology/deploy/security/alerts.htm>

Choosing Oracle Content DB Options

After you install and configure Oracle Content DB, you may want to customize your setup for a particular deployment scenario. For example, you may want to integrate Oracle Content DB with an antivirus solution, or run the Oracle Content DB application on a different port number.

This chapter provides information about the following topics:

- [Enabling Oracle Content DB Error Reporting and Site Quota Warning Notifications](#)
- [Setting Up Antivirus Integration](#)
- [Managing Storage Options](#)
- [Changing the Oracle Content DB Port Number](#)
- [Allowing Access to Oracle Content DB from Outside the Firewall](#)
- [Changing a Middle-Tier Host Name or IP Address](#)
- [Changing the Oracle Database URL](#)
- [Using Oracle Drive with Oracle Content DB](#)

Enabling Oracle Content DB Error Reporting and Site Quota Warning Notifications

You can choose to configure an SMTP server to use with Oracle Content DB. Choosing this option enables the following functionality:

- **Web client error reports.** If users encounter unexpected errors in the Oracle Content DB Web client, a dialog box appears, prompting the user to report information about the error. If the user chooses to send a report, the information is sent to the administrator e-mail address.
- **Site quota warning notifications.** When the quota consumed by the Site reaches 95 percent of the allocated quota, an e-mail notification is sent to the administrator e-mail address, and to any users of the Site with the Quota Administrator role.

Use the Application Server Control to set up an SMTP server for use with Oracle Content DB.

To enable Web client error reporting and Site quota warning notifications:

1. Set up an SMTP server, if you do not have one running already. This can be any SMTP server.

2. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
3. On the Content DB Home page, click the **Administration** tab.
4. In the Domain Properties table row, click the **Go to Task** icon.
5. On the Domain Properties page, click **IFS.DOMAIN.EMAIL.Administrator Address**. You may need to move to the next page to find this property, or you can use the **Search** field.
6. Enter the e-mail address of an administrator where you want error reports and Site quota warning notifications to be sent, then click **OK**.
7. Click **IFS.DOMAIN.EMAIL.Smtphost**.
8. Enter the host name for the SMTP server you want to use with Oracle Content DB, then click **OK**.
9. Click **IFS.DOMAIN.EMAIL.Smtphost**.
10. Enter the port number for the SMTP server you want to use with Oracle Content DB, then click **OK**.
11. Click **IFS.DOMAIN.EMAIL.Smtptimeoutlength**.
12. Enter the number of seconds you want Oracle Content DB to wait for the SMTP server to return from sending e-mail (for example, 60), then click **OK**.
13. Click **IFS.DOMAIN.EMAIL.Smtphost**.
14. Enter the name of a user for the SMTP server you want to use with Oracle Content DB, then click **OK**.
15. Return to the Cluster Topology page and restart the Oracle Content DB domain. See "[Starting and Stopping the Oracle Content DB Domain](#)" on page 7-1 for information about how to do this.

Setting Up Antivirus Integration

Oracle Content DB integrates with a partner solution, the Symantec AntiVirus Scan Engine (SAVSE), to provide options to verify that content is virus free and to clean files that are infected.

After antivirus integration has been set up, files will be scanned for viruses whenever they are opened for read access, using the latest available virus definitions. The following files will be excluded from the scanning process:

- Files that are quarantined
- File formats (such as .doc) that are excluded by the administrator
- Files that have already been scanned using the current virus definitions

If a file is infected with a virus, it will be marked as quarantined, and users will not be able to open the file until it is repaired. Contents of the file will remain unreadable even if virus checking is disabled by the administrator.

The Virus Repair Agent is responsible for repair attempts and retrieving the latest virus definitions. Whenever the agent becomes active, it polls the SAVSE server for updated virus definitions, and then attempts to repair the quarantined files. The agent will not attempt to repair the following files:

- Files that have exceeded the maximum number of repair attempts

- Files that have already experienced repair attempts using the current virus definitions

The following sections describe how to set up virus checking in Oracle Content DB:

- [Setting Up SAVSE](#)
- [Enabling Antivirus Functionality in Oracle Content DB](#)
- [Excluding Formats from Being Scanned](#)
- [Performance Implications of Scanning for Viruses](#)

Setting Up SAVSE

SAVSE must be installed and configured properly to function with Oracle Content DB. You must license the SAVSE server separately; the SAVSE license is not included with Oracle Content DB.

The following options must be set:

- You must select ICAP as the communication protocol. No other protocols are supported.
- You must set the scan policy to Scan and Repair or Scan Only. If you choose Scan Only, no repair attempts will be made. The Scan and Delete and Scan, Repair or Delete options are not supported.
- You must enable the ICAP 403 response. This parameter cannot be set using the SAVSE administration tool; instead, it must be manually set in the SAVSE configuration file.

Enabling Antivirus Functionality in Oracle Content DB

After the SAVSE server has been installed and configured, you can enable antivirus functionality in Oracle Content DB. You can also set the maximum number of repair attempts for quarantined documents, and configure how often the Virus Repair Agent is activated. Use the Application Server Control to perform these tasks.

Enabling Antivirus Functionality and Setting the Maximum Number of Repair Attempts

To enable antivirus functionality and set the maximum number of repair attempts:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Domain Properties table row, click the **Go to Task** icon.
4. On the Domain Properties page, click the **IFS.DOMAIN.ANTIVIRUS.Enabled** property, set the value to **true**, and click **OK**.
5. Click the **IFS.DOMAIN.ANTIVIRUS.Host** property, enter the host name or IP address of the computer where the SAVSE server is running, and click **OK**.
6. Click the **IFS.DOMAIN.ANTIVIRUS.MaxRepairAttempts** property, enter the number of times you want the Virus Repair Agent to attempt to repair a file, and click **OK**.
7. Click the **IFS.DOMAIN.ANTIVIRUS.Port** property, enter the value for the SAVSE listener port, and click **OK**.

8. Return to the Cluster Topology page and restart the Oracle Content DB domain. See "[Starting and Stopping the Oracle Content DB Domain](#)" on page 7-1 for information about how to do this.

Configuring the Virus Repair Agent

To configure how often the Virus Repair Agent becomes active:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Server Configurations table row, click the **Go to Task** icon.
4. Click **VirusRepairAgentConfiguration**. You may need to move to the next page to find this agent, or you can use the **Search** field.
5. In the Properties section, click **IFS.SERVER.TIMER.ActivationPeriod**.
6. Change the **Value** as necessary.
7. On the Edit Property page, click **OK**.
8. On the Edit Server Configuration page, click **OK**.
9. Return to the Cluster Topology page and restart the node (OC4J_Content instance) that runs this agent. See "[Starting, Stopping, and Restarting OC4J_Content Instances](#)" on page 7-3 for information about how to do this.

Excluding Formats from Being Scanned

You can exclude formats from being scanned for viruses to improve system performance. For example, you may choose to only scan formats with a higher probability of being infected, such as .zip files. Use the Application Server Control to exclude formats from virus checking.

To exclude formats from being scanned:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Formats table row, click the **Go to Task** icon.
4. Click the name of the format you want to exclude from virus scanning.
5. Select **Omitted From Antivirus Scan**.
6. Click **OK**.

Performance Implications of Scanning for Viruses

The performance of Oracle Content DB may be affected by enabling the virus checking option. The performance impact depends on the following factors:

- The frequency of virus definition updates made to the SAVSE service. Each time virus definitions are updated, *all* files that are opened (except for quarantined or excluded files) are scanned - none are excluded based on having already been scanned with these definitions, because the definitions are new.

After a virus definition update, overall system performance will degrade initially, but will gradually return to normal as more files are scanned with the current virus definitions and are therefore excluded from subsequent scans.

- The size and frequency of use of the Oracle Content DB repository.
- The type and size of the data in the repository.
- The probability of the number of attempted reads on unique files. Since files will only be scanned the first time they are opened against the current definitions, the frequency of unique files will affect performance.
- The performance of the SAVSE service. This is the most significant performance factor.
- The number of files whose format has been excluded from scanning by the administrator. Excluding certain formats will reduce the number of scans and improve system performance.

Managing Storage Options

The Oracle Content DB storage management options provide support for both offline and near-line storage. In offline and near-line storage, content that is infrequently accessed is moved from expensive online media, such as a disk array, to a cheaper offline medium, such as tape. The metadata and search indexes are kept online and are readily available.

Oracle Content DB uses BFILES to support offline and near-line storage. A BFILE is a read-only Oracle data type consisting of a directory object and a file name. Updating a document whose content is stored as a BFILE results in the content being reloaded from the external storage as a new binary large object (BLOB), where the modifications are made. The new content will be indexed, depending on its format. End users will be unaware of where their content is stored.

This section provides information about the following topics:

- [Data Aging and Archiving](#)
- [Specifying Storage Management Options](#)

Data Aging and Archiving

Oracle Content DB provides both data aging and data archiving through BFILES. Through data aging, content that has not been accessed for a specified interval can be automatically moved from a BLOB to a BFILE. Through data archiving, content in the [Archive](#) is automatically moved from a BLOB to a BFILE.

Content that has been moved to a BFILE is still accessible, and is visible as any content would be when users are browsing or searching.

BFILE aging and archiving are not enabled by default. Follow the instructions in the subsequent sections to set up BFILE aging and archiving:

- [Setting Up Data Aging](#)
- [Setting Up Data Archiving](#)

Setting Up Data Aging

Oracle Content DB is not set up for BFILE aging by default. To configure BFILE aging, you must first set domain properties that enable BFILE aging, then you must configure and activate the Content Agent. You can also specify storage management options.

To set domain properties that enable BFILE aging:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Domain Properties table row, click the **Go to Task** icon.
4. Click **IFS.DOMAIN.BFILE.Enabled**, set the value to **true**, and click **OK**.
5. Click **IFS.DOMAIN.BFILE.AgingEnabled**, set the value to **true**, and click **OK**.
6. Return to the Cluster Topology page and restart the Oracle Content DB domain. See "[Starting and Stopping the Oracle Content DB Domain](#)" on page 7-1 for information about how to do this.

To configure and activate the Content Agent:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Server Configurations table row, click the **Go to Task** icon.
4. Click **ContentAgentConfiguration**.
5. Edit the server configuration properties as necessary; see the Content Agent properties in [Appendix E, "Server Configuration Properties"](#) for more information about specific properties. In particular, you may want to edit **IFS.SERVER.AGENT.CONTENTAGENT.RetentionPeriod**; this property specifies the inactivity interval for files before they are moved to a BFILE.
6. Click **OK**.
7. Return to the **Administration** tab of the Content DB Home page.
8. In the Node Configurations table row, click the **Go to Task** icon.
9. Click the name of the node configuration that corresponds to the node where you want to run the Content Agent.
10. On the Edit Node Configuration page, in the Servers section, click **ContentAgent**.
11. Select **Initially Started** and click **OK**.
12. On the Edit Node Configuration page, click **OK**.
13. Return to the Cluster Topology page, select the node based on the node configuration you edited, and click **Restart**.

After you have set the domain properties for BFILE aging and configured the Content Agent, you can set storage management options as described in "[Specifying Storage Management Options](#)" on page 4-7.

Setting Up Data Archiving

Oracle Content DB is not set up for BFILE archiving by default. To configure BFILE archiving, you must set domain properties that enable BFILE archiving. You can also specify storage management options.

To set domain properties that enable BFILE archiving:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Domain Properties table row, click the **Go to Task** icon.
4. Click **IFS.DOMAIN.BFILE.Enabled**, set the value to **true**, and click **OK**.
5. Click **IFS.DOMAIN.BFILE.ArchivingEnabled**, set the value to **true**, and click **OK**.
6. Return to the Cluster Topology page and restart the Oracle Content DB domain. See "[Starting and Stopping the Oracle Content DB Domain](#)" on page 7-1 for information about how to do this.

After you have set the domain properties for BFILE archiving, you can set storage management options as described in "[Specifying Storage Management Options](#)" on page 4-7.

Specifying Storage Management Options

Optionally, you can change the default base path and policy for BFILE storage using the Application Server Control. These settings apply to all types of BFILE storage, including BFILE aging and BFILE archiving.

To specify storage management options:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Storage Management table row, click the **Go to Task** icon.

[Figure 4–1](#) shows the Storage Management page.

Figure 4–1 Storage Management Page

Storage Management

You can use BFILES to provide offline and near-line storage capabilities. A BFILE is a read-only Oracle data type consisting of a directory object and a filename. Specify the BFILE location and policy for BFILE storage.

Revert Apply

BFILE Location

Enter the base path where you want to store BFILE data (the operating system files). The directory or drive you specify must be both readable and writable by the database processes.

* BFILE Base Path

On UNIX, specify an absolute path starting with '/' or use './' to specify a path relative to the database's Oracle home. On Windows, specify a path in the format '%server\share'.

BFILE Policy

The BFILE Policy determines whether the BFILE data (the operating system files) should be deleted when BFILE references are deleted from the database.

Delete BFILE References? Yes, delete the operating system files
 No, retain the operating system files

Revert Apply

4. Change the **BFILE Base Path**. The default base path is:

`ORACLE_HOME/ifsbfiles/content_services_schema`

`ORACLE_HOME` refers to the database Oracle home on the database computer.

Each BFILE has a relative path in addition to the base path. The relative path is:

`/yyyy/dd/mm/hh/mm/ss/ifsbfile_id`

In the relative path, `ifsbfile_id` is the file naming pattern that associates a unique ID to each piece of content.

5. Change the **BFILE Policy**. This policy determines whether the operating system files should be deleted when the BFILE references are deleted from the database. If you are storing BFILES on an optical device that does not permit deletion, you should specify that the operating system files should be retained.
6. Click **Apply**.

Changing the Oracle Content DB Port Number

If you want to change the Oracle Content DB application port to a different port number, perform the tasks listed in the following sections:

- [Changing the Port Number in Oracle HTTP Server](#)
- [Changing the Port Number in Oracle Content DB](#)

Changing the Port Number in Oracle HTTP Server

Before you can change the port number in Oracle Content DB, you must first change the port number in Oracle HTTP Server by modifying the Oracle HTTP Server HTTP Listen Directive in the `httpd.conf` file, and then restarting the Oracle Application Server middle tier. See "Managing Ports" in *Oracle Application Server Administrator's Guide* for full instructions.

Changing the Port Number in Oracle Content DB

Use the Application Server Control to update the Oracle Content DB Application Port domain property and restart the OC4J_Content instance:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Domain Properties table row, click the **Go to Task** icon.
4. On the Domain Properties page, click **IFS.DOMAIN.APPLICATION.ApplicationPort**.
5. Enter the new port number in the **Value** field and click **OK**. If you are using a load balancer with multiple Oracle Content DB middle tiers, enter the load balancer port.
6. Return to the Cluster Topology page, select the appropriate **OC4J_Content** instance, and click **Restart**.

Allowing Access to Oracle Content DB from Outside the Firewall

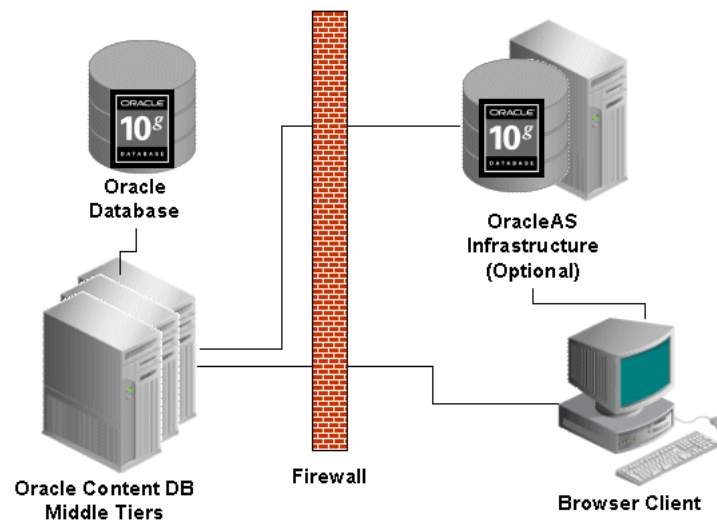
You can set up Oracle Content DB so that users outside the firewall can have access. To do this, follow these steps:

1. **Open ports**. Disable the firewall for the following ports:
 - Database listener port (typically 1521)

- Apache port (Oracle HTTP Server port)
 - Oracle Internet Directory ports (if you are using Oracle Internet Directory, and if Oracle Internet Directory is running inside the firewall)
 - Load balancer port (if you use a load balancer)
2. **Set firewall timeout periods.** You must set the operating system parameter `TCP_keeplive` to 120 minutes.

Figure 4–2 shows a possible firewall scenario with the database and middle tiers inside the firewall, and with OracleAS Infrastructure outside the firewall.

Figure 4–2 Sample Firewall Configuration



Changing a Middle-Tier Host Name or IP Address

You can run a script to change the host name or IP address of a middle-tier host in Oracle Content DB. You can only run the script if you have a multiple-computer deployment of Oracle Content DB. In other words, you can only run the script if your middle tier does not run on the same host as Oracle Database (or Oracle Internet Directory, if you are using Oracle Internet Directory as your user repository).

To change the host name or IP address of your middle tier:

1. Shut down all middle-tier processes, including `OC4J_Content` and the Application Server Control.

See Also:

- ["Starting, Stopping, and Restarting OC4J_Content Instances"](#) on page 7-3 for information about stopping `OC4J_Content`
 - *Oracle Application Server Administrator's Guide* for information about stopping the Application Server Control
2. Change the host name or IP address on your middle-tier computer.
 3. Change the host name or IP address for all of your other Oracle Application Server components. To do this, run the `chgiphost` utility, located in `ORACLE_HOME/CHGIP/scripts`, and follow the prompts. For more information, see

"Changing Network Configurations" in *Oracle Application Server Administrator's Guide*.

4. Run the Oracle Content DB script `changehostname`, located in the following directory:

```
ORACLE_HOME/content/bin
```

Specify the old host name or IP address and the new host name or IP address as arguments. For example:

```
changehostname old_host_name new_host_name
```

or

```
changehostname old_ip_address new_ip_address
```

If you need to change both the host name and the IP address, you must run the script twice, once to change the host name and once to change the IP address.

Note: You can view log information for this script in `changehostname.log`, located in:

```
ORACLE_HOME/content/logs
```

5. Start all middle-tier processes, including OC4J_Content and the Application Server Control.

See Also:

- ["Starting, Stopping, and Restarting OC4J_Content Instances"](#) on page 7-3 for information about starting OC4J_Content
- *Oracle Application Server Administrator's Guide* for information about starting the Application Server Control

Changing the Oracle Database URL

If you change the host name for your Oracle Database, you need to update the database URL stored on each Oracle Content DB middle tier. To do this, on each middle tier, update the `oc4j.properties` file for the OC4J_Content instance. You can find this file at:

```
ORACLE_HOME/j2ee/OC4J_Content/config
```

You also need to update the database URL if you change from a regular Oracle Database configuration to an Oracle RAC configuration.

Using Oracle Drive with Oracle Content DB

Oracle Drive is a native Windows application that lets users use Windows Explorer, Microsoft Office, and other Windows applications to access content in Oracle Content DB and other Oracle WebDAV servers such as OracleAS Portal. Oracle Drive displays files and folders in Oracle Content DB as a mapped drive in Windows Explorer. Oracle Drive also provides an effective offline solution that lets users edit files on their computers when offline, and then synchronize with the server when they reconnect.

Oracle Drive is available on the Downloads page of the Oracle Technology Network (OTN) at:

<http://www.oracle.com/technology/software/>

Oracle Drive runs on Microsoft Windows 2000 and Windows XP. For the most up-to-date certification information, see *OracleMetaLink* at <http://metalink.oracle.com>.

Oracle Drive requires Microsoft .NET Framework 1.1. The Oracle Drive installation installs the Microsoft .NET Framework 1.1 on the client computer.

You can set up an administrator-configured installation of Oracle Drive so that Oracle Drive is automatically deployed on user workstations, or you can copy the Oracle Drive executable to an accessible location so that users can install Oracle Drive themselves. You can also include service details with the Oracle Drive executable so that users don't have to configure their Oracle Drive service. The following sections provide more information about these topics:

- [Setting Up an Administrator-Configured Installation of Oracle Drive](#)
- [Packaging Service Information with the Oracle Drive Executable](#)
- [Installing Oracle Drive](#)

Setting Up an Administrator-Configured Installation of Oracle Drive

Setting up an automatic installation of Oracle Drive for your users is strongly encouraged. Oracle Drive is the client of choice for uploading and downloading many files at once, and also provides synchronization capabilities. Setting up an administrator-configured install will encourage user adoption and reduce support calls.

Configuring Oracle Drive Service Details For Your Users

You can choose to specify Oracle Drive service details as part of your Oracle Drive deployment. Setting up an Oracle Drive service for your users is strongly recommended so that users do not have to configure Oracle Drive themselves. Note that individual users can still edit service details as necessary for their own computers.

To specify Oracle Drive service details, update the parameters in the `config.xml` file. Then, specify the location of the `config.xml` file in the `update.xml` file. Both of these files need to be copied to an HTTP server that is accessible to all your users, without requiring a login.

Finally, specify the location of the `update.xml` file in `odrive.ini`, then copy it to the same location as the `ODriveSetup.msi` file. See "[Preparing for Deployment Using Active Directory](#)" on page 4-15 for more information about `ODriveSetup.msi`.

These steps are detailed in the following sections:

- [Setting Up config.xml](#)
- [Setting Up update.xml](#)
- [Setting Up odrive.ini](#)

Setting Up config.xml The `config.xml` file contains the details for the Oracle Drive service you want to deploy. Update `config.xml` by providing your own values for each parameter. Then, copy the file to an HTTP server that is accessible to all your users, without requiring a login. After you download the Oracle Drive installation files, you can find `config.xml` in the `\Extra` folder.

You can configure multiple services for your users by providing additional `<item>` entries, with parameters, in `config.xml`. Refer to [Table 4-1](#) for information about the parameters in `config.xml`.

[Example 4-1](#) shows the format of the `config.xml` file, with sample values for two services.

Example 4-1 config.xml

```
<wfc-config>

<item>
  <type>odrive-support</type>
  <techsupportemail>odriveissues@oracle.com</techsupportemail>
</item>

<item>
  <type>service</type>
  <name>Oracle Content DB</name>
  <hostname>myhost1.company.com</hostname>
  <port>7777</port>
  <secure>1</secure>
  <server-directory>/users/mydir</server-directory>
  <drive-letter>k</drive-letter>
  <sharing-level>3</sharing-level>
  <map-home>1</map-home>
  <auto-reconnect>2</auto-reconnect>
  <basic-authentication>0</basic-authentication>
  <bypass-proxy>1</bypass-proxy>
</item>

<item>
  <type>service</type>
  <name>Oracle Portal</name>
  <hostname>myhost2.company.com</hostname>
  <port>7778</port>
  <secure>1</secure>
  <server-directory>/my_location</server-directory>
  <drive-letter>z</drive-letter>
  <sharing-level>3</sharing-level>
  <map-home>1</map-home>
  <auto-reconnect>2</auto-reconnect>
  <basic-authentication>0</basic-authentication>
  <bypass-proxy>1</bypass-proxy>
</item>

</wfc-config>
```

Table 4-1 Parameter Values for config.xml

Parameter Name	Description
<code><type></code>	The value for this parameter must be "service" or "odrive-support." Do not change this value.
<code><techsupportemail></code>	The e-mail address that will be used by Oracle Drive when users click Report a Problem . By default, this parameter is set to <code>odriveissues@oracle.com</code> . Although this address is an actual address, e-mails sent to this address will not receive responses; instead, users will receive an auto-reply message. You can keep the default value for this parameter, or provide an alternate e-mail address.

Table 4–1 (Cont.) Parameter Values for config.xml

Parameter Name	Description
<name>	The name of the service (for example, Oracle Content DB) as it will appear in Oracle Drive.
<hostname>	The host name of the Oracle Content DB server (for example, myhost.mycompany.com).
<port>	The port number of the Oracle Content DB server (for example, 7778). If you do not specify this value, the port number defaults to either 80 or 443, depending on the value you specify for <secure>.
<secure>	Whether HTTP or HTTPS will be used to connect to Oracle Content DB. The possible values are: <ul style="list-style-type: none"> ■ 0 (use HTTP) ■ 1 (use HTTPS)
<server-directory>	The Oracle Content DB folder location to mount, or in other words, the folder location that will appear as the top-level folder when users connect to Oracle Content DB using Oracle Drive (for example, /content/dav/my_site/Libraries/mydir). You must include /content/dav at the beginning of the specified path.
<drive-letter>	The Windows drive letter to use for this service. The value can be any drive letter from D-Z. If you do not specify a value, or if the letter you specify is not available, the first drive letter available will be used.
<sharing-level>	The default value for the refresh interval to use for this service. The longer the refresh interval, the better the performance. However, when the refresh interval is longer, files and directories are refreshed less frequently, so users may notice a lag in seeing file and directory changes made by other users. In addition, the longer the refresh interval, the fewer server resources are needed (such as CPU or disk I/O). The possible values are: <ul style="list-style-type: none"> ■ 0 (1 hour) ■ 1 (15 minutes) ■ 2 (3 minutes) ■ 3 (15 seconds)
<map-home>	Whether to map to the Personal Library of the user by default (if the Personal Library exists). The possible values are: <ul style="list-style-type: none"> ■ 1 (map to the Personal Library of the user) ■ 2 (do not map to the Personal Library of the user) The Personal Library can only be mounted if the value for <server-directory> begins with /content/dav.
<auto-reconnect>	Whether or not to automatically connect to the service when Oracle Drive starts. The possible values are: <ul style="list-style-type: none"> ■ 1 (automatically connect to the service) ■ 2 (do not automatically connect to the service)

Table 4–1 (Cont.) Parameter Values for config.xml

Parameter Name	Description
<basic-authentication>	<p>Whether users can use basic authentication to connect to WebDAV servers that require cleartext passwords. The possible values are:</p> <ul style="list-style-type: none"> ■ 0 (do not use basic authentication) ■ 1 (use basic authentication) <p>Because Oracle Content DB does not require cleartext passwords, enter 0 for this parameter.</p>
<bypass-proxy>	<p>Whether Oracle Drive uses a proxy server when communicating with the WebDAV server. The possible values are:</p> <ul style="list-style-type: none"> ■ 0 (do not bypass the proxy server) ■ 1 (bypass the proxy server)

Setting Up update.xml The `update.xml` file holds the value for the location of the `config.xml` file. After you download the Oracle Drive installation files, you can find `update.xml` in the Extra folder.

Edit the `update.xml` file by providing your own values for each parameter:

- `<date>`: Provide a string value (such as a date, in any format, or other representation) that corresponds to the configuration file version you are using. If Oracle Drive detects that the string value has changed since the last time it started, Oracle Drive will process the new `config.xml` file.
- `<location>`: Provide the URL to `config.xml`.

Then, copy the file to an HTTP server that is accessible to all your users, without requiring a login.

[Example 4–2](#) shows the format of the `update.xml` file, with sample values.

Example 4–2 update.xml

```
<?xml version="1.0" ?>
<config-update>
  <date>2006.07.31 13:41:PST</date>
  <location>http://myserver.mycompany.com/config.xml</location>
</config-update>
```

Setting Up odrive.ini The `odrive.ini` file holds the value for the location of the `update.xml` file. After you download the Oracle Drive installation files, you can find `odrive.ini` in the Extra folder.

Update `odrive.ini` by providing the URL for your `update.xml` file, then copy `odrive.ini` to the same directory where the `ODriveSetup.msi` file is located. See the "[Preparing for Deployment Using Active Directory](#)" on page 4-15 for more information about `ODriveSetup.msi`.

[Example 4–3](#) shows the format of the `odrive.ini` file, with sample values.

Example 4–3 odrive.ini

```
[General]
AutoupdateURL=http://myserver.mycompany.com/odrive/update.xml
```

Preparing for Deployment Using Active Directory

You must use a Windows Domain Controller computer to deploy Oracle Drive using Active Directory. If you need to promote a Windows 2000 or 2003 server to be a Domain Controller, you can use the Microsoft utility `DCPromo.exe`.

You must also install Active Directory on the Domain Controller computer, if it is not installed already.

Finally, you must extract the `ODriveSetup.msi` file, along with other files required for installation, from the Oracle Drive installation executable. To do this:

1. Exit Oracle Drive, if it is running. To do this, right-click the Oracle Drive icon in the system tray and choose **Exit**.
2. Open a command prompt window and navigate to the directory where the self-extracting EXE is located (for example, `OracleDrive10.2.exe`).
3. In the command prompt window, run the self-extracting EXE with the `/T` option, specifying a temporary location. For example:

```
OracleDrive10.2.exe /T:c:\temp
```

This action will extract nine files from the self-extracting EXE, including the installation executable.

4. In the command prompt window, navigate to the temporary location (for example, `c:\temp`).
5. In the command prompt window, run the Oracle Drive installation executable in administrative mode, as follows:

```
executable_name /a
```

For example:

```
ODriveSetup10.2.0.0.0.exe /a
```

6. Follow the wizard instructions. On the Network Location screen, specify the location on your local (not network) drive where you want to put the MSI and other files.
7. Click **Finish** to exit the wizard.
8. Copy the files to a public share accessible to all the users of that domain. If you are specifying Oracle Drive service details for your users, make sure to copy `odrive.ini` to the same location.

Deploying Oracle Drive Using Active Directory

You can use Active Directory to automatically deploy Oracle Drive (using MSI) on user workstations. With this technique, you can deploy Oracle Drive on all computers for your users from a single server.

Microsoft Windows 2000 or later operating systems include tools that allow administrators to install and maintain software applications based on Group Policy. An administrator can assign Oracle Drive to a particular computer by creating a computer-level software distribution Group Policy. Assigning Oracle Drive to user computers is the simplest way to use Group Policy to manage a package. With this method, Oracle Drive is automatically installed on the computer the first time a designated computer is started and the software installation portion of the Group Policy is applied.

This feature allows administrators to set up the environment required for the whole group, including specifying Oracle Drive service details.

To set up an automatic installation of Oracle Drive using Active Directory and MSI:

1. From the Windows **Start** menu, choose **Active Directory for Users and Computers**. The Active Directory application appears.
2. In the tree view, under the domain name, create a new organization unit (for example, OdriveOU).
3. By default, all the computers in the domain appear in the Computers organization unit. Move the computers on which you want to deploy Oracle Drive to the new organization unit you created in Step 2.

Oracle recommends you deploy Oracle Drive to a small subset of computers first, for testing purposes, before deploying to your entire organization.
4. Right-click the organization unit you created and select **Properties**.
5. Click the **Group Policy** tab and create a new group policy object link.
6. Double-click the group policy object link you created in Step 5. The Group Policy Object Editor appears.
7. In the tree view, go to **Computer Configuration > Software Settings > Software Installation**. Ensure that **Software Installation** is selected, then right-click in the right pane and choose **New > Package**.
8. Specify the extracted MSI file for the new package, then, in the Deploy Software dialog box, select **Advanced** for the deployment method.
9. After you have created the new package, right-click the package and select **Properties**. Click the **Deployment** tab and ensure that the **Deployment type** is set to **Assigned**, then click **OK**.

Any errors that occur during the deployment of Oracle Drive will appear in the Event Log for the Windows Domain Controller computer. The Event Log can be viewed locally, or remotely.

Most files installed with Oracle Drive are put in the Oracle Drive installation directory. In addition, Oracle Drive installs additional files in the `System32` directory for use by Windows. [Table 4–2](#) lists these additional files.

Table 4–2 Files Installed by Oracle Drive Into the System32 Directory

File Name	File Location
tdfsd.sys	<code>Windows_folder\System32\Drivers</code>
TDSHELL.dll	<code>Windows_folder\System32</code>
TDHook.dll	<code>Windows_folder\System32</code>
XDNP.dll	<code>Windows_folder\System32</code>
ODriveHelper.dll	<code>Windows_folder\System32</code>

Redeploying Oracle Drive

You can upgrade the version of Oracle Drive on user workstations by redeploying Oracle Drive using Active Directory.

To redeploy Oracle Drive:

1. On the Windows Domain Controller computer, from the **Start** menu, choose **Active Directory for Users and Computers**. The Active Directory application appears.
2. In the tree view, right-click the organization unit you created for the Oracle Drive deployment and select **Properties**.
3. Click the **Group Policy** tab, then double-click the group policy object link. The Group Policy Object Editor appears.
4. In the tree view, go to **Computer Configuration > Software Settings > Software Installation**. Right-click the package in the right pane and choose **All Tasks > Redeploy application**.

Removing Oracle Drive from User Workstations

You can undeploy Oracle Drive from user workstations using Active Directory.

To undeploy Oracle Drive:

1. On the Windows Domain Controller computer, from the **Start** menu, choose **Active Directory for Users and Computers**. The Active Directory application appears.
2. In the tree view, right-click the organization unit you created for the Oracle Drive deployment and select **Properties**.
3. Click the **Group Policy** tab, then double-click the group policy object link. The Group Policy Object Editor appears.
4. In the tree view, go to **Computer Configuration > Software Settings > Software Installation**. Right-click the package in the right pane and choose **All Tasks > Remove**.

Packaging Service Information with the Oracle Drive Executable

As an alternative to automatically installing Oracle Drive on user workstations, you can provide service information as part of the Oracle Drive executable. Using this method, users install Oracle Drive themselves, but do not have to configure service details after installation completes.

To include service information with the Oracle Drive executable:

1. Download the Oracle Drive installation files to a location on your local hard drive (for example, `C:\odrive`).
2. In the `Extra` folder, open the file `config.xml` in a text editor. Provide service details, then copy the file to an accessible location. See "[Setting Up config.xml](#)" on page 4-11 for more information.
3. In the `Extra` folder, open the file `update.xml` in a text editor. Provide the location of `config.xml`, then copy the file to an accessible location. See "[Setting Up update.xml](#)" on page 4-14 for more information.
4. In the `Extra` folder, open the file `odrive.ini` in a text editor and provide the location of `update.xml`. See "[Setting Up odrive.ini](#)" on page 4-14 for more information.
5. In the `Extra` folder, open the file `OracleDrive10.2.SED` in a text editor. Edit the `TargetName`, `SourceFiles0`, and `SourceFiles1` properties, as necessary:
 - For `TargetName`, provide the location where you want to put the Oracle Drive executable.

- For `SourceFiles0`, provide the location on your hard drive where you copied the `Binaries` folder.
- For `SourceFiles1`, provide the location on your hard drive where you copied the `Extra` folder.

If you copied the Oracle Drive files to `C:\odrive`, you can keep the defaults and skip this step.

The following example shows a portion of the `OracleDrive10.2.SED` file:

```

TargetName=C:\odrive\OracleDrive10.2.exe
FriendlyName=Oracle Drive 10.2.0.0.0
AppLaunched=ODUpgrade.exe
PostInstallCmd=<None>
AdminQuietInstCmd=
UserQuietInstCmd=
FILE0="ODriveSetup10.2.0.0.0.exe"
FILE1="ODUpgrade.exe"
FILE2="dotnetfx.exe"
FILE3="odrive.ini"
[SourceFiles]
SourceFiles0=C:\odrive\binaries\
SourceFiles1=C:\odrive\extra\
[SourceFiles0]
%FILE0%=
%FILE1%=
%FILE2%=
[SourceFiles1]
%FILE3%=

```

6. Use the IExpress utility to re-package the files into a self-extracting executable. To do this, open a command prompt and go to the location where the SED file is located, then run this command:

```
iexpress /N OracleDrive10.2.SED
```

7. Copy the Oracle Drive executable to a location where users can download it. You can find the executable at the location you specified for `TargetName` in the SED file.

Installing Oracle Drive

If you choose not to set up the administrator-configured installation of Oracle Drive, you can download the installation files from the Oracle Technology Network (OTN), then copy the files to a location where your users can download them. Alternatively, your users can download Oracle Drive from OTN themselves.

To install Oracle Drive, there must available disk space equivalent to twice the size of the install files

The following instructions explain how to install Oracle Drive.

Note: If you install Oracle Drive on a computer that has firewall software running, such as the native Windows XP firewall, you may see a message similar to the following:

Windows Security Alert: To help protect your computer, Windows Firewall has blocked some features of this program. Do you want to keep blocking this program? ODFWAgent.exe

If you see this message, select **Unblock** to allow Oracle Drive to run.

To install Oracle Drive:

1. Double-click the Oracle Drive executable.
2. If you are accessing the installation files from a remote location, in the File Download window, select **Run this program from its current location**, then click **Yes** in the warning dialog box.

You can also download the installation program to your local hard drive and run it from there. After downloading, double-click the executable file to begin installation.
3. If you have a previous version of Oracle Drive installed, the installation wizard prompts you to uninstall the previous version first. You must close any browser windows you have open before proceeding.
4. Oracle Drive requires Microsoft .NET Framework 1.1. If you do not have Microsoft .NET Framework 1.1, the installation wizard will install it for you.
5. On the Choose Setup Language screen, select a language and click **OK**.
6. On the Welcome screen, click **Next**.
7. On the Destination Folder screen, accept the default installation directory, or click **Change** to select a different installation directory. Then, click **Next**.
8. On the Miscellaneous Options screen, choose whether to add a shortcut to Oracle Drive on your desktop, and whether you want Oracle Drive to start automatically when Windows starts. Then, click **Next**.
9. On the Ready to Install the Program screen, click **Install** to install Oracle Drive, or click **Back** to change any values that you entered.
10. On the InstallShield Wizard Completed screen, click **Finish**.
11. The Oracle Drive installer prompts you to restart your computer. Select **Yes** to restart your computer automatically, or select **No** and restart manually.

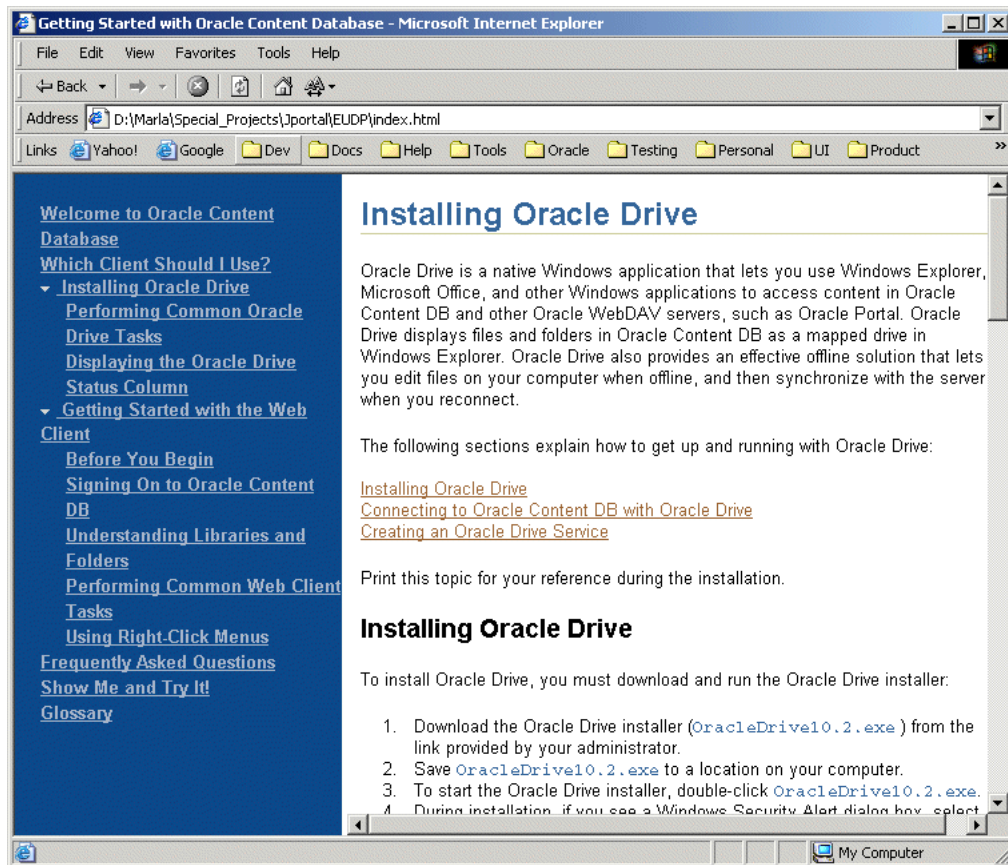
For complete information about how to set up a WebDAV connection between Oracle Drive and Oracle Content DB, as well as information about how to use Oracle Drive, see the Oracle Drive Help. Or, go to the Oracle Content DB New User Orientation (available from the Oracle Content DB Launch Page) for information about installing and using Oracle Drive.

Customizing the New User Orientation

Oracle Content DB comes with a New User Orientation, a set of customizable help pages that users can access from the Oracle Content DB launch page. These pages provide valuable information, such as how to sign on to the Web client and how to get started with Oracle Drive, that can help new users get started with Oracle Content DB. The New User Orientation is only available in English.

Figure 4-3 shows the New User Orientation.

Figure 4-3 Oracle Content DB New User Orientation



You can customize the HTML pages to make the information more useful for your users. For example, the topic called Signing On to Oracle Content DB includes the following text:

"Open a browser window and go to the Oracle Content DB launch page. If you don't know the URL, ask your administrator."

You can replace the value for "the Oracle Content DB URL" with the actual URL (for example, `http://content_db_host_name:port/content`).

You can replace any text in the New User Orientation help files. However, text that is especially appropriate for customization is highlighted in red.

The New User Orientation pages are located on each middle tier, in the following directory:

```
ORACLE_HOME/Apache/Apache/htdocs/eudp/
```

Then main entry point for the New User Orientation help files is `index.html`.

When you update HTML files in the New User Orientation, make sure to update the files on each middle tier.

Managing Oracle Content DB Users

Oracle Content DB supports three types of user repository: Oracle Internet Directory, a third-party LDAP solution (such as iPlanet or Open LDAP), or a file-based user repository. This chapter explains how to use each type of user repository with Oracle Content DB.

This chapter contains the following topics:

- [Using Oracle Internet Directory with Oracle Content DB](#)
- [Using a Third-Party LDAP Server with Oracle Content DB](#)
- [Using a File-Based User Repository with Oracle Content DB](#)
- [User Provisioning in Oracle Content DB](#)
- [Deleting Users in Oracle Content DB](#)
- [Updating User Information in the Oracle Content DB Web Client](#)

Using Oracle Internet Directory with Oracle Content DB

You can use Oracle Internet Directory, part of Oracle Identity Management, as the user repository for Oracle Content DB. Oracle Internet Directory is a general purpose directory service that enables fast retrieval and centralized management of information about dispersed users and network resources. It combines LDAP Version 3 with the high performance, scalability, robustness, and availability of an Oracle Database.

To use Oracle Internet Directory as your Oracle Content DB user repository, you must first install OracleAS Infrastructure, which contains Oracle Identity Management. You must install at least Oracle Internet Directory. Then, provide required details about Oracle Internet Directory during Oracle Content DB installation.

This section provides the following topics:

- [Logging In to Oracle Content DB for the First Time](#)
- [Managing Users in Oracle Internet Directory](#)

Logging In to Oracle Content DB for the First Time

If you are using Oracle Internet Directory as the user repository for Oracle Content DB, use the `orcladmin` user name and password to log in to Oracle Content DB for the first time. This user has all the application administration roles.

After you have created additional users in Oracle Internet Directory, and after those users have logged in to Oracle Content DB, you can delegate application administration roles to other users, as needed.

Managing Users in Oracle Internet Directory

You can use a variety of administration tools to manage users in Oracle Internet Directory. For example, you can use Oracle Internet Directory command-line tools like `ldapadd` and `ldapmodify`, you can use the Oracle Internet Directory Self-Service Console (`oiddas`), or you can use Oracle Directory Manager.

See Also:

- *Oracle Identity Management Guide to Delegated Administration* for information about how to use the Oracle Internet Directory Self-Service Console
- *Oracle Identity Management User Reference* for information about how to use Oracle Internet Directory command-line tools
- *Oracle Internet Directory Administrator's Guide* for information about how to use Oracle Directory Manager

Using a Third-Party LDAP Server with Oracle Content DB

Oracle Content DB supports the following third-party LDAP solutions:

- Microsoft Active Directory
- Sun Directory Server (iPlanet)
- OpenLDAP
- eDirectory

To use a third-party LDAP solution as your user repository for Oracle Content DB, you must first install the third-party LDAP server. Then, provide required details about your third-party LDAP server during Oracle Content DB installation.

For complete information about which third-party LDAP solutions are supported by Oracle Content DB, see *Oracle Application Server Certification Information*.

Note: You cannot configure SSL for the connection between Oracle Content DB and a third-party LDAP server during installation. You can only set up SSL for the connection between Oracle Content DB and a third-party LDAP server after installation. See "[Setting Up Server Only SSL Between Oracle Content DB and Your LDAP Server](#)" on page 3-2 for more information.

This section contains the following topics:

- [Logging In to Oracle Content DB for the First Time](#)
- [Managing Users in a Third-Party LDAP Solution](#)

Logging In to Oracle Content DB for the First Time

If you are using a third-party LDAP server as the user repository for Oracle Content DB, use the user name and password you provided during Oracle Content DB

installation to log in to Oracle Content DB for the first time. This user has all the application administration roles.

After you have created additional users in your user repository, and after those users have logged in to Oracle Content DB, you can delegate application administration roles to other users, as needed.

Managing Users in a Third-Party LDAP Solution

Use the administration tools provided for your third-party LDAP user repository to create, modify, and delete users. Refer to the documentation for your LDAP server for more information.

Using a File-Based User Repository with Oracle Content DB

You can choose to use a file-based user repository with Oracle Content DB. File-based user repositories store user data in a file on each middle-tier computer. To use a file-based user repository as your user repository for Oracle Content DB, select **File-Based** in the Specify User Repository screen during Oracle Content DB installation.

This section contains the following topics:

- [Logging In to Oracle Content DB for the First Time](#)
- [Using a File-Based User Repository with Multiple Oracle Content DB Middle Tiers](#)
- [Managing Users in a File-Based User Repository](#)

Logging In to Oracle Content DB for the First Time

If you are using a file-based user repository with Oracle Content DB, use the `contentadmin` user name to log in to Oracle Content DB for the first time. The password for this user is the same as the Oracle Content DB schema password. This user has all the application administration roles.

After you have created additional users, and after those users have logged in to Oracle Content DB, you can delegate application administration roles to other users, as needed.

Using a File-Based User Repository with Multiple Oracle Content DB Middle Tiers

LDAP-based user repositories, such as Oracle Internet Directory and third-party LDAP solutions, provide a centralized user list against which users are authenticated. In contrast, file-based user repositories store user lists on each middle tier in the `jazn-data.xml` file. The `jazn-data.xml` file is located in `ORACLE_HOME/content/settings`.

Because of this, if you have multiple Oracle Content DB middle tiers, you must ensure that the `jazn-data.xml` files on each middle tier are kept in sync. For example, when you add, modify, or delete users in a file-based user repository, you must add, modify, or delete them on each middle tier.

Because of this limitation, using a file-based user repository is not recommended for production systems. You should use Oracle Internet Directory or a third-party LDAP solution for production deployments of Oracle Content DB.

Managing Users in a File-Based User Repository

You can use the Application Server Control to manage users in a file-based user repository (recommended), or you can use the OracleAS JAAS Provider Admintool.

Using the Application Server Control to Manage Users

Using the Application Server Control is the best way to manage users in a file-based user repository. For example, to add users using the Application Server Control, follow these steps:

1. Connect to the Application Server Control.
2. On the Cluster Topology page, in the Members table, click the **OC4J_Content** link.
3. Click the **Administration** tab.
4. In the Security Providers table row, under the Security heading, click the **Go to Task** icon.
5. In the Application Level Security section, in the **content** table row, click the **Edit** icon. Do not click the **content** link.
6. Click the **Realms** tab.
7. For the ContentDB realm, in the Users column, click the number that shows how many users are in the realm.
8. Click **Create**.
9. Fill in the fields, as necessary. Do not create user names that contain the slash (/) character.
10. If you have multiple middle tiers, repeat these steps for the OC4J_Content instances for the other middle tiers.

See Also: *Oracle Containers for J2EE Security Guide* for full information on using the Application Server Control to manage users in a file-based user repository

Using the OracleAS JAAS Provider Admintool to Manage Users

You can use the OracleAS JAAS Provider Admintool to manage users in a file-based user repository. The Admintool is a lightweight Java application that provides administration for users, roles, policies, and login modules for a file-based user repository. However, you must restart OC4J_Content for changes made by the Admintool to take effect.

You can add, modify, and delete users with the Admintool even if Oracle Content DB is not running.

Admintool functions can be called directly from the command line, or through an interactive shell. The Admintool is located in `ORACLE_HOME/j2ee/home/jazn.jar`.

The general command-line syntax is as follows:

```
% java -jar jazn.jar [-user username -password pwd] [option1 option2 ... ]
```

The following example shows how to add a user through the interactive shell:

```
% java -jar jazn.jar -shell
AbstractLoginModule username : oc4jadmin
AbstractLoginModule password : admin_password
JAZN:> adduser jazn.com user_name user_password
```


See Also: *Oracle Containers for J2EE Security Guide* for full information on using the OracleAS JAAS Provider Admintool

User Provisioning in Oracle Content DB

User provisioning is done on-demand the first time a user logs in to Oracle Content DB. Because users are not provisioned until they log in for the first time, they may not be available in Oracle Content DB even though they exist in the user repository.

For example, after you add a user to your user repository, you may want to add that user to a particular Library in Oracle Content DB. However, you will not be able to search for and add the user until after the user has logged in for the first time.

All user searches in Oracle Content DB are made against the list of users who have already been provisioned in Oracle Content DB. User searches are not made against the actual user repository.

Deleting Users in Oracle Content DB

After you delete users in your user repository, you must run the `deleteuser` script to remove the users from the Oracle Content DB schema. You must run this script regardless of whether you are using Oracle Internet Directory, a third-party LDAP solution, or a file-based user repository.

Running the `deleteuser` Script

The `deleteuser` script is located in:

```
ORACLE_HOME/content/bin
```

To use the script, follow these steps:

1. Create a text file that lists the names of the users you deleted in your user repository. For example:

```
john.smith  
jane.doe
```

Note: The format of user names can vary, depending on the format used by your user repository (for example, `bob`, `john.smith`, or `jane.doe@mydomain.com`). Make sure to specify user names in the same format as your user repository. In other words, list actual user names that are used to log in to Oracle Content DB.

2. At the command line, go to `ORACLE_HOME/content/bin`.
3. Run the following command:

```
./deleteuser ORACLE_HOME input_file
```

For `ORACLE_HOME`, provide the full path name of the Oracle home. For `input_file`, provide the name and path of the file you created in Step 1. For example:

```
./deleteuser $ORACLE_HOME $ORACLE_HOME/content/bin/userstobedeleted.txt
```

What Happens to User Content When a User Is Deleted?

Because all files in Oracle Content DB reside in Libraries, users do not own content. All content belongs to the Library in which it is located. When users are deleted from Oracle Content DB, any data that was uploaded by that user remains in the Oracle Content DB repository.

In some cases, you may want to delete the Personal Library of a deleted user. To do this, you must sign on to Oracle Content DB as a user with the Content Administrator role and switch to Administration Mode. You can then navigate to the appropriate Personal Library and delete it.

Updating User Information in the Oracle Content DB Web Client

In the Oracle Content DB Web client, user information appears in two places: in the User Profile screen, available only to User Administrators, and the User Preferences screen, available to all users.

User Profile Information

In the Oracle Content DB Web client, in Administration mode, user administrators can view user profile information for each user. The following fields are displayed:

- User Name
- First Name
- Last Name
- E-mail Address
- Personal Library

If you are using an LDAP server for your user repository (either Oracle Internet Directory or a third-party LDAP server), some of these values may be provided by the LDAP server. Values provided by the LDAP server are read-only in Oracle Content DB; in order to update these preferences, you must update the information in the LDAP server. The information is then updated in Oracle Content DB by the User Connect Agent. Alternatively, the user administrator can manually refresh the information for a particular user from the Oracle Content DB Web client.

User profile values that are not provided by the LDAP server can be updated in Oracle Content DB by the User Administrator. These values will exist only in Oracle Content DB and will not exist in the user repository.

User Preferences Information

Similar to user profiles, users can view their preferences in the Oracle Content DB Web client. If you are using an LDAP server for your user repository (either Oracle Internet Directory or a third-party LDAP server), some of these values may be provided by the LDAP server. Values provided by the LDAP server are read-only in Oracle Content DB; in order to update these preferences, the user must update their information in the LDAP server. The information is then updated in Oracle Content DB by the User Connect Agent. Alternatively, the user can manually refresh their profile information from the Oracle Content DB Web client.

User preferences that are not provided by the LDAP server can be updated by the user in Oracle Content DB. These values will exist only in Oracle Content DB and will not exist in the user repository.

Setting the First Name, Last Name, and E-mail Address Attributes

If you are using a file-based user repository as your Oracle Content DB user repository, there is no way to provide the First Name, Last Name, and E-mail Address user profile values when you create users. To set these values, log in to the Oracle Content DB Web client as a User Administrator and switch to Administration mode. Then, access the user profile for each user you added and set these attributes.

End users cannot provide values for the First Name, Last Name, and E-mail Address attributes. Only User Administrators can edit these values.

Using Custom BPEL Workflows in Oracle Content DB

You can define custom BPEL workflow processes in [Oracle BPEL Process Manager](#), and then register them in Oracle Content DB. The custom BPEL workflow processes are managed in Oracle BPEL Process Manager.

Note: Oracle Content DB comes with two default workflow processes, Parallel Vote and Serial Approval. Oracle Content DB uses [Oracle Workflow](#) to manage these default workflow processes. Oracle Workflow is configured and integrated with Oracle Content DB during Oracle Content DB configuration.

This chapter provides information about the following topics:

- [About Custom Workflows](#)
- [Creating Custom Workflows in Oracle BPEL Process Manager](#)
- [Registering Custom Workflows with Oracle Content DB](#)
- [Deleting Custom Workflows from Oracle Content DB](#)

About Custom Workflows

Custom workflows can be created in Oracle BPEL Process Manager, an Oracle product that provides a framework for designing, deploying, monitoring, and administering processes based on BPEL standards. Custom workflows are only available to the default Site in Oracle Content DB; additional Sites cannot use custom workflows.

After you have created a custom workflow in Oracle BPEL Process Manager, you can use the Application Server Control to register the workflow in Oracle Content DB. You must provide detailed information about the workflow, including the names of the launch event and cancel event, as well as specific parameters that are used in the workflow.

Custom workflows can be blocking or nonblocking. A blocking workflow is one that requires an action for it to complete. For example, you can create a blocking workflow to handle document approval for publication: action on the part of the approvers is required before a document is published. An example of a nonblocking workflow is one that handles sending out notifications for published documents; in this case, a document can be published without waiting for the notifications to be sent.

About BPEL

The Business Process Execution Language (BPEL) is an XML-based language for enabling task-sharing across multiple enterprises using a combination of Web services. BPEL is based on the XML Schema, Simple Object Access Protocol (SOAP), and Web Services Description Language (WSDL). Using BPEL, you design a business process that integrates a series of discrete services into an end-to-end process flow. For more information about BPEL and Oracle BPEL Process Manager, see *Oracle BPEL Process Manager Developer's Guide*.

Creating Custom Workflows in Oracle BPEL Process Manager

For information about using Oracle BPEL Process Manager, see *Oracle BPEL Process Manager Developer's Guide*. For information about creating custom workflows for use with Oracle Content DB, see the Oracle Content DB developer documentation.

Registering Custom Workflows with Oracle Content DB

After the custom workflow has been created in Oracle BPEL Process Manager, you can register the custom workflow with Oracle Content DB using the Application Server Control.

To register custom workflows in Oracle Content DB:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Custom Workflows table row, click the **Go to Task** icon.
4. Click **Register Workflow**.
5. Enter a name for the workflow. The name you provide must match the name of the workflow you created in Oracle BPEL Process Manager.
6. Enter a description of the workflow (optional).
7. Enter the **Launch Event** for the workflow. The event you provide must match the name of the corresponding Partner Link Correlation ID in Oracle BPEL Process Manager. The Launch Event cannot exceed 30 characters.
8. Enter the **Cancel Event** for the workflow. If you have a corresponding Partner Link Correlation ID in Oracle BPEL Process Manager, the event you provide must match the name of the Correlation ID. The Cancel Event cannot exceed 30 characters.

Typically, the Cancel Event is not used. If this is the case, you can provide any string for this field (for example, CANCEL_MY_WORKFLOW).
9. Select **Blocking** if this workflow is a blocking workflow. A blocking workflow is one that requires an action for it to complete.
10. Select **Approvers Required** if this workflow requires approvers.
11. Click **Add** to add parameters for this workflow.
12. On the Register Workflow - Add Parameter page, specify information for the parameter you want to add:

- **Name:** The name you provide must match the name of the parameter in Oracle BPEL Process Manager. The parameter name cannot exceed 30 characters.
- **Description:** Enter an optional description of the parameter.
- **Fixed Value:** Select this option if you do not want to allow changes to this parameter after the workflow has been created.
- **Required:** Select this option if this parameter is required for the workflow to complete.
- **Type:** Select one of the following type options for this parameter:
 - String
 - Boolean
 - Integer Number Range
 - Enumerated String
 - Date
 - Decimal Number Range
 - Path
 - Time Period
 - User/Group

If you select **Integer Number Range**, **Decimal Number Range**, or **Time Period**, you can optionally specify a minimum and maximum value for this parameter. If you select **Enumerated String**, you must specify values for this parameter. To do this, specify a value and click **Add**. You can manage the list of enumerated values by using the arrows provided to alter the order of the list. You can remove values by clicking **Remove**.

13. Click **OK** on the Register Workflow - Add Parameter page.
14. Optionally, provide a default value for the parameter by specifying a value in the **Default Value** column of the Parameters table. If you selected **Fixed Value** for this parameter, you must provide a default value. Note the following:
 - To specify a default for a Date type parameter, click the calendar icon to ensure that the date you specify appears in the correct format (MM/dd/yyyy).
 - For a Path type parameter, you must supply a valid Oracle Content DB path (for example, /mysite/mylibrary/myfolder).
 - For a User/Group type parameter, you must supply a valid Oracle Content DB user or group name.
15. Repeat Steps 11 through 14 to add additional parameters as needed. You can modify parameters that you have already added by clicking the parameter name.
16. Click **OK** on the Register Workflow page.

You cannot edit a registered workflow. If you need to make any changes, you must delete the custom workflow, then register it again.

Deleting Custom Workflows from Oracle Content DB

You can use the Application Server Control to delete custom workflows. If any folder or Library in Oracle Content DB has been configured to use a particular custom workflow, the custom workflow cannot be deleted.

To delete custom workflows:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Custom Workflows table row, click the **Go to Task** icon.
4. Select the workflow you want to delete and click **Delete**.
5. On the Warning page, click **Yes**. The workflow will be deleted as soon as the last active workflow completes.

Managing Oracle Content DB Processes

You can use the Application Server Control to manage Oracle Content DB processes, including starting and stopping servers and managing nodes. You can also manage Oracle Content DB domain and node processes from the command line using the `opmnctl` utility. To manage Oracle Content DB using the Application Server Control or `opmnctl`, OPMN must be started on all middle tiers.

This chapter provides information about the following topics:

- [About the Oracle Content DB Domain](#)
- [Managing Nodes at Run Time](#)
- [Managing Services at Run Time](#)
- [Managing Servers at Run Time](#)
- [Managing Oracle Content DB from the Command Line](#)

About the Oracle Content DB Domain

An Oracle Content DB **domain** is a logical grouping of Oracle Content DB nodes and an Oracle Database instance that contains the Oracle Content DB data.

The Oracle Content DB software runs as a set of middle tier processes, called **nodes**. Oracle Content DB node processes manage one or more **services**, **agents**, and **protocol** servers.

Each node runs on a particular middle tier, or in other words, within a particular Oracle home. You can have multiple middle tiers on the same computer.

Each node runs as part of an **OC4J** process. On each middle tier, the OC4J instance for the Oracle Content DB node is `OC4J_Content`. You cannot have more than one node on a single middle tier.

Starting and Stopping the Oracle Content DB Domain

You can start and stop the domain using the Application Server Control. Even if your domain is distributed across multiple middle tiers, you can start and stop the domain from a single middle tier.

The steps described in the following sections assume that all Oracle Application Server instances for Oracle Content DB are part of the same cluster. See *Oracle Application Server Administrator's Guide* for information about how to configure OracleAS Clusters.

Starting the Domain

To start the Oracle Content DB domain from any middle tier:

1. Access the Application Server Control.
2. On the Cluster Topology page, in the Members table, select all Oracle Content DB processes (OC4J_Content instances) across all middle tiers. If you only have one middle tier, you only need to select one OC4J_Content process.

Figure 7–1 shows the Cluster Topology page.

Figure 7–1 Cluster Topology Page

Cluster Topology Page Refreshed Aug 30, 2006 1:56:08 PM CDT • View

Overview

Hosts 1 Application Servers 1
 OC4J Instances 3 HTTP Server Instances 1

Members

View By Application Servers

Start Stop Restart

[Select All](#) | [Select None](#) | [Expand All](#) | [Collapse All](#)

Select	Focus	Name	Status	Type	Category	Host	CPU (%)	Memory (MB)
<input type="checkbox"/>		▼ All Application Servers						
<input type="checkbox"/>	<input checked="" type="checkbox"/>	▼ Aug29basoid.stbec05.us.oracle.com		Application Server		stbec05		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	▶ home (JVMs: 1)	↑	OC4J			0.07	174.99
<input type="checkbox"/>		HTTP_Server	↑	Oracle HTTP Server			0.03	53.31
<input type="checkbox"/>	<input checked="" type="checkbox"/>	▶ OC4J_Content (JVMs: 1)	↑	OC4J			0.00	328.72
<input type="checkbox"/>	<input checked="" type="checkbox"/>	▶ OC4J_Portal (JVMs: 1)	↑	OC4J			0.06	171.54

Indicates the active ASControl instance.
 TIP If a parent topology member is selected all contained members are implicitly selected.

3. Click **Start**. The entire Oracle Content DB domain is started across all middle tiers.

Note: Oracle HTTP Server (HTTP_Server) must also be running on each middle tier for Oracle Content DB to function properly.

Restarting the Domain

To restart the Oracle Content DB domain from any middle tier:

1. Access the Application Server Control.
2. On the Cluster Topology page, in the Members table, select all Oracle Content DB processes (OC4J_Content instances) across all middle tiers.
3. Click **Restart**, then on the Confirmation page, click **Yes**. Only those processes that are running are affected. Processes that are not running will not be started.

Stopping the Domain

To stop the Oracle Content DB domain from any middle tier:

1. Access the Application Server Control.

2. On the Cluster Topology page, in the Members table, select all Oracle Content DB processes (OC4J_Content instances) across all middle tiers.
3. Click **Stop**, then on the Confirmation page, click **Yes**. The entire Oracle Content DB domain is stopped across all middle tiers.

Note: If you are performing scheduled maintenance and want to stop one middle tier at a time, you can start and stop individual node processes. See "[Starting, Stopping, and Restarting OC4J_Content Instances](#)" on page 7-3 for more information.

Managing Nodes at Run Time

You can use the Application Server Control to start, stop, and restart nodes (OC4J_Content instances), as well as modify run-time node properties.

You can also use the `opmnctl` utility to start, stop, and restart nodes, as well as check node status; see "[Managing Oracle Content DB from the Command Line](#)" on page 7-16 for more information.

This section contains the following topics:

- [Starting, Stopping, and Restarting OC4J_Content Instances](#)
- [Modifying Nodes at Run Time](#)

Starting, Stopping, and Restarting OC4J_Content Instances

You can start, stop, and restart OC4J_Content instances (in other words, Oracle Content DB **nodes**) using the Application Server Control. Even if you have multiple middle tiers, you can start, stop, and restart OC4J_Content instances from a single middle tier, regardless of where the OC4J_Content instances are located.

If an OC4J_Content instance fails to start, stop, or restart, check the logs for more information. Click **Logs** in the upper right corner of any Application Server Control page to search for and view the `application.log` file for the OC4J_Content instance.

Starting OC4J_Content Instances

To start an OC4J_Content instance using the Application Server Control:

1. On the Cluster Topology page, in the Members table, select the OC4J_Content instance you want to start.
2. Click **Start**. The Status column displays a green arrow pointing up, indicating that the OC4J_Content instance is up.

Stopping OC4J_Content Instances

To stop an OC4J_Content instance using the Application Server Control:

1. On the Cluster Topology page, in the Members table, select the OC4J_Content instance you want to stop.
2. Click **Stop**.
3. On the Confirmation page, click **Yes**. The Status column displays a red arrow pointing down, indicating that the OC4J_Content instance is down.

Restarting OC4J_Content Instances

You can only restart OC4J_Content instances that are already started.

To restart an OC4J_Content instance using the Application Server Control:

1. On the Cluster Topology page, in the Members table, select the OC4J_Content instance you want to restart.
2. Click **Restart**.
3. On the Confirmation page, click **Yes**. The OC4J_Content instance is stopped, then started again.

Modifying Nodes at Run Time

You can make run-time changes to nodes, such as changing the service used by the node or changing servers. Changes made at run time are lost when the node is restarted. If you want to make permanent changes, modify the [node configuration](#) for the node and then restart the node.

To modify a node at run time using the Application Server Control:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. In the Services section, you can create, modify, or delete services for this node. See "[Managing Services at Run Time](#)" on page 7-4 for more information.
3. In the Servers section, you can create, modify, or delete servers for this node. See "[Managing Servers at Run Time](#)" on page 7-11 for more information.

Managing Services at Run Time

You can use the Application Server Control to create or delete [services](#) for a particular node. When you create a service, you specify what [service configuration](#) object provides its properties.

You can make temporary (run-time) changes to a service by modifying the service from the Content DB Home page. You can also dynamically configure the Committed Data Cache, Read-only Connection Pool, and the Writeable Connection Pool while the service runs. Changes made to services at run time are lost when the node is restarted.

You can also make permanent changes to a service by modifying its service configuration; see "[Managing Service Configurations](#)" on page 8-8 for more information.

This section contains the following topics:

- [Creating Services](#)
- [Modifying Run-Time Service Parameters](#)
- [Managing the Committed Data Cache](#)
- [Managing the Connection Pools](#)
- [Deleting Services](#)

Creating Services

You can create services for a particular node by modifying the node at run time, or by modifying the appropriate node configuration. You can also create services when you create node configurations.

Creating Services at Run Time

To create a service by modifying the node at run time:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, in the Services section, click **Create**.
3. On the Create Service page, enter a name for the service. It must be unique within the node. Service names are not case-sensitive.
4. Choose a **Service Configuration** on which to base this service.
5. Click **OK** on the Create Service page.

These changes will be lost when the node is restarted.

Permanently Adding Services to a Node

To permanently add a service to a node by modifying its node configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. Click the name of the node configuration for which you want to add a service.
5. In the Services section, click **Add**.
6. On the Add Service page, enter a name for the service. It must be unique within the node. Service names are not case-sensitive.
7. Select a **Service Configuration** on which to base this service.
8. Select **Active** if you want this service to be automatically started by the node.
9. Click **OK** on the Add Service page.
10. Click **OK** on the Edit Node page.

Changes take effect when the node is restarted.

Modifying Run-Time Service Parameters

You can make run-time changes to services, such as limiting concurrent sessions or choosing whether or not to accept new sessions. Changes you make at run time are lost when the node is restarted. To make permanent changes to a service, edit the service configuration directly. See "[Modifying Service Configurations](#)" on page 8-10 for more information.

To modify run-time service parameters:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, in the Services section, click the name of the service you want to modify.
3. Click the **Administration** tab.
4. In the Service Properties table row, click the **Go to Task** icon.
5. You can change the following properties:
 - **Concurrent Sessions:** You can have an unlimited number of concurrent sessions, or you can limit concurrent sessions to a specified number. If you have an unlimited number of concurrent sessions, you may run out of memory. See "[Oracle Content DB Sizing Guidelines](#)" on page 2-4 for more information.
 - **Accepting New Sessions:** Select this option if you want the service to accept additional sessions.
 - **Disposed on Last Disconnected Session:** Select this option if you want the service to shut down automatically when the last session is disconnected.
6. Click **Apply** to save your changes.
7. Use the locator links to return to the Content DB Home page.

These changes will be lost when the node is restarted.

Changing the Service Configuration Used by the Service

You can change the service configuration for a particular service from the Edit Node Configuration page:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. On the Node Configurations page, click the name of the node configuration that uses the service you want to modify.
5. In the Services section, click the name of the service you want to change.
6. Select a new service configuration from the **Configuration** list and click **OK**.
7. On the Edit Node page, click **OK**.

Changes take effect when the node is restarted.

Managing the Committed Data Cache

The **Committed Data Cache** provides caching of the attribute values of frequently used objects without a database request, improving performance and scalability. Least recently used data is periodically purged from the cache. Each service has its own Committed Data Cache.

You can make run-time changes to the Committed Data Cache properties for a service using the Application Server Control. You can also view Committed Data Cache

statistics for a service. See ["Monitoring Service Performance"](#) on page 9-2 for information about viewing or resetting the statistics.

See ["Oracle Content DB Sizing Guidelines"](#) on page 2-4 for more information about cache settings.

Making Run-Time Changes to Committed Data Cache Properties

To make run-time changes to Committed Data Cache properties:

1. Connect to the Application Server Control and go to the Content DB Home page. See ["Accessing the Oracle Content DB Home Page"](#) on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the name of the service you want to modify.
3. Click the **Administration** tab.
4. In the Data Cache table row, click the **Go to Task** icon.

[Figure 7-2](#) shows the Committed Data Cache Administration page.

Figure 7-2 Committed Data Cache Administration Page

Committed Data Cache Administration

* Cache Capacity	<input type="text" value="7500"/>	<input type="button" value="Calculate"/>
<small>Click "Calculate" to automatically set the purge triggers and purge target based on cache capacity.</small>		
* Normal Purge Trigger	<input type="text" value="5000"/>	
* Urgent Purge Trigger	<input type="text" value="5500"/>	
* Emergency Purge Trigger	<input type="text" value="6000"/>	
* Purge Target	<input type="text" value="4000"/>	

5. You can change the following cache settings:
 - **Cache Capacity:** The absolute maximum size of the data cache of the service, in LibraryObjects. (The LibraryObject class is the base class for all persistent Oracle Content DB objects.) The service data cache holds the attribute values of recently used LibraryObjects.
After you specify Cache Capacity, you can click **Calculate** to automatically fill in the values for the other parameters based on the capacity you specified.
 - **Normal Purge Trigger:** The cache size, in LibraryObjects, at which the service data cache schedules a low-priority purge of data that has not been recently used.
 - **Urgent Purge Trigger:** The cache size, in LibraryObjects, at which the service data cache schedules a high-priority purge of data that has not been recently used. The value must be greater than the Normal Purge Trigger value.
 - **Emergency Purge Trigger:** The cache size, in LibraryObjects, at which the service data cache performs an immediate purge of data that has not been recently used. The value must be greater than the Urgent Purge Trigger value, but less than the Cache Capacity value.
 - **Purge Target:** The target cache size, in LibraryObjects, upon completion of a purge cycle. The value must be less than the Normal Purge Trigger value.
6. Click **Apply** after you are finished specifying cache settings.

Changes you make at run time are lost when the node is restarted. To make permanent changes to Committed Data Cache properties, edit the service

configuration directly. See ["Modifying Service Configurations"](#) on page 8-10 for more information.

[Table 7-1](#) maps the properties on the Committed Data Cache Administration page with their service configuration parameter equivalents.

Table 7-1 Committed Data Cache Service Configuration Properties

Property	Service Configuration Parameter Equivalent
Cache Capacity	IFS.SERVICE.DATACACHE.Size
Normal Purge Trigger	IFS.SERVICE.DATACACHE.NormalTrigger
Urgent Purge Trigger	IFS.SERVICE.DATACACHE.UrgentTrigger
Emergency Purge Trigger	IFS.SERVICE.DATACACHE.EmergencyTrigger
Purge Target	IFS.SERVICE.DATACACHE.PurgeTarget

Managing the Connection Pools

There are two connection pools used by each service: the **Read-Only Connection Pool** and the **Writable Connection Pool**. The Read-Only Connection Pool is a set of database connections shared by the sessions to perform database read operations. The Writeable Connection Pool is a set of database connections shared by the sessions to perform database read and write operations within a database transaction.

A minimum number of connections are created in each pool when the service is started. Depending on the number of concurrent operations performed by the sessions, and the type of operations, additional connections may be added to each pool up to a specified maximum.

You can make run-time changes to the Connection Pool properties for a particular service using the Application Server Control. You can also view Read-Only and Writeable Connection Pool statistics for a particular service. See ["Monitoring Service Performance"](#) on page 9-2 for information about viewing or resetting the statistics.

See ["Oracle Content DB Sizing Guidelines"](#) on page 2-4 for more information about connection pool settings.

About the Statement Cache

To improve performance, Oracle Content DB reuses Oracle prepared statements (objects used to query and update the database) when possible. Because Oracle Content DB stores statements in the statement cache, similar queries can reuse existing statements. Least recently used statements are purged when the number of statements in the cache equals the Statement Cache Purge Trigger value.

You can manage statement cache settings from the Connection Pool Administration page. You can also view statement cache statistics (number of attempted purges and purge count) on the Connection Pool Statistics page. See ["Monitoring Service Performance"](#) on page 9-2 for more information.

Making Run-Time Changes to Connection Pool Properties

To make run-time changes to Connection Pool properties:

1. Connect to the Application Server Control and go to the Content DB Home page. See ["Accessing the Oracle Content DB Home Page"](#) on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the name of the service you want to modify.

3. Click the **Administration** tab.
4. In the Read-Only Connection Pool or Writable Connection Pool table row, click the **Go to Task** icon.

Figure 7-3 shows the Read-Only Connection Pool Administration page.

Figure 7-3 Read-Only Connection Pool Administration Page

Read-Only Connection Pool Administration

Revert Apply

* Minimum Number of Connections	<input type="text" value="2"/>
* Target Maximum Number of Connections	<input type="text" value="10"/>
* Absolute Maximum Number of Connections	<input type="text" value="20"/>
* Statement Cache Purge Target	<input type="text" value="95"/>
* Statement Cache Purge Trigger	<input type="text" value="105"/>
* Target Size Timeout (ms)	<input type="text" value="1000"/>
* Maximum Size Timeout (ms)	<input type="text" value="10000"/>
Default Number of Rows Prefetched	0

Figure 7-4 shows the Writable Connection Pool Administration page.

Figure 7-4 Writable Connection Pool Administration Page

Writable Connection Pool Administration

Revert Apply

* Minimum Number of Connections	<input type="text" value="2"/>
* Target Maximum Number of Connections	<input type="text" value="10"/>
* Absolute Maximum Number of Connections	<input type="text" value="20"/>
* Statement Cache Purge Target	<input type="text" value="160"/>
* Statement Cache Purge Trigger	<input type="text" value="200"/>
* Target Size Timeout (ms)	<input type="text" value="1000"/>
* Maximum Size Timeout (ms)	<input type="text" value="10000"/>
Default Number of Rows Prefetched	0

5. On the Read-Only Connection Pool Administration page or Writable Connection Pool Administration page, you can change the following settings:
 - **Minimum Number of Connections:** The initial number of database connections in the connection pool.
If you change this property, ensure the value you specify is greater than the current size for this connection pool. You can view the current connection pool size from the Performance tab for the service. See "[Monitoring Service Performance](#)" on page 9-2 for more information.
 - **Target Maximum Number of Connections:** The target maximum number of database connections in the connection pool. The value must be greater than or equal to the Minimum Number of Connections value.
 - **Absolute Maximum Number of Connections:** The absolute maximum number of database connections in the connection pool. The value must be greater than or equal to the Target Maximum Number of Connections value.
 - **Statement Cache Purge Target:** The target cache size, in number of statements, for the statement cache upon completion of a purge cycle. The value must be less than the Statement Cache Purge Trigger value.

- **Statement Cache Purge Trigger:** The cache size, in number of statements, at which the statement cache schedules a purge.
- **Target Size Timeout:** The maximum period, in milliseconds, that the service will postpone a connection allocation request when there are no unallocated connections, when the current size of the connection pool is greater than or equal to its target size but less than the maximum size. If a database connection does not become available within this period, a new connection will be created.
- **Maximum Size Timeout:** The maximum period, in milliseconds, that a service will postpone a connection allocation request when there are no unallocated connections, when the current size of the connection pool is equal to its maximum size. If a database connection does not become available within this period, the allocation request will fail, and an exception will occur.

6. Click **Apply** after you are finished specifying connection pool settings.

Changes you make at run time are lost when the node is restarted. To make permanent changes to Connection Pool properties, edit the service configuration directly. See ["Modifying Service Configurations"](#) on page 8-10 for more information.

[Table 7–2](#) maps the properties on the Read-Only Connection Pool Administration page and Writable Connection Pool Administration page with their service configuration parameter equivalents.

Table 7–2 Connection Pool Service Configuration Properties

Property	Service Configuration Parameter Equivalent
Minimum Number of Connections	IFS.SERVICE.CONNECTIONPOOL.READONLY.MinimumSize IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MinimumSize
Target Maximum Number of Connections	IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSize IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSize
Absolute Maximum Number of Connections	IFS.SERVICE.CONNECTIONPOOL.READONLY.MaximumSize IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSize
Statement Cache Purge Target	IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheTarget IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheTarget
Statement Cache Purge Trigger	IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheSizeTrigger IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheSizeTrigger
Target Size Timeout	IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSizeTimeout IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSizeTimeout
Maximum Size Timeout	IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSizeTimeout IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSizeTimeout

Deleting Services

You can delete services for a node by modifying the node at run time, or by modifying the appropriate node configuration.

If you delete a service with active sessions, and if there are data transfers in progress over those sessions, data may be lost when you delete the service. In addition, any servers using this service will stop accepting new requests.

Deleting Services at Run Time

To delete a service by modifying the node at run time:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, in the Services section, select the service you want to delete and click **Delete**. Each node must have one active service.
3. On the Confirmation page, click **Yes**.

If you delete a service at run time that is defined in the node configuration, the service will reappear on the node when the node is restarted. To permanently delete the service, you must remove it from the node configuration, as described in the following section.

Permanently Removing Services from a Node

To permanently remove a service from a node by modifying its node configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. On the Node Configurations page, click the name of the node configuration that uses the service you want to remove.
5. In the Services section, select the service you want to remove and click **Remove**.
You cannot remove a service if it is the only service defined in the node configuration. Each node must have at least one active service.
6. Click **OK**.

Changes take effect when the node is restarted.

Managing Servers at Run Time

You can use the Application Server Control to create or delete **servers** for a particular node. When you create a server, you specify what **server configuration** object provides its properties.

You can make temporary (run-time) changes to a server by modifying the server from the Content DB Home page. Changes made to servers at run time are lost when the node is restarted.

You can also make permanent changes to a server by modifying its server configuration. See "[Managing Server Configurations](#)" on page 8-11 for more information.

This section contains the following topics:

- [Creating Servers](#)
- [Starting, Stopping, Restarting, Suspending, and Resuming Servers](#)
- [Modifying Run-Time Server Parameters](#)
- [Reloading Servers](#)
- [Deleting Servers](#)

Creating Servers

You can create servers for a particular node by modifying the node at run time, or by modifying the appropriate node configuration. You can also create servers when you create node configurations.

Creating Servers at Run Time

To create a server by modifying the node at run time:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, in the Servers section, click **Create**.
3. On the Create Server page, enter a name for the server. It must be unique within the node.
4. Select a **Service Name** to support this server.
5. Select a **Server Configuration** on which to base this server.
6. If you want this server to be started after it has been created, ensure that **Start the server after it has been created** is selected. Otherwise, deselect this option.
7. Click **OK**.

These changes will be lost when the node is restarted.

Permanently Adding Servers to a Node

To permanently add a server to a node by modifying its node configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. Click the name of the node configuration for which you want to add a server.
5. In the Servers section, click **Add**.
6. On the Add Server page, enter a name for the server. It must be unique within the node.
7. Select a **Server Configuration** on which to base this service.
8. Select a **Service** to support this server.
9. For **Initial Priority**, select the Java thread priority of the server.

10. Select **Active** to deploy this server on the node at run time. If you do not select this option, this server will not appear in the Servers list on the Node page.
11. Select **Initially Started** if you want this server to be automatically started by the node. You should only select this option for active nodes.
12. Click **OK**.
13. On the Edit Node page, click **OK**.

Changes take effect when the node is restarted.

Starting, Stopping, Restarting, Suspending, and Resuming Servers

Which servers and agents start up with the node are defined in the node configuration. Any servers and agents marked "Active" and "Initially Started" in the node configuration are started automatically when you start the domain.

You can also manually start, stop, restart, suspend, and resume servers from the Content DB Home page for a particular node. The Create, Delete, and Reload buttons are discussed in separate sections.

To manage servers from the Content DB Home page for a particular node:

1. Connect to the Application Server Control and go to the Content DB Home page. See ["Accessing the Oracle Content DB Home Page"](#) on page 1-3 for information about how to do this.

[Figure 7-5](#) shows the Servers section of the Content DB Home page.

Figure 7-5 Servers Section of Content DB Home Page

Servers

Status Legend: ▶ Started ■ Stopped ▶ Starting ■ Stopping ■ Suspended

Select	Name ▲	Type	Status	Last Start Time	Last Stop Time	Service	Priority
<input checked="" type="radio"/>	BackgroundRequestAgent	AGENT	▶	Aug 29, 2006 2:22:17 PM PDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	CleanupAgent	AGENT	▶	Aug 29, 2006 2:22:26 PM PDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	ContentAgent	AGENT	■	Unavailable	Unavailable	IfsDefaultService	5
<input type="radio"/>	ContentGarbageCollectionAgent	AGENT	▶	Aug 29, 2006 2:22:19 PM PDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	DanglingObjectAVCleanupAgent	AGENT	▶	Aug 29, 2006 2:22:20 PM PDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	EcmHttpServer	HTTP	▶	Aug 29, 2006 2:22:20 PM PDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	EventExchangerAgent	AGENT	▶	Aug 29, 2006 2:22:22 PM PDT	Unavailable	IfsDefaultService	5
<input type="radio"/>	ExpirationAgent	AGENT	▶	Aug 29, 2006 2:22:17 PM PDT	Unavailable	IfsDefaultService	5

2. On the Content DB Home page, in the Servers section, there is a list of all servers for this OC4J_Content instance. Check the Status column to see whether a particular server is started, stopped, starting, stopping, or suspended. Use the following buttons to manage servers:
 - **Start:** Use this option to start a server that is not running.
 - **Stop:** Use this option to stop a server that is running or suspended.
 - **Restart:** Use this option to stop and then start a server that is running. This option does not refresh the server configuration information.
 - **Suspend:** Use this option to suspend a server that is running.

- **Resume:** Use this option to resume a server that is suspended.

The Suspend and Resume functions are not available for all protocol servers.

If a server fails to start, check for errors in the `application.log` file for the OC4J_Content instance.

Ensuring Servers Are Started When the Node Is Started

Which servers and agents start with the node are defined in the node configuration. Servers and agents marked Active and Initially Started in the node configuration are started automatically when you start the domain.

To ensure that a particular server starts when the node restarts, you must modify the node configuration for the node where the server is running:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. Click the name of the node configuration you want to modify.
5. In the Servers section, select the server you want to change and click **Edit**.
6. Select **Initially Started**.
7. Click **OK**.
8. On the Edit Node page, click **OK**.

Modifying Run-Time Server Parameters

You can make run-time changes to servers, such as changing the Java thread priority of the server or changing run-time server properties. Changes you make at run time are lost when the node is restarted or when the server is reloaded. To make permanent changes to a server, edit the server configuration directly. See "[Modifying Server Configurations](#)" on page 8-15 for more information.

To modify run-time server parameters:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, in the Servers section, click the name of the server you want to modify.
3. In the General section, click **Change Priority** to change the Java thread priority of the server. On the Change Priority page, select a new priority and click **OK**. Most servers and agents let you change the Java thread priority at run time, but a few servers do not provide this option.
4. The run-time properties for the server are displayed in the Runtime Properties section. Properties that can be modified at run time are displayed as links. Click the name of a property to update it. Some run-time properties can only be modified when the server is stopped.
5. Use the locator links to return to the Content DB Home page.

These changes will be lost when the server is reloaded or when the node is restarted.

Changing the Server Configuration Used by the Server

To change the configuration used by a server, delete the existing server and then create a new server from the Content DB Home page. Alternatively, you can change the configuration for a server from the Edit Node Configuration page:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. Click the name of the node configuration that contains the server you want to modify.
5. In the Servers section, select the server you want to change and click **Edit**.
6. Select a new server configuration from the **Configuration** drop-down list.
7. Click **OK**.
8. On the Edit Node page, click **OK**.

Changes take effect when the server is reloaded or when the node is restarted.

Reloading Servers

If you modify a server configuration, you need to reload the server before the changes take effect. Restarting a server and reloading a server are different functions:

- **Restart** stops and then starts the server. You can only restart servers that are started. Restarting the server will not pick up changes to server configuration properties.
- **Reload** does the following:
 - Stops the server, if it is not stopped already.
 - Deletes the server.
 - Creates a new instance of the server, picking up any changes to the server configuration properties.
 - Returns the server to the state it was in when you clicked Reload (stopped, running, or suspended).

Both restarting and reloading a server will disconnect any users connected to that server.

To reload a server:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, in the Servers section, select the server you want to reload (for example, `EcmHttpServer`).
3. Click **Reload**, then click **Yes** on the Confirmation page. The server picks up the new server properties.

Deleting Servers

You can delete servers from a node by modifying the node at run time, or by modifying the appropriate node configuration.

Deleting Servers at Run Time

To delete a server by modifying the node at run time:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, in the Servers section, select the server you want to delete and click **Stop**, if it is not stopped already. You cannot delete a server that is running or suspended.
3. Select the server again and click **Delete**.
4. On the Confirmation page, click **Yes**. The server still appears in the server list, but the following message is displayed: "This server is configured but not loaded now."

If you delete a server at run time that is defined in the node configuration, the server will reappear on the node when the node is restarted. To permanently delete the server, you must remove it from the node configuration, as described in the following section.

Permanently Removing Servers from a Node

To permanently remove a server from a node by modifying its node configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. Click the name of the node configuration that contains the server you want to remove.
5. In the Servers section, select the server you want to remove and click **Remove**.
6. Click **OK**.

Changes take effect when the node is restarted.

Managing Oracle Content DB from the Command Line

Use `opmnctl`, the command-line tool for OPMN, to manage the Oracle Content DB domain and nodes. The OPMN command-line tool can be found in:

```
ORACLE_HOME/opmn/bin
```

Checking Node Status

Use the following command to check the status of Oracle Content DB nodes (OC4J_ Content instances) on the local middle tier:

```
./opmnctl status
```

Include the `@cluster` option to check nodes on all middle tiers, as follows:


```
./opmnctl @cluster status
```

Starting, Stopping, or Restarting the Oracle Content DB Domain

Use the following commands to start, stop, or restart Oracle Content DB domain processes (OC4J_Content instances) across all Oracle Content DB middle tiers:

```
./opmnctl @cluster startproc process-type=OC4J_Content  
./opmnctl @cluster stopproc process-type=OC4J_Content  
./opmnctl @cluster restartproc process-type=OC4J_Content
```

Starting, Stopping, or Restarting Node Processes

Use the following commands to start, stop, or restart Oracle Content DB node processes (OC4J_Content instances) on the local middle tier:

```
./opmnctl startproc process-type=OC4J_Content  
./opmnctl stopproc process-type=OC4J_Content  
./opmnctl restartproc process-type=OC4J_Content
```

To start, stop, or restart a particular Oracle Content DB node process on a remote middle tier, include the Oracle Application Server instance name for the remote middle tier. For example:

```
./opmnctl @instance:remote_instance_name startproc process-type=OC4J_Content
```

If you are unsure of which Oracle Application Server instance name to use, use the `opmnctl @cluster status` command to list Oracle Application Server instance names.

Note: Before you log in to Oracle Content DB after starting a node process (OC4J_Content instance), make sure that both the OC4J_Content instance and Oracle HTTP Server are running. To do this, use the following command:

```
opmnctl status
```

Changing Oracle Content DB Configuration Settings

Your initial Oracle Content DB domain configuration is based on default settings. You can change this configuration at any time using the Application Server Control.

When the Oracle Content DB domain is started, it uses the **domain properties** contained in the repository to determine domain behavior, such as the maximum size of a single file that can be uploaded to Oracle Content DB. Each node (OC4J_Content instance) has a **node configuration** that determines its run-time behavior. Each service has a **service configuration** that determines its size and characteristics. The **server configuration** for each server or agent provides values for properties, such as the default port number or activation period.

This chapter provides information about the following topics:

- [Managing Domain Properties](#)
- [Managing Node Configurations](#)
- [Managing Service Configurations](#)
- [Managing Server Configurations](#)

Managing Domain Properties

Domain properties are settings that apply to the entire domain. When the Oracle Content DB domain is started, it uses the domain properties contained in the repository to determine domain behavior, such as the maximum size of a single file that can be uploaded to Oracle Content DB.

You can view all the domain properties using the Application Server Control. Only underlined properties can be changed.

Changing Domain Properties

To change domain properties:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Domain Properties table row, click the **Go to Task** icon. The Domain Properties page appears.


[Figure 8–1](#) shows the Domain Properties page.

Figure 8–1 Domain Properties Page

Page Refreshed Aug 29, 2006 6:09:50 PM CDT

Domain properties with names displayed as links can be changed. Domain properties that contain inner properties display a Details icon. Click the icon to view the inner properties.

Search

Name ▲	Type	Value
IFS.DOMAIN.ACCESSCONTROLLIST.BypassNameUniquenessCheck	BOOLEAN	true
IFS.DOMAIN.ACCESSCONTROLLIST.CompositeAclSupported	BOOLEAN	false
IFS.DOMAIN.ACLINDEX.EventTarget	PUBLICOBJECT	
IFS.DOMAIN.AGENTEVENTTARGET.VersionPurgeAgent	PUBLICOBJECT	IFS.DOMAIN.AGENTEVENTTARGET.Vers
<u>IFS.DOMAIN.ANTIVIRUS.Enabled</u>	BOOLEAN	false
<u>IFS.DOMAIN.ANTIVIRUS.Host</u>	STRING	localhost
IFS.DOMAIN.ANTIVIRUS.Implementation	STRING	oracle.ifs.util.scanner.lcapScanner
IFS.DOMAIN.ANTIVIRUS.LastDefinitionUpdate	DATE	
<u>IFS.DOMAIN.ANTIVIRUS.MaxRepairAttempts</u>	INTEGER	10
<u>IFS.DOMAIN.ANTIVIRUS.Port</u>	INTEGER	7117
<u>IFS.DOMAIN.APPLICATION.ApplicationHost</u>	STRING	stbec05.us.oracle.com
IFS.DOMAIN.APPLICATION.ApplicationInitializerClassName	STRING	oracle.ifs.fdk.impl.FdkConfigurationImpl
<u>IFS.DOMAIN.APPLICATION.ApplicationMountPoint</u>	STRING	/content/app
<u>IFS.DOMAIN.APPLICATION.ApplicationPort</u>	INTEGER	80
<u>IFS.DOMAIN.APPLICATION.ApplicationUseHttps</u>	BOOLEAN	false

- Click the name of the property you want to change. Only underlined properties can be changed. See [Table 8–1](#) for a list of properties that can be edited.

You may need to move to the next page to find some properties, or you can use the **Search** field. For example, enter **workflow** and click **Go** (or press Enter) to see a list of workflow-related domain properties. You can use the question mark (?) and asterisk (*) wildcards.

- Make the changes to the property and click **OK**.
- Return to the Cluster Topology page and restart the Oracle Content DB domain. See "[Starting and Stopping the Oracle Content DB Domain](#)" on page 7-1 for information about how to do this.

Table 8–1 Oracle Content DB Domain Properties That Can Be Edited

Domain Property	Description
IFS.DOMAIN.ANTIVIRUS.Enabled	Determines whether Oracle Content DB is configured to work with the Symantec AntiVirus Scan Engine (SAVSE) to provide virus scanning and repair functionality. The default value is false.
IFS.DOMAIN.ANTIVIRUS.Host	The host name or IP address of the computer where the SAVSE server is running.
IFS.DOMAIN.ANTIVIRUS.MaxRepairAttempts	The number of times the Virus Scan Agent will try to repair a file.
IFS.DOMAIN.ANTIVIRUS.Port	The port number for the SAVSE listener.
IFS.DOMAIN.APPLICATION.ApplicationHost	The host name of the Oracle Content DB application (where a user connects; for example, content.oracle.com).
IFS.DOMAIN.APPLICATION.ApplicationMountPoint	The mount point for the Oracle Content DB application (usually /content/app). Typically, you do not change this value. If you do change this value, be aware that additional configuration is required.
IFS.DOMAIN.APPLICATION.ApplicationPort	The port number for the Oracle Content DB application (typically 7777 on UNIX or 80 on Windows).

Table 8–1 (Cont.) Oracle Content DB Domain Properties That Can Be Edited

Domain Property	Description
IFS.DOMAIN.APPLICATION.ApplicationUseHttps	Determines whether the Oracle Content DB application uses SSL. If SSL is enabled, users connect using HTTPS, rather than HTTP (for example, <code>https://content.oracle.com</code>).
IFS.DOMAIN.APPLICATION.WebDavMountPoint	The mount point for the content/DAV servlet (usually <code>/content/dav</code>). Typically, you do not change this value. If you do change this value, be aware that additional configuration is required.
IFS.DOMAIN.BFILE.AgingEnabled	Determines whether Oracle Content DB is configured for BFILE aging. The default value is false.
IFS.DOMAIN.BFILE.ArchivingEnabled	Determines whether Oracle Content DB is configured for BFILE archiving. The default value is false.
IFS.DOMAIN.BFILE.Enabled	If set to true, enables Oracle Content DB to store content as BFILES. The default value is false.
IFS.DOMAIN.CREDENTIALMANAGER.Idm	<p>If you are using an LDAP server for your user repository, and if you set up SSL for the connection between the LDAP server and Oracle Content DB, you will need to update the following two subproperties:</p> <ul style="list-style-type: none"> ■ IFS.DOMAIN.CREDENTIALMANAGER.Idm.LdapSslEnabled: Determines whether the connection between the LDAP server and Oracle Content DB uses SSL. ■ IFS.DOMAIN.CREDENTIALMANAGER.Idm.LdapPort: The port number for the LDAP server. <p>Do not change the values of the other subproperties.</p>
IFS.DOMAIN.CREDENTIALMANAGER.ServiceToServiceAuthenticationEnabled	This property is not used.
IFS.DOMAIN.DOCUMENT.DefinitionObjectExpirationPeriod	The default time, in seconds, before temporary DefinitionObject instances that were created without specifying an explicit expiration period are freed from the system.
IFS.DOMAIN.EMAIL.AdministratorAddress	The e-mail address of an administrator where Site quota warning notifications are sent. Error reports generated by the Oracle Content DB Web client are also sent to this address.
IFS.DOMAIN.EMAIL.Smtphost	The host name for the SMTP server used by Oracle Content DB.
IFS.DOMAIN.EMAIL.Smtport	The port number for the SMTP server used by Oracle Content DB.
IFS.DOMAIN.EMAIL.Smtptimeoutlength	How long Oracle Content DB waits for the SMTP server to return from sending e-mail.
IFS.DOMAIN.EMAIL.Smtuser	The name of a user for the SMTP server used by Oracle Content DB.
IFS.DOMAIN.LIBRARYOBJECT.SERVICECONFIGURATION.DefaultServiceConfiguration	The service configuration used by some internal Oracle Content DB processes to connect to the repository. The default is <code>SmallServiceConfiguration</code> .

Table 8–1 (Cont.) Oracle Content DB Domain Properties That Can Be Edited

Domain Property	Description
IFS.DOMAIN.MEDIA.CONTENTTRANSFER. ContentLimit	<p>The maximum size of a single file that can be uploaded to Oracle Content DB. The value you specify is interpreted as the maximum number of megabytes or characters allowed for a single upload of data. This limit does not apply to administrators.</p> <p>The value you specify is interpreted in different ways depending on file type:</p> <ul style="list-style-type: none"> ■ For binary files, this number is the maximum number of megabytes. For example, if you enter 5, the limit will be 5 megabytes for binary files. ■ For text files, such as ASCII or HTML, the number you specify is first converted into bytes, then applied as a maximum character limit, taking into account multibyte encoding. For example, if you enter 5, the limit will be 5 x 1,048,576 (or 5,242,380) characters for text files. <p>Set this property to 0 (the default) if you do not want to limit the size of single-file uploads. Users will then be able to upload any file whose size is within the last calculated available quota, as of the beginning of the upload.</p>
IFS.DOMAIN.PROTOCOLS.DAV.Cleartext AuthenticationEnabled	Determines whether WebDAV clients can connect to the server using cleartext authentication.
IFS.DOMAIN.PROTOCOLS.DAV.Null ResourceLockExpirationPeriod	The time period, in seconds, after which namespaces reserved over WebDAV as part of a Null Resource Lock are released. The default value is 3600.
IFS.DOMAIN.PROTOCOLS.DAV. PersistentCookieName	This property is not used.
IFS.DOMAIN.PROTOCOLS.DAV.UserAgents	A custom list of User-Agent headers for well-known WebDAV clients. This property is empty by default; do not provide values unless instructed by Oracle Support Services.
IFS.DOMAIN.RETENTION.CENTERA. Configuration	This property is not used.
IFS.DOMAIN.RETENTION.SNAPLOCK. Configuration	This property is not used.
IFS.DOMAIN.RETENTION.StorageDevice	This property is not used.
IFS.DOMAIN.SEARCH.AttemptContext SearchRewrite	Determines whether Oracle Content DB attempts to generate fast-response SQL for text searches. The default value is true.
IFS.DOMAIN.WORKFLOW.BPEL.Worklist URL	The URL of the Oracle BPEL Process Manager Worklist application.
IFS.DOMAIN.WS.Cleartext AuthenticationRequiresHttps	If set to true (recommended), does not allow cleartext authentication over Web services, unless the Oracle Content DB application has been configured for SSL.

Managing Node Configurations

The run-time behavior of a node is specified in its **node configuration** object. Each node has its own corresponding node configuration. If you want to make permanent changes to a node, such as changing servers or services, modify the node configuration for the node. If you want to make temporary (run-time) changes to a node, modify the node itself. Changes made at run time are lost when the node is restarted.

Nodes and node configurations do not have identical names. Nodes use the name of the corresponding OC4J instance (OC4J_Content). The display name for each node is the same as the OPMN process type.

Nodes and node configurations do not have identical names. Nodes take the name of the corresponding OC4J instance (OC4J_Content), while node configurations have names in the following format:

```
application_server_instance_name_HTTP_Node
```

The display name for each node is the same as the OC4J instance name (OC4J_Content), and is also used as the OPMN process type for the node. For example, you can start OC4J_Content using the following OPMN command:

```
opmnctl startproc process-type=OC4J_Content
```

For the OC4J_Content node to function properly, it must be set to **Active** in its node configuration object. See the following section for more information.

This section contains the following topics:

- [Modifying Node Configurations](#)
- [Adjusting Java Parameters for Nodes](#)

Modifying Node Configurations

You can make changes to existing node configurations, such as changing which protocol servers and agents run on a node.

Important: You must restart the node for your changes to take effect.

To modify a node configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Node Configurations table row, click the **Go to Task** icon.
4. On the Node Configurations page, click the name of the node configuration you want to modify.
5. Change the node configuration properties, as necessary. The node configuration properties are described in [Table 8–2](#).

Table 8–2 Node Configuration Properties

Property Name	Description and Usage Notes
Description	Description of the node configuration.
Access Control	The access level associated with the node configuration. Keep the default value.
Active	Whether the node configuration is enabled in the Oracle Content DB repository.

Table 8–2 (Cont.) Node Configuration Properties

Property Name	Description and Usage Notes
Maximum Sessions Per User	<p>The maximum number of user sessions allowed for a given user. The default value is 50. If this limit is reached, no new sessions for that user will be allowed on that node until a session ends, either through a logout or a session time out.</p> <p>To allow an unlimited number of sessions for each user, set the value to 0.</p> <p>Because this value is set for each node, different users may experience different session limits. For example, if you have multiple middle tiers, user sessions may be distributed in different ways, depending on load balancing.</p>
Maximum Concurrent Requests Per User	<p>The maximum number of outstanding requests allowed for a given user. An outstanding request is a request that the server is still processing, such as a search. The default value is 3.</p> <p>To allow an unlimited number of outstanding requests for each user, set the value to 0.</p> <p>Outstanding requests are also limited across all users, through the property <code>IFS.SERVICE.MaximumConcurrentSessions</code>. See Appendix D, "Service Configuration Properties" for more information.</p>
Transaction Timeout (seconds)	<p>The inactivity timeout period for a transaction that spans multiple requests. This setting usually applies to Web services clients, because they are the only clients that can have transactions that span multiple requests. If there is an outstanding transaction and there is no request on the corresponding session for the transaction timeout period, the transaction will time out. The default value is 120.</p> <p>Do not set this property to a value lower than 15.</p>
Transaction Timeout Check Interval (seconds)	<p>The interval between successive checks for transactions that need to be timed out. The default value is 30. Follow these guidelines for setting this value:</p> <ul style="list-style-type: none"> ■ This value must be smaller than the Transaction Timeout. ■ Setting a small value for this property may have a performance impact. ■ A large value for this parameter can significantly increase the actual transaction timeout period. For example, if the Transaction Timeout is 120 seconds, and the Transaction Timeout Check Interval is 30 seconds, then a given transaction will time out between 120 and 150 seconds of inactivity, depending on the timing of the transaction check.
Guest Session Pool Target Size	<p>The number of sessions kept in the guest session pool. If the number of sessions in the guest pool is equal to the Guest Session Pool Target Size up on the return of a session, the session will be disconnected, rather than returned to the pool. The default value is 10.</p> <p>If you are not allowing guest access, you can set this value to 0.</p>
Guest Session Pool Maximum Size	<p>The maximum number of guest sessions that can be in use at a given time. The default value is 100.</p> <p>If you are not allowing guest access, you can set this value to 0. This value must be greater than the Guest Session Pool Target Size (if the Guest Session Pool Target Size is greater than 0).</p>

Table 8–2 (Cont.) Node Configuration Properties

Property Name	Description and Usage Notes
System Session Pool Target Size	The number of sessions kept in the system session pool. If the number of sessions in the system pool is equal to the System Session Pool Target Size up on the return of a session, the session will be disconnected, rather than returned to the pool. The default value is 5. Do not set this property to a value lower than 5.
System Session Pool Maximum Size	The maximum number of system sessions that can be in use at a given time. The default value is 50. This value must be greater than the System Session Pool Target Size.

6. In the Services section, you can add, edit, or remove services for this node.
 - To add a service, click **Add**, specify information for the service, and click **OK**.
 - To change service properties, click the name of the service you want to modify. On the Edit Service page, change the appropriate information and click **OK**.
 - To remove a service, select it and click **Remove**. Each node must have at least one active service.
7. In the Servers section, you can add, edit, and remove protocol servers and agents for this node. You can also activate or deactivate servers for the node.
 - To add a server, click **Add**, specify information for the server, and click **OK**. To actively run a protocol server or agent on this node, make sure to select **Active** and **Initially Started**.
 - To change server properties, click the name of the server you want to modify. On the Edit Server page, change the appropriate information and click **OK**.

If you want a server to automatically start when the node is started, on the Edit Server page, select **Active** and **Initially Started**.
 - To remove a server, select it and click **Remove**.
 - To activate or deactivate multiple servers, click **Activate/Deactivate**. On the Activate/Deactivate Servers page, you can move servers between the Active Servers list and the Inactive Servers list. Then, click **OK**.
8. On the Edit Node page, click **OK** to save the changes. You must restart the node for your changes to take effect.

Adjusting Java Parameters for Nodes

You can specify command-line arguments for the Java VM for this node. See ["Calculating Xmx Settings"](#) on page 12-2 for more information about how to determine the correct Xmx setting.

To adjust the Java parameters and arguments for a node:

1. Connect to the Application Server Control.
2. From the Cluster Topology page, click the **OC4J_Content** instance for which you want to change Java parameters.
3. Click the **Administration** tab.

4. In the Server Properties table row, under the Properties heading, click **Go to Task**.
5. In the Command Line Options section, under the Start-parameters: Java Options heading, you can add additional options to the Options table. You can also select **Verbose:gc** to log all garbage collection activity, or enter the amount of memory for the Java heap in the **Initial heap size** field.
6. Click **Apply**.
7. Return to the Cluster Topology page, select **OC4J_Content**, and click **Restart**.

Managing Service Configurations

A **service configuration** holds the default values used when a service is started for an Oracle Content DB node. This section explains how to manage service configurations using the Application Server Control.

This section contains the following topics:

- [About Service Configurations](#)
- [Creating Service Configurations](#)
- [Modifying Service Configurations](#)
- [Deleting Service Configurations](#)

About Service Configurations

Each service configuration specifies values for service properties such as session parameters, the sizes of the data cache and database connection pools, and the default search timeout period. See [Appendix D, "Service Configuration Properties"](#) for a complete list of service configuration properties. Service configurations are uniquely named in a domain.

Whenever a new Oracle Content DB schema is created, three service configuration objects are generated:

- `SmallServiceConfiguration`
- `MediumServiceConfiguration`
- `LargeServiceConfiguration`

These objects are named to reflect the sizes of their data caches.

Use the Application Server Control to create or edit service configuration objects. The services read their service configuration properties only when they start. You must stop and restart the affected nodes for changes to take effect. The changes you make this way are applied each time you start a service and overwrite any changes you make on a service while it is running.

[Figure 8–2](#) shows the Service Configurations page.

Figure 8–2 Service Configurations Page**Service Configurations**

Page Refreshed Aug 29, 2006 6:16:03 PM CDT

A service configuration holds the default values used when a service is started for a node.

Search

|

Select	Name <small>△</small>	ACL	Modified
<input checked="" type="radio"/>	LargeServiceConfiguration	Private (system)	Tuesday, August 29, 2006 4:19:54 PM CDT
<input type="radio"/>	MediumServiceConfiguration	Private (system)	Tuesday, August 29, 2006 4:19:54 PM CDT
<input type="radio"/>	SmallServiceConfiguration	Private (system)	Tuesday, August 29, 2006 4:19:54 PM CDT

Creating Service Configurations

Use the Application Server Control to create service configurations.

To create a new service configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Service Configurations table row, click the **Go to Task** icon.
4. On the Service Configurations page, decide whether or not to create a new service configuration based on the properties of an existing service configuration.
 - Select a service configuration and click **Create Like** to base the new service configuration on an existing service configuration (highly recommended).
 - Click **Create** to create the service configuration without basing it on an existing configuration.

In both cases, the New Service Configuration page appears. If you clicked **Create Like**, the service configuration properties have been filled with those of the existing service.

[Figure 8–3](#) shows the New Service Configuration page.

Figure 8–3 New Service Configuration Page

Cancel OK

Click "OK" to create the object, or "Cancel" to cancel this operation.

General

* Name

Description

Access Control

Properties

Search Go

Remove Add Previous 1-25 of 75 Next 25

Select	Name	Type	Value
<input type="radio"/>	IFS_SERVICE.ACLCACHE.EmergencyTrigger	INTEGER	6000
<input type="radio"/>	IFS_SERVICE.ACLCACHE.NormalTrigger	INTEGER	5000
<input type="radio"/>	IFS_SERVICE.ACLCACHE.PurgeTarget	INTEGER	4000
<input type="radio"/>	IFS_SERVICE.ACLCACHE.Size	INTEGER	7500
<input type="radio"/>	IFS_SERVICE.ACLCACHE.UrgentTrigger	INTEGER	5500
<input type="radio"/>	IFS_SERVICE.CaseSensitiveAuthentication	BOOLEAN	true
<input type="radio"/>	IFS_SERVICE.CheckForOrphanSessionsPeriod	INTEGER	60
<input type="radio"/>	IFS_SERVICE.CONNECTIONPOOL_READONLY.MaximumSizeTimeout	INTEGER	10000

5. In the General section, enter a name for the new service configuration.
6. Enter a description of the service.
7. Keep the default value for **Access Control**.
8. Add, remove, or update the properties of the new service.
9. Click **OK**.

Modifying Service Configurations

You can use the Application Server Control to make changes to service configurations, such as changing the capacity of the Committed Data Cache or changing the number of maximum concurrent sessions. Changes take effect when the node is restarted.

To modify a service configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Service Configurations table row, click the **Go to Task** icon.
4. On the Service Configurations page, click the name of the service configuration you want to modify.
5. On the Edit page, update the information in the General section, as necessary:
 - **Description:** Enter a description of the service configuration.
 - **Access Control:** Keep the default value.
6. To add new properties for this service configuration, follow these steps:
 - a. In the Properties section, click **Add**.

- b. Provide a name for the new property.
 - c. Select a **Type** (such as string, integer, or Boolean). The page refreshes to display the appropriate **Value** field. For example, if you select **BOOLEAN**, a true or false list is displayed.
 - d. Enter or select a value for the property.
 - e. Click **OK**.
7. To edit a service configuration property, click the name of the property, update the value, and click **OK**.
 8. To remove a property from this service configuration, select the property, click **Remove**, then click **Yes**.
 9. Click **OK**.

Services only read their service configuration properties as they start. You must stop and restart the node on which the service is running before your changes will take effect. When the node restarts, the changes you made to the service configuration overwrite any run-time changes made on the service.

Deleting Service Configurations

You cannot delete a service configuration that is being used by a service. If the service configuration you want to delete is being used by a service, perform one of the following tasks:

- Change the service configuration being used by the service by modifying the node configuration
- Delete the service from the node configuration

You cannot delete the service if it is the only service defined in the node configuration. Each node must have at least one active service.

To delete a service configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Service Configurations table row, click the **Go to Task** icon.
4. On the Service Configurations page, select the service configuration you want to delete.
5. Click **Delete**.
6. On the Confirmation page, click **Yes**.

Managing Server Configurations

A **server configuration** holds the default values used when a server is started for an Oracle Content DB node. This section explains how to manage service configurations using the Application Server Control.

This section contains the following topics:

- [About Server Configurations](#)
- [Creating Server Configurations](#)

- [Modifying Server Configurations](#)
- [Deleting Server Configurations](#)

About Server Configurations

Server configurations specify their server types as Java classnames. In addition to the server type, each server configuration specifies values for parameters relevant to that type. See [Appendix E, "Server Configuration Properties"](#) for more information.

Most of the server configuration information is used by the server itself. Only the server Java class entry is used by the node to instantiate a new server.

When Oracle Content DB is installed, server configurations are automatically created for each protocol server and agent. You can edit these configurations, or create additional server configurations using the Application Server Control. Any changes you make will appear the next time the node is restarted, or when the server is unloaded and then loaded again.

Server configuration objects are of two types:

- **Abstract:** Used to set base values for the properties, which can then be inherited by some other configuration. You cannot start a server from an abstract server configuration.
- **Non-abstract:** Can be used to start servers.

When you create a new server configuration, you can let it inherit the properties from one or more server configurations. You can use the same values as inherited, or use different values.

Inheritance operations are accessed from the New Server Configuration page, shown in [Figure 8-4](#). See "[Creating Server Configurations](#)" on page 8-13 for more information on creating new server configurations.

Figure 8–4 Inheritance Operations on the New Server Configuration Page

Inherited Server Configurations

[Return to Top](#)

A server configuration can inherit properties from other server configurations. The order in which the inherited server configurations are listed is significant. Those listed first take precedence.

Available Configurations

- BackgroundRequestAgentConfiguration
- CleanupAgentConfiguration
- ContentAgentConfiguration
- ContentGarbageCollectionAgentConfiguration
- DanglingObjectAVCleanupAgentConfiguration
- EcmHttpServerConfiguration
- EventExchangerAgentConfiguration
- ExpirationAgentConfiguration
- FolderIndexAgentConfiguration
- FolderIndexAnalyzerAgentConfiguration

Description

Move

Move All

Remove

Remove All

Inherited Configurations

Description

Properties

[Return to Top](#)

Inherited and locally defined properties are shown for the server configuration. If you change the inherited server configurations, click "Update Inherited Properties" to revise the inherited properties. Click "Add", "Edit", or "Remove" to manage locally defined properties.

Search

|

Select	Name	Inherited	Type	Value
<input checked="" type="radio"/>	ECM_AGENT_BACKGROUNDREQUESTAGENT.EventBatchSize		INTEGER	5000
<input type="radio"/>	IFS_SERVER_Class		STRING	oracle.ifs.ecm.agents.BackgroundRequestAgent
<input type="radio"/>	IFS_SERVER_SESSION.User		STRING	system
<input type="radio"/>	IFS_SERVER_TIMER.ActivationPeriod		STRING	20m
<input type="radio"/>	IFS_SERVER_TIMER.InitialDelay		STRING	15m

Changing Values of Inherited Properties

To change the value of an inherited property, create a new property in the inherited server configuration that is identical in name to the one in the parent server configuration, but has values that override those in the parent server configuration.

Viewing Inherited Properties

View the inherited properties to determine whether the property in the current server configuration object is local to this object or taken from a parent server configuration object. You can also differentiate between inherited server configuration objects and those that are local to the server configuration.

Creating Server Configurations

Use the Application Server Control to create new server configurations.

To create a new server configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See ["Accessing the Oracle Content DB Home Page"](#) on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Server Configurations table row, click the **Go to Task** icon.
4. On the Server Configurations page, decide whether or not to create a new server configuration based on the properties of an existing server.
 - Select a server configuration and click **Create Like** to base the new server configuration on an existing configuration.

- Click **Create** to create the server configuration without basing it on an existing configuration.

In both cases, the New Server Configuration page appears. If you clicked **Create Like**, the server configuration properties have been filled with those of the existing server.

5. On the New Server Configuration page, in the General section, enter a name for the new server configuration.
6. Enter a description of the server.
7. Keep the default value for **Access Control**.
8. Select **Abstract** to prevent this server from being instantiated. An abstract server configuration is used to set base values for properties, which can then be inherited by another server configuration. You cannot start a server from an abstract server configuration.
9. In the Inherited Server Configurations section, select the existing configurations from which the new configuration will inherit properties. Select configurations from the **Available Configurations** list and move them to the **Selected Configurations** list.
10. If you change the list of inherited server configurations, click **Update Inherited Properties** in the Properties section to display the properties of the inherited server configurations.

The order of the items in the Inherited Configurations list determines which configuration takes precedence.

11. To edit server configuration properties, follow these steps:
 - a. In the Properties section, click the name of the property you want to change.
 - b. Update the value of the property.
 - c. Click **OK**.

Inherited server configuration properties cannot be edited. Inherited properties display an icon in the Inherited column, and their names are not rendered as links. To change the value of these properties, add a new property that is identical in name to the inherited property, but with a value that overrides the value of the inherited property.

12. To add new server configuration properties, follow these steps:
 - a. Click **Add** in the Properties section.
 - b. Enter a name for the new property. If you are adding a property to override an inherited property, make sure the name matches the inherited property.
 - c. Select a **Type** (such as string, integer, or Boolean). The page refreshes to display the appropriate **Value** field. For example, if you select **BOOLEAN**, a true or false list is displayed.
 - d. Enter or select a value for the property.
 - e. Click **OK**. If you added a property to override an inherited property, the property name changes to a link, and the Inherited icon no longer appears.
13. To remove server configuration properties, select a property and click **Remove**.
14. After you complete the server configuration, click **OK**.

Modifying Server Configurations

You can use the Application Server Control to make important changes to server configurations, such as changing which configurations to inherit and editing, adding, or removing server configuration properties. Changes take effect when the server is reloaded or when the node is restarted.

See [Appendix E, "Server Configuration Properties"](#) for more information about specific server configuration parameters.

To modify an existing server configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Server Configurations table row, click the **Go to Task** icon.
4. On the Server Configurations page, click the name of the server configuration you want to modify.
5. On the Edit page, update the information in the General section as necessary:
 - **Description:** Enter a description of the server configuration.
 - **Access Control:** Keep the default value.
 - **Abstract:** Choose whether to make the server configuration abstract. An abstract server configuration is used to set base values for properties, which can then be inherited by some other server configuration. You cannot start a server from an abstract server configuration.
6. In the Inherited Server Configurations section, use the arrow buttons to add or remove server configurations from which this server configuration will inherit properties.
7. If you change the list of inherited server configurations, click **Update Inherited Properties** in the Properties section to display the properties of the inherited server configurations.

The order of the items in the Inherited Configurations list determines which configuration takes precedence.

8. To edit server configuration properties, follow these steps:
 - a. In the Properties section, click the name of the property you want to change.
 - b. Update the value of the property.
 - c. Click **OK**.

Inherited server configuration properties cannot be edited. Inherited properties display an icon in the Inherited column, and their names are not rendered as links. To change the value of these properties, add a new property that is identical in name to the inherited property, but with a value that overrides the value of the inherited property.

9. To add new server configuration properties, follow these steps:
 - a. Click **Add** in the Properties section.
 - b. Enter a name for the new property. If you are adding a property to override an inherited property, make sure the name matches the inherited property.

- c. Select a **Type** (such as string, integer, or Boolean). The page refreshes to display the appropriate **Value** field. For example, if you select **BOOLEAN**, a true or false list is displayed.
 - d. Enter or select a value for the property.
 - e. Click **OK**. If you added a property to override an inherited property, the property name changes to a link, and the Inherited icon no longer appears.
10. To remove server configuration properties, select a property and click **Remove**.
 11. After you complete the server configuration, click **OK**.

Servers only read their server configuration properties when they are reloaded, or when the node is restarted. You must reload the server before your changes will take effect. See "[Reloading Servers](#)" on page 7-15 for more information. These server configuration changes overwrite changes you make on a server while it is running.

Deleting Server Configurations

You cannot delete a server configuration that is being used by a server. If the server configuration you want to delete is being used by a server, first edit the node configuration to remove the server, then delete the server configuration. Alternatively, you can change the server configuration being used by the server.

To delete a server configuration:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Server Configurations table row, click the **Go to Task** icon.
4. On the Server Configurations page, select the server configuration you want to delete.
5. Click **Delete**.
6. On the Confirmation page, click **Yes**.

Monitoring Domain, Node, Service, and Server Performance

Use the Application Server Control to monitor Oracle Content DB domain, node, service, and server performance. You can use this information to get an overall picture of the performance of the domain, or to determine whether the configuration of the domain needs to be changed.

This chapter provides information about the following topics:

- [Monitoring Node Performance](#)
- [Monitoring Service Performance](#)
- [Monitoring Server Performance](#)
- [Viewing Logs](#)

Monitoring Node Performance

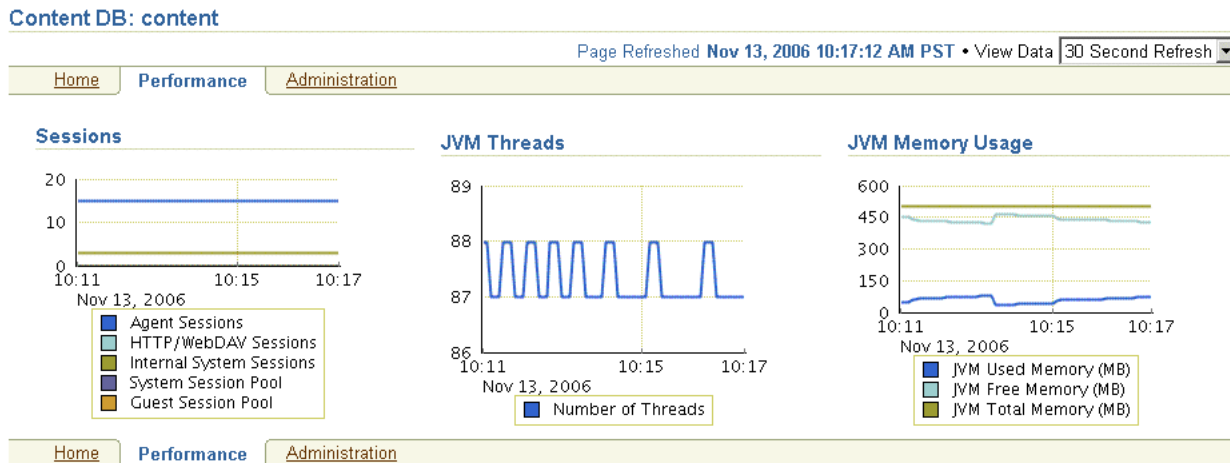
You can use the Application Server Control to view performance information for each Oracle Content DB node (OC4J_Content instance), including number of sessions, JVM threads, and JVM total, used, and free memory.

To view node performance information:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Performance** tab.

[Figure 9-1](#) shows the Performance tab of the Content DB Home page.

Figure 9–1 Performance Tab of Content DB Home Page



- The following charts are displayed:
 - The Sessions chart provides information about the number of **sessions** supported by this node. These sessions are Library sessions, not user sessions.
 - The JVM Threads chart shows the number of JVM threads in the node.
 - The JVM Memory Usage chart shows the amount of memory being used by the node.
- To refresh the information, refresh your browser, or choose one of the following settings for **View Data** in the upper right portion of the page:
 - Manual Refresh (requires that you refresh your browser in order to refresh the information)
 - 30 Second Refresh
 - 1 Minute Refresh
 - 5 Minute Refresh

For some browser configurations, the data is refreshed automatically, even if you select **Manual Refresh**.

Monitoring Service Performance

You can view real-time statistics for the Committed Data Cache, the Read-Only Connection Pool, and the Writable Connection Pool for each service. You can also reset the statistics.

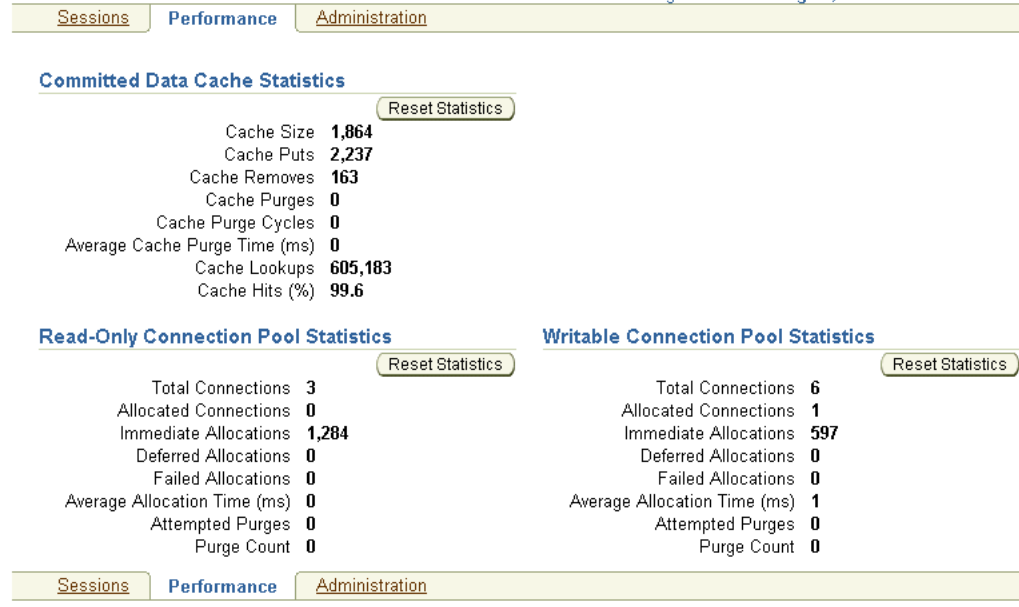
- Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
- Click the name of the service for which you want to see statistics (for example, **IfsDefaultService**).
- Click the **Performance** tab.

[Figure 9–2](#) shows the Performance tab of the Service page.

Figure 9–2 Performance Tab of Service Page

Service: lfsDefaultService

Page Refreshed Aug 29, 2006 6:21:43 PM CDT



4. The Committed Data Cache Statistics section displays the following:
 - Cache Size
 - Cache Puts
 - Cache Removes
 - Cache Purges
 - Cache Purge Cycles
 - Average Cache Purge Time (ms)
 - Cache Lookups
 - Cache Hits (%)
5. The Read-Only Connection Pool Statistics and Writable Connection Pool Statistics sections display the following:
 - Total Connections
 - Allocated Connections
 - Immediate Allocations
 - Deferred Allocations
 - Failed Allocations
 - Average Allocation Time (ms)
 - Attempted Purges
 - Purge Count
6. Click **Reset Statistics** in the Committed Data Cache, Read-Only Connection Pool, or Writable Connection Pool areas to reset cache or connection pool statistics.

Logging Service Performance Information

The Statistics Agent captures the statistics for the Committed Data Cache, as well as the Read-Only and Writeable Connection Pools, and writes them to the `application.log` file. You can also configure this agent to write statistics to a document stored in the Oracle Content DB repository.

See "[Viewing Logs](#)" on page 9-4 for information about the application log. See "[Statistics Agent](#)" on page E-12 for information about the Statistics Agent.

Monitoring Server Performance

You can monitor server performance by viewing Dynamic Monitoring Service (DMS) metrics that were defined for some servers. DMS metrics are a special type of performance metric that can be defined in Oracle Application Server. DMS metrics for Oracle Content DB include:

- WebDAV Servers
- Servers

Some DMS metric information can be viewed on the Content DB Home page, and on the Server page for some servers. For example, the Servers section of the Node page shows the Last Start Time and Last Stop Time for each server, while the Oracle Content DB HTTP Server (EcmHttpServer) page displays Requests Completed, Average Request Processing Time (seconds), Downloaded Content Size (MB), and Uploaded Content Size (MB).

DMS metrics can also be viewed using the `dmstool` utility and AggreSpy. For more information about DMS metrics and how to view them, see *Oracle Application Server Performance Guide*.

Viewing Logs

The following sections provide a list of Oracle Content DB logs, and information about how to view logs in the Application Server Control. This section contains the following topics:

- [Oracle Content DB Logs](#)
- [Viewing Oracle Content DB Logs from the Application Server Control](#)
- [Changing the Log Level for Oracle Content DB Processes](#)

Oracle Content DB Logs

The application log for OC4J_Content records information for nodes. This log is useful for troubleshooting the Oracle Content DB application and the WebDAV server. All errors are logged with stack traces. By default, application logs are located in:

```
ORACLE_HOME/j2ee/OC4J_Content/application-deployments/Content/OC4J_Content_
default_island_1/application.log
```

```
ORACLE_HOME/opmn/logs/Content~OC4J_Content~default_island~1
```

You can also view `ContentConfig.log`, the log for the Oracle Content DB Configuration Assistant that ran during Oracle Content DB installation. This log is located in:

```
ORACLE_HOME/content/log/ContentConfig.log
```

The `changehostname` utility generates a log in the same location:

```
ORACLE_HOME/content/log/changehostname.log
```

Viewing Oracle Content DB Logs from the Application Server Control

You can view a variety of logs from the Application Server Control. This feature lets you view the logs without having to remember the individual log location.

To view log, click the **Logs** link in the upper-right corner of any Application Server Control page.

- The Log Files page provides a complete list of logs. Expand an entry in the tree to view logs relevant to that entry. For example:
 - To see the application log for OC4J_Content, expand **OC4J**, then expand **OC4J_Content**, then expand **Application content**.
 - Expand **Enterprise Manager** to see Application Server Control logs.
 - Expand **Content DB**, then expand **Configuration Assistant** to view `ContentConfig.log`.
- You can also use the Search function to locate logs. To do this, select the items in the table that correspond to the logs you want to see and click **Search**.

On the Search Logs page, be sure to select **Unknown** in the Message Types section. Oracle Content DB logs are not categorized by the other message types listed (Internal Error, Warning, Trace, Error, and Notification).

Click the name of a log to see the log data. By default, the last 500 lines in the log appear in the log viewer. You can view up to 2000 lines. To download the contents of the entire log, click the log name at the top of the screen. If the log is large, the download may take several minutes.

Changing the Log Level for Oracle Content DB Processes

You can use the Application Server Control to change the log level for certain Oracle Content DB processes, using the System MBean Browser.

To change the log level of Oracle Content DB processes:

1. Access the Application Server Control.
2. On the Cluster Topology page, in the Members table, click the **OC4J_Content** instance that is running the processes for which you want to change the log level.
3. Click the **Administration** tab.
4. In the System MBean Browser table row, under the JMX heading, click the **Go to Task** icon.
5. In the System MBean Browser tree view, access the J2EELogging option, as follows:
 - a. Under the **OC4J** node in the tree, expand **J2EEServer**.
 - b. Under the **J2EEServer** node, expand the **standalone** node.
 - c. Expand **J2EELogging**.
 - d. Click the **oracle** link.
6. On the MBean: J2EELogging:oracle page, click the **Operations** tab.
7. Click **setLoggerLevel**.

8. In the Parameters table, in the **loggerName** table row, enter the name of the logger (Java package) for which you want to set the log level. [Table 9-1](#) shows the loggers that correspond to some Oracle Content DB functional areas.

Table 9-1 Logger Names for Some Oracle Content DB Functional Areas

Functional Area	Logger Names
All	oracle.ifs Note: Because oracle.ifs is the root logger for Oracle Content DB, changing the log level for oracle.ifs can greatly increase the output in <code>application.log</code> .
Repository/Oracle CM SDK layer	oracle.ifs.beans oracle.ifs.common oracle.ifs.search oracle.ifs.server
Oracle Content DB business logic layer	oracle.ifs.ecm
FDK/Client Service layer	oracle.ifs.fdk
Oracle Content DB Web application	oracle.ifs.web
WebDAV server	oracle.ifs.protocols.dav
All agents	oracle.ifs.ecm.agents oracle.ifs.management.servers

There are many other Oracle Content DB loggers, in addition to the ones listed in [Table 9-1](#). If you are not sure which loggers to enter, first set the log level for **oracle.ifs** to **FINEST**. Then, view the log output in `application.log` and note the loggers (package names) in which you are interested. Once you know the loggers for which you want to adjust logging, return to the Application Server Control and set the log level for those loggers. Be sure to revert the log level for `oracle.ifs` after you have set logging for individual loggers, to reduce the output in `application.log`.

9. In the Parameters table, in the **levelName** table row, enter the level of logging you want for the selected logger. Oracle Content DB supports the following levels:
 - **SEVERE:** Log only nonrecoverable problems
 - **WARNING:** Log only recoverable problems
 - **INFO:** General level of log information
 - **FINE:** Level for debugging or tracing key operations
 - **FINER:** Level for debugging or tracing the entry and exit of methods
 - **FINEST:** Level for debugging or tracing within a method

The **CONFIG** level is not supported for Oracle Content DB logging.

10. Click **Invoke Operation**.

Managing Oracle Content DB Formats

Oracle Content DB associates a format (also known as a MIME type) with each document. You can add, modify, and delete formats using the Application Server Control.

This chapter provides information about the following topics:

- [About Formats](#)
- [Adding Formats](#)
- [Modifying Formats](#)
- [Deleting Formats](#)
- [Default Formats](#)

About Formats

The **format** of a document indicates the file type (for example, .doc or .zip). Oracle Content DB needs to know the format of documents to determine how to index their content.

A format contains the following information:

- **MIME type:** Specifies the type of content stored in Oracle Content DB, such as `text/plain` or `text/html`.
- **Extension type:** Specifies the default extension for files that use this format, such as `.fm` or `.jar`.
- **Binary setting:** Determines whether files that use this format are of binary type.
- **Index setting:** Determines whether files that use this format need to be indexed.
- **Omitted From Antivirus Scan:** Determines whether files that use this format need to be omitted from antivirus scans.

Indexing a format type is the basis of content searching in Oracle Content DB. If a format is not indexed, content searches will fail. Content searches can also fail when formats are indexed incorrectly.

See Appendix B, "Oracle Text Supported Document Formats" in *Oracle Text Reference* for information about which formats can be indexed by Oracle Text.

Adding Formats

You can add more formats to Oracle Content DB for special types of content. See "[Default Formats](#)" on page 10-4 for a list of default formats.

To add a format:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Formats table row, click the **Go to Task** icon.
4. On the Formats page, click **New Format**. The New Format page appears.

[Figure 10-1](#) shows the New Format page.

Figure 10-1 New Format Page

5. Enter the following information:
 - **Name:** Provide a name for the format (for example, FrameMaker or Jar).
 - **MIME Type:** Specify the type of content stored in Oracle Content DB, such as `text/plain` or `text/html`. Click the Flashlight icon to select from a list of MIME types.
 - **Extension:** Specify the default extension for files that use this format, such as `.fm` or `.jar`. Click the Flashlight icon to select from a list of file extensions.
 The names of files uploaded from UNIX or Linux clients are case-sensitive. If the case of the extension for your format (for example, `.ZIP`) does not match the case of the extension for the file uploaded from UNIX or Linux (for example, `.zip`), the uploaded file will be classified as the Unknown format, and the content will not be indexed. Files that are not indexed do not show up in content search results.
 - **Binary:** Specify whether files that use this format are of binary type.
 - **Omitted From Antivirus Scan:** Specify whether files that use this format need to be omitted from antivirus scans.
 - **Indexed:** Specify whether files that use this format need to be indexed.
6. Click **OK**.

Modifying Formats

You can modify formats using the Application Server Control. The Unknown format is a required system format and cannot be modified.

To modify a format:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Formats table row, click the **Go to Task** icon.
4. On the Formats page, click the name of the format you want to modify.
5. On the Edit Format page, you can change the following information:
 - **MIME Type:** Specify the type of content stored in Oracle Content DB, such as `text/plain` or `text/html`. Click the Flashlight icon to select from a list of MIME types.
 - **Extension:** Specify the default extension for files that use this format, such as `.fm` or `.jar`. Click the Flashlight icon to select from a list of file extensions.
The names of files uploaded from UNIX or Linux clients are case-sensitive. If the case of the extension for your format (for example, `.ZIP`) does not match the case of the extension for the file uploaded from UNIX or Linux (for example, `.zip`), the uploaded file will be classified as the Unknown format, and the content will not be indexed. Files that are not indexed do not show up in content search results.
 - **Binary:** Specify whether files that use this format are of binary type.
 - **Omitted From Antivirus Scan:** Specify whether files that use this format need to be omitted from antivirus scans.
 - **Indexed:** Specify whether files that use this format need to be indexed. Changing this setting only affects new documents that are uploaded to Oracle Content DB; the index setting for existing documents that use this format will not be changed. To force indexing of existing documents, upload the documents again after changing this setting.
6. Click **OK**.

Some formats must be indexed. For these formats, the index setting cannot be changed.

Deleting Formats

You can delete formats using the Application Server Control. The Unknown format is a required system format and cannot be deleted.

To delete a format:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Formats table row, click the **Go to Task** icon.
4. On the Formats page, select the format you want to delete.
5. Click **Delete**.
6. On the Warning page, click **Yes**.

Default Formats

Table 10–1 provides a list of default formats.

Table 10–1 Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting? ¹
Advanced Stream Redirector File	asx	No	Yes
Advanced Streaming Format	asf	No	Yes
Apple Quicktime	mov	Yes	No
Apple Quicktime (qt)	qt	Yes	No
Audio Interchange File (aif)	aif	Yes	No
Audio Interchange File (aifc)	aifc	Yes	No
Audio Interchange File (aiff)	aiff	Yes	No
Basic audio	au	Yes	No
Bitmap image	bmp	Yes	No
c file	c	Yes	Yes
C Header	h	Yes	Yes
C++ Header (h++)	h++	Yes	Yes
C++ Header (hh)	hh	Yes	Yes
C++ Header (hpp)	hpp	Yes	Yes
C++ Header (hxx)	hxx	Yes	Yes
C++ Source Code (C++)	c++	Yes	Yes
C++ Source Code (cc)	cc	Yes	Yes
C++ Source Code (cpp)	cpp	Yes	Yes
CC++ Source Code (cxx)	cxx	Yes	Yes
Comma-Separated Values	csv	Yes	Yes
Compiled WML Document	wmlc	No	Yes
Compiled WML Script	wmlsc	No	Yes
Compressed File	taz	No	Yes
Corel Photo-Paint Image	cpt	No	Yes
Corel Vector Graphic Drawing	cdr	No	Yes
Corel Vector Pattern	pat	No	Yes
CorelDraw Template	cdt	No	Yes
Debian Linux Package	deb	No	Yes
Difference File	diff	Yes	Yes
Email Message	eml	Yes	No
Encapsulated PostScript	eps	Yes	Yes
Extensible HyperText Markup Language File	xhtml	Yes	Yes
Extensible Markup Language	xml	Yes	Yes

Table 10–1 (Cont.) Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting?¹
FileMaker Pro Spreadsheet	fm	Yes	Yes
FrameMaker Book	book	Yes	Yes
FrameMaker FBDOC	fbdoc	Yes	Yes
FrameMaker FRAME	frame	Yes	Yes
FrameMaker FRM	frm	Yes	Yes
FrameMaker MAKER	maker	Yes	Yes
GIF	gif	Yes	No
GNU tar Compressed File Archive (GNU Tape Archive)	gtar	No	Yes
GZIP	gz	No	Yes
HTML	htm	Yes	Yes
HTML unix	html	Yes	No
Hypertext Cascading Style Sheet	css	Yes	Yes
JAR	jar	No	Yes
Java Bytecode	class	No	Yes
java file	java	Yes	Yes
Java Serialized Object File	ser	No	Yes
JavaScript Source Code	js	Yes	Yes
JNLP	jnlp	No	Yes
JPEG	jpg	Yes	No
JPEG (jpe)	jpe	Yes	No
JPEG (jpeg)	jpeg	Yes	No
JSP	jsp	Yes	Yes
Lotus 123 Spreadsheet	wk	Yes	Yes
Macintosh Sound Resource	snd	No	Yes
Macromedia Director Movie	dir	No	Yes
Macromedia Director Protected Movie File	dxr	No	Yes
Macromedia Flash Format File	swf	No	Yes
Macromedia Flash Format File - swfl	swfl	No	Yes
MHTML Document mhtm	mht	Yes	Yes
MHTML Document mhtml	mhtml	Yes	Yes
Microsoft AVI	avi	Yes	No
Microsoft PowerPoint	ppt	Yes	Yes
Microsoft Powerpoint (pot)	pot	Yes	Yes
Microsoft Powerpoint Show	pps	Yes	Yes
Microsoft Wave Audio	wav	Yes	No

Table 10–1 (Cont.) Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting?¹
MIDI	mid	No	Yes
Money Data File	mny	No	Yes
MP3 Playlist File	m3u	No	Yes
MPEG	mpg	No	Yes
MPEG (mpe)	mpe	No	Yes
MPEG (mpeg)	mpeg	No	Yes
MPEG - mpega	mpega	Yes	No
MPEG Layer 2	mp2	Yes	No
MPEG Layer 3 Audio	mp3	Yes	No
MPEG Layer 3 Audio Stream	mpga	Yes	No
MS Access	mdb	Yes	Yes
MS DOS Batch Processing	bat	Yes	Yes
MS Excel	xls	Yes	Yes
MS Excel (xlb)	xlb	Yes	Yes
MS Executable File	exe	No	Yes
MS Windows Dynamic Link Library	dll	No	Yes
MS Word	doc	Yes	Yes
MS Word (dot)	dot	Yes	Yes
MS Works	msw	Yes	Yes
Object File	o	No	Yes
OpenOffice.org Drawing	sda	No	Yes
OpenOffice.org Presentation	sdd	Yes	Yes
Outlook Express News File	nws	No	Yes
PCX	pcx	No	Yes
PDF	pdf	Yes	Yes
PERL Program File	pl	Yes	Yes
Portable (Public) Network Graphic	png	No	Yes
portable pixmap	ppm	No	Yes
Postscript	ps	No	Yes
postscript-ai	ai	No	Yes
Project File	mpp	Yes	Yes
Real Audio (ra)	ra	Yes	No
Real Audio (ram)	ram	Yes	Yes
Real Media (rm)	rm	Yes	No
Real Video	rv	Yes	No
RedHat Package Manager	rpm	No	Yes

Table 10–1 (Cont.) Default System Formats

Format Name	Extension	Indexed by Default?	Can Change Index Setting?¹
RichText	rtf	Yes	Yes
RichText (rtx)	rtx	Yes	Yes
Schedule/Schedule+ Data	scd	No	Yes
SGI Video	movie	No	Yes
Shell Script	sh	Yes	Yes
Shockwave Movie	dcr	No	Yes
Sourcecode	src	Yes	Yes
Standard General Markup Language	sgml	Yes	Yes
Tab Separated Values File	tsv	Yes	Yes
Tar	tar	No	Yes
Tcl (Tool Command Language) Language Script	tcl	Yes	Yes
Text	txt	Yes	Yes
Text Document (text)	text	Yes	Yes
TIFF	tif	Yes	No
TIFF (tiff)	tiff	Yes	No
Tk Language Script	tk	Yes	Yes
UNIX Compressed Archive File	z	No	Yes
UNIX csh Shell Script	csh	Yes	Yes
UNIX Tar File Gzipped	tgz	No	Yes
Unknown	(N/A)	No	No
Unknown Binary	bin	No	Yes
URL Reference	url	No	Yes
vCalendar File	vcs	No	Yes
vCard File	vcf	Yes	Yes
Visio Drawing	vsd	Yes	Yes
VRML	vrml	No	Yes
Windows Help File	hlp	No	Yes
Windows Icon	ico	No	Yes
Wireless Markup Language File	wml	Yes	Yes
WML Script	wmls	Yes	Yes
Word Perfect	wpd	Yes	Yes
Wordperfect 5.1 Document	wp5	Yes	Yes
XFIG Graphic File	fig	No	Yes
xpixmap	xpm	No	Yes
xpixmap pm	pm	No	Yes
Zip	zip	No	Yes

¹ Some formats must be indexed. For these formats, the index setting cannot be changed.

Managing the Oracle Content DB Site

The Oracle Content DB [Site](#) is an organizational entity that is used to manage settings for all Oracle Content DB users. The Site has an allocated quota that specifies the amount of content (in MB, GB, or TB) that can be stored in the Site.

You can use the Application Server Control to modify settings for the Site. You can also grant the Security Administrator role to a particular Site user.

This chapter provides information about the following topics:

- [About the Oracle Content DB Site](#)
- [Modifying Site Settings](#)
- [Granting the Security Administrator Role](#)

About the Oracle Content DB Site

There are a designated set of application administrators for the Site who can manage quota, specify Site settings, and perform other tasks. The application administration roles include the User Administrator, Content Administrator, and Quota Administrator. For more information about the application administrator roles and tasks, see *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite*.

The Site has an allocated quota that specifies the amount of content (in MB, GB, or TB) that can be stored in the Site. When the quota consumed by the Site reaches 95 percent of the allocated quota, an e-mail notification is sent to the administrator e-mail address, and to any users of the Site with the Quota Administrator role. The administrator e-mail address is specified in the `IFS.DOMAIN.EMAIL.AdministratorAddress` domain property. See "[Changing Domain Properties](#)" on page 8-1 for information about how to specify this administrator e-mail address.

Quota warning e-mail notifications are only sent if you have configured an SMTP server for use with Oracle Content DB. see "[Enabling Oracle Content DB Error Reporting and Site Quota Warning Notifications](#)" on page 4-1 for more information.

Quota warning e-mail notifications are issued by the Cleanup Agent. You can change the properties of this agent to adjust the warning threshold, or to specify whether files in the [Archive](#) count against Site quota. See "[Cleanup Agent](#)" on page E-3 for more information about these properties.

Modifying Site Settings

You can change settings for the Site, including changing the Site name, updating Site quota, and changing the location of Personal Libraries for new users.

To modify Site settings:

1. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
2. On the Content DB Home page, click the **Administration** tab.
3. In the Site Management table row, click the **Go to Task** icon. The Site Management page appears.

Figure 11-1 shows the Site Management page.

Figure 11-1 Site Management Page

Site Management Revert Apply

General

* Name
 Realm **dc=us,dc=oracle,dc=com**
 * Allocated Quota MB
 Used Quota **1 MB**
 Active Users **2**
 Enabled

Personal Libraries

The following properties allow you to change the location of all new users' Personal Libraries. The location of existing users' Personal Libraries will not be affected.

* Locator Class Name
 * Root Path

4. If necessary, provide a new name for the Site. Since the Site name is used as the top folder name for the Site, any bookmarks to existing URLs will break. Also, in Oracle Drive, any paths designated for scheduled backups will need to be changed.

You cannot use the following characters in the Site name: backslash (\), slash (/), colon (:), asterisk (*), question mark (?), quotation mark ("), left angle bracket (<), right angle bracket (>), and vertical bar (|). Keep Site names short to avoid long path names, and avoid using spaces because these characters will be replaced by %20 in URLs, making the URL long and hard to read.

5. Specify the amount of quota you want to allocate in the **Allocated Quota** field, then specify whether you want to allocate the quota in Megabytes (MB), Gigabytes (GB), or Terabytes (TB) by selecting from the list. The quota you allocate must be larger than the quota that has already been used by the Site.
6. In the Personal Libraries section, you have the option of changing the location of the Personal Libraries for new users. Using this option requires custom Java code; contact your Oracle Support Services representative for more information. To change the location of the Personal Libraries for new users, provide the following two parameters:
 - **Locator Class Name:** Specify the name of the custom class you created for the new Personal Library location.
 - **Root Path:** Specify the new root path for the Personal Libraries.

Only the Personal Libraries for new users will use the new path. Personal Libraries for existing users will remain in the old location.

7. Click **Apply**.

Granting the Security Administrator Role

If all existing Site users with the Security Administrator role are deleted or deprovisioned, you can use the Application Server Control to grant the Security Administrator role to a Site user.

For more information about the Security Administrator role, see *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite*.

To grant the Security Administrator role to a Site user:

1. Ensure that the user to whom you want to grant the Security Administrator role has been created, and that this user has logged in to Oracle Content DB at least once.
2. Connect to the Application Server Control and go to the Content DB Home page. See "[Accessing the Oracle Content DB Home Page](#)" on page 1-3 for information about how to do this.
3. On the Content DB Home page, click the **Administration** tab.
4. In the Site Security table row, click the **Go to Task** icon.
5. On the Grant Security Role page, enter the name of the user to whom you want to grant the Security Administrator role. This user must be an existing Oracle Content DB user who has already been provisioned. In other words, this user must have logged in to Oracle Content DB at least once.
6. Click **Apply**.

Oracle Content DB Maintenance and Tuning

This chapter provides information about ongoing system maintenance, performance tuning, and recovery. As with any production system, your implementation of Oracle Content DB needs to include a basic disaster recovery plan.

This chapter provides information about the following topics:

- [Backup and Recovery](#)
- [Service Configurations and Java Memory Sizing](#)
- [Performance Tuning](#)
- [Analyzing Performance Problems](#)

Backup and Recovery

Always back up the system before upgrading, migrating new data, or making other major changes:

- **Oracle Database tier:** See *Oracle Database Backup and Recovery User's Guide* for complete information about backing up Oracle Database. In addition, note the following:
 - In addition to the Oracle Content DB schema, there is a special schema that ensures secure connectivity to other systems, called `CONTENT$CM`. When you back up your system, make sure to include this schema.
 - Make sure to back up the Oracle Workflow schema, `OWF_MGR`.
 - If you use BFILES, make sure to back them up also.
- **Oracle Content DB middle tier:** There is no backup and recovery tool for the middle tier. To back up the middle tier, make a complete copy of the Oracle home. Also, make a copy of the `oraInventory` directory on the middle-tier computer.

Service Configurations and Java Memory Sizing

In Oracle Content DB, the default service configurations specify the maximum number of Library **sessions** that can connect to the service. Restricting the number of Library sessions reduces the likelihood of getting out of memory errors in the `OC4J_Content.default_island.1` or in the `application.log` files.

When the maximum number of Library sessions is restricted, you may see the following errors:

- Oracle Content DB Web client: "The maximum number of concurrent sessions has been reached. Please try your request again later."

- OC4J_Content.default_island.1 or application.log: "IFS-20127: Service too busy (maximum concurrent sessions)"

If you see either error, modify the node configuration to change the service configuration from small to medium or from medium to large. You can also create a custom service configuration. If you use the large service configuration, or if you create a custom service configuration, you must adjust your `-Xmx` setting.

If you see `java.lang.OutOfMemory` errors in your `OC4J_Content.default_island.1` or `application.log` files, then you also need to adjust your `-Xmx` setting.

[Table 12-1](#) describes factors that might require you to change the `-Xmx` setting.

Table 12-1 Xmx Settings

Service Configuration	Setting for IFS.SERVICE.MaximumConcurrentSessions	Expected PCCU	Recommended Size for Xmx (Java Maximum Memory)	Need to change the default Xmx setting of 256MB?
Small	40	25	64 MB	No
Medium	70	45	162 MB	No
Large	200	125	430 MB	Yes

Note: The term PCCU refers to Peak Concurrent Connected Users. PCCU is the number of users who are signed on to Oracle Content DB and have performed an operation during the peak hour of the day. If you do not know the number of peak hour users, assume 10 percent of your Oracle Content DB user population.

See "[Creating Service Configurations](#)" on page 8-9 for additional information about creating custom service configurations. See "[Modifying Node Configurations](#)" on page 8-5 for information about changing service configurations for a node.

Calculating Xmx Settings

A general guideline for calculating the `Xmx` setting is:

$$Xmx = PCCU * 2.8MB$$

Alternatively, you can use the following equation to determine a more precise value:

$$Xmx = (PCCU * 1.6 \text{ sessions per PCCU} * 1MB \text{ per session}) + (DATACACHE.Size * 3KB \text{ per data cache object}) + (20\% \text{ JVM overhead for garbage collection})$$

The maximum value for the `Xmx` setting depends on your operating system. On Linux operating systems, the setting cannot exceed 2GB. On Solaris operating systems, the setting cannot exceed 4GB. Oracle recommends that the `Xmx` setting does not exceed 2GB for Oracle Content DB.

See "[Adjusting Java Parameters for Nodes](#)" on page 8-7 for information about how to change the `Xmx` setting.

Adjusting Service Configuration Settings

If you expect that your peak concurrent connected users (PCCU) will exceed 125, create a custom service configuration using the following recommendations:

```
MaximumConcurrentSessions = 1.6 * PCCU
DATACACHE.Size = 400 * PCCU
DATACACHE.EmergencyTrigger = 0.80 * DATACACHE.Size
DATACACHE.UrgentTrigger = 0.75 * DATACACHE.Size
DATACACHE.NormalTrigger = 0.65 * DATACACHE.Size
DATACACHE.PurgeTarget = 0.55 * DATACACHE.Size
CONNECTIONPOOL.WRITEABLE.MaximumSize = 0.05 * PCCU
CONNECTIONPOOL.WRITEABLE.TargetSize = 0.04 * PCCU
CONNECTIONPOOL.WRITEABLE.MinimumSize = 5
CONNECTIONPOOL.READONLY.MaximumSize = 0.05 * PCCU
CONNECTIONPOOL.READONLY.TargetSize = 0.04 * PCCU
CONNECTIONPOOL.READONLY.MinimumSize = 5
```

The other settings in the service configuration generally do not need to be adjusted.

Performance Tuning

Performance is typically affected by network I/O, hard-disk drive I/O, memory (random access memory) I/O, or some combination of these three or other factors. Adjusting one of the factors sometimes moves the performance problem to a new location, so you must approach the tuning task in a logical manner.

In addition to the information provided in the following section, see ["Storing Files in an Oracle Database"](#) on page 2-11 and ["Oracle Content DB Metadata and Infrastructure"](#) on page 2-13 for information about how to calculate the appropriate space for document storage.

See *Oracle Database Performance Tuning Guide* for complete information about performance tuning.

Running the Oracle Content DB analyze.sql Script

Oracle Content DB uses Oracle Database Cost-Based Optimizer (CBO) to determine the most efficient way to run SQL statements. For the CBO to work properly, the Oracle Content DB `analyze.sql` script needs to be run as part of regular Oracle Content DB operations, especially after large volume changes to the data, such as after users have loaded a large number of files into the database instance. This script generates statistics about the distribution of data in Oracle Content DB so that the CBO can choose the most efficient way to execute SQL statements. For more information about the Cost-Based Optimizer, see *Oracle Database Performance Tuning Guide*.

Run the script during periods that are not busy to avoid impeding system performance.

The `analyze.sql` script, which makes calls to the `DBMS_STATS` package, exports schema statistics to a backup table, so you can restore statistics later, if necessary, as discussed in ["Restoring Prior Statistics"](#) in the following section. To run the script, first ensure that a SQL*Plus client has been installed. Then, enter the following at the command line:

```
cd ORACLE_HOME/content/admin/sql
sqlplus content_db_schema/password@connect_string @analyze.sql content_db_schema
```

This script may take a while to run, especially if Oracle Content DB contains a large number of documents.

Restoring Prior Statistics

Before gathering new statistics, the `analyze.sql` script exports backup statistics to the `IFS_BACKUP_STATS` table, marking the set of statistics with a time stamp. You can query the table for existing saved sets by running this SQL statement:

```
SQL> select distinct statid from IFS_BACKUP_STATS;
```

This query returns a list of all statistics by statistic ID (the date and time stamp). For example:

```
STATID
-----
01-MAY-02 02:15.36
04-MAY-02 20:00.15
08-MAY-02 02:15.48
11-MAY-02 06:21.40
11-MAY-02 20:15.37
```

You can then restore the statistics from a day and time when you know performance was better. For example, if you find that after using the statistics from the 8:00 p.m. run of the `analyze` script that performance is worse, then you can restore the statistics from earlier that day using:

```
SQL> call dbms_stats.import_schema_stats (content_db_schema,
'IFS_BACKUP_STATS', '08-MAY-02 06:21.40', content_db_schema);
```

By restoring the statistics, you are directing the CBO to revert to the way it previously ran SQL statements.

Analyzing Performance Problems

After ensuring that you have run statistics properly and have enough free hard-disk space to support the tablespaces, you may still have performance problems. If you have performance problems, you must determine whether the performance bottleneck is caused by Oracle Database, Oracle Content DB, or other factors.

To isolate the problem, start looking at which processes are running and how many resources they are using:

1. Run `top` (on UNIX) or start the Task Manager (on Windows platforms) as you reproduce the problem.
2. Determine whether a Java process, the Oracle shadow process, I/O, or a combination is the bottleneck during that time.

If the Database Is Causing the Problem

If the problem is the Oracle shadow process, use the Statspack utility to determine the SQL statement that is causing the largest number of buffer gets, and run Explain Plan on it.

If you see full table scans, then that may be the cause of the problem; the optimizer may not be choosing an appropriate plan. Report that problem to Oracle Support Services. Additional work must be done to isolate the problem.

For more information about the Statspack utility and Explain Plan, see *Oracle Database Performance Tuning Guide*.

If the Java Processes Are Causing the Problem

You may not have enough memory. For example, if you see any `java.lang.OutOfMemoryError` errors in your logs, increase your maximum memory (`Xmx`) settings for that JVM. See ["Modifying Node Configurations"](#) on page 8-5 for more information about changing the `Xmx` setting.

If users are experiencing poor response times, and `top` (on UNIX) or its equivalent (for example, Task Manager on Windows platforms), shows a Java process running at 100 percent of a CPU for a minute or longer, then the `Xmx` setting for Java may be too small.

1. Turn on verbose garbage collection (`verbosegc`). To do this, edit the Java Parameters of the node configuration. See ["Adjusting Java Parameters for Nodes"](#) on page 8-7 for more information.

In the node log file, output related to garbage collection appears as follows:

```
[Full GC 1476K->1476K(2112K) , 0.0549430 secs]
```

A Full GC occurs when the Garbage Collector has exhausted all available memory in the nursery, and has to go into the rest of the heap to reclaim memory.

2. If Full GCs occur more than once every 10 minutes (not just after startup), increase your `Xmx` settings for that JVM.

Viewing Cache Statistics and Changing Cache Settings

If the problem is an Oracle Content DB Java process, start by checking the percentage of cache hits for the Oracle Content DB service using the Application Server Control, as follows:

1. Connect to the Application Server Control and go to the Content DB Home page. See ["Accessing the Oracle Content DB Home Page"](#) on page 1-3 for information about how to do this.
2. Click the name of the service (for example, `IfsDefaultService`). The Service page appears.
3. Click the **Performance** tab.
4. In the Committed Data Cache Statistics section, you can view real-time data for Cache Size, Cache Puts, Cache Removes, Cache Purges, Cache Purge Cycles, Cache Lookups, and Cache Hits.

The goal is to have a high percentage of Cache Hits; as much as 100 percent is possible. If the percentage of Cache Hits for the service is less than 98 percent, the size of the Committed Data Cache may be too small.

Because the Statistics Agent captures the real-time data, you can also see prior statistics by viewing the node log or application log. You can also configure this agent to write statistics to a document stored in the Oracle Content DB repository. See ["Statistics Agent"](#) on page E-12 for information about the Statistics Agent.

5. To change the run-time Cache settings, click the **Administration** tab.
6. In the Data Cache table row, click the **Go to Task** icon.
7. Proportionately increase all Cache settings (Cache Capacity, Normal Purge Trigger, Urgent Purge Trigger, Emergency Purge Trigger, Purge Target) and click **Apply**.

This will increase your memory usage on the middle tier computer by approximately 3 KB for each object. For example, if you increase cache capacity by 5000, your memory usage will grow by 15 MB.

To make the changes permanent, update the service configuration. See ["Modifying Service Configurations"](#) on page 8-10 for more information.

Viewing Connection Pool Statistics and Changing Connection Pool Settings

Check the target and maximum number of connections for the Read-Only and Writable Connection Pools using the Application Server Control, as follows:

1. Connect to the Application Server Control and go to the Content DB Home page. See ["Accessing the Oracle Content DB Home Page"](#) on page 1-3 for information about how to do this.
2. Click the name of the service (for example, **IfsDefaultService**). The Service page appears.
3. Click the **Performance** tab.
4. Look at the statistics in the Read-Only and Writable Connection Pool Statistics sections.

You will need to increase the Target Maximum Number of Connections and Absolute Maximum Number of Connections if any of the following is true:

- Failed Allocations is greater than zero.
- Total Connections is more than two higher than Target Maximum Number of Connections.
- Deferred Allocations is greater than 5 percent, and Average Allocation Time (ms) is more than 10 milliseconds.

Because the Statistics Agent captures the real-time data, you can also see prior statistics by viewing the node log or application log. You can also configure this agent to write statistics to a document stored in the Oracle Content DB repository. See ["Statistics Agent"](#) on page E-12 for information about the Statistics Agent.

5. To change the run-time Connection Pool settings, click the **Administration** tab.
6. In the Read-Only Connection Pool or Writable Connection Pool table row, click the **Go to Task** icon.
7. Increase the **Target Maximum Number of Connections** and **Absolute Maximum Number of Connections**, and click **Apply**.

Each additional Target or Absolute connection will use approximately 8 MB for each connection on the middle tier and 1 MB for each connection on the database.

To make the changes permanent, update the service configuration. See ["Modifying Service Configurations"](#) on page 8-10 for more information.

Troubleshooting Oracle Content DB

Use this appendix to troubleshoot problems in your Oracle Content DB installation.

This appendix provides information about the following topics:

- [Solving General Administration Problems](#)
- [Solving Performance Problems](#)

Solving General Administration Problems

[Table A-1](#) provides information about how to troubleshoot general Oracle Content DB administration problems.

Table A-1 General Administration Issues

Problem	Probable Cause	Corrective Action
The administrator has uploaded files and removed them, and does not see the space retrieved in the tablespace.	The Initial Time of Day and Activation Period has been set incorrectly for the Content GarbageCollectionAgent.	Use the Application Server Control to view the Initial Time of Day and Activation Period entries for the Content Garbage Collection Agent. Also check the node log and see if the Content Garbage Collection Agent is being activated at periodic intervals.
When using Oracle Internet Directory, users fail to be provisioned, or newly provisioned users cannot be added to Libraries.	Required user attributes were not set in Oracle Internet Directory.	The following Oracle Internet Directory user attributes must be nonnull for all users: <code>sn</code> , <code>givenName</code> , <code>mail</code> . In addition, all users must have a nonnull user name. The user name is specified by the <code>orclCommonNicknameAttribute</code> in the OracleContext of the realm. See <i>Oracle Internet Directory Administrator's Guide</i> for more information about viewing the <code>orclCommonNicknameAttribute</code> .
After adding a user to a file-based user repository using the OracleAS JAAS Provider Admintool, the new user cannot log in to Oracle Content DB.	OC4J_Content was not restarted after the user was added.	After you add a user to a file-based user repository using the OracleAS JAAS Provider Admintool, you must restart OC4J_Content before the user can log in to Oracle Content DB. Alternatively, you can use the Application Server Control to add users. You do not need to restart OC4J_Content after adding users with the Application Server Control.
In the Oracle Content DB Web client, in Administration Mode, user administrators can see users who were deleted in the user repository, as well as update the profile information for these users.	The <code>deleteuser</code> script was not run after deleting the users in the user repository.	You must run the <code>deleteuser</code> script to remove users from Oracle Content DB after you delete users in the user repository. See "Deleting Users in Oracle Content DB" on page 5-5 for more information.
Users cannot access Properties dialog boxes or other dialog boxes in the Oracle Content DB Web client.	Pop-up blockers are blocking these application dialog boxes.	Users must disable pop-up blockers to access some features of the Oracle Content DB Web client. Users can hold down the Ctrl key while clicking Launch to bypass most pop-up blockers. In addition, users can refer to the Help for the browser for more information about pop-up settings.

Table A-1 (Cont.) General Administration Issues

Problem	Probable Cause	Corrective Action
In the user preferences dialog in the Oracle Content DB Web client, the values for First Name, Last Name, and E-mail Address are blank and cannot be updated by users.	The User Administrator has not provided these values.	If you are using a file-based user repository as your Oracle Content DB user repository, there is no way to provide the First Name, Last Name, and E-mail Address user profile values when you create users. To set these values, log in to the Oracle Content DB Web client as a User Administrator and switch to Administration mode. Then, access the user profile for each user you added and set these attributes.
You have added a user to your user repository, but cannot find this user in Oracle Content DB user searches.	The user has not yet logged in to Oracle Content DB.	Because users are not provisioned until they log in for the first time, they may not appear in Oracle Content DB searches, even though they exist in the user repository. You must wait until the user logs in to Oracle Content DB before searching for the user, or attempting to add the user to a Library.
Cannot connect to Oracle Content DB.	The Oracle Content DB server may be using DHCP.	If Oracle Content DB is using DHCP, use the current IP address of the server to connect, rather than the host name. All Oracle Content DB protocols are affected, including HTTP.
In the Application Server Control, the following error message appears for a particular server on the Node page: "This server is configured but not loaded now."	The server may not have been configured correctly, or the server may have an initialization or loading problem. This message also appears when the server has been deleted from the node at run time, but still exists in the node configuration.	Check the node log for information about possible initialization and loading errors for this server.
Cannot log in as cn=orcladmin (Oracle Internet Directory user repository only).	You forgot or do not know the cn=orcladmin password.	You can reset the password in the Metadata Repository database. The DSE root attribute name is orclsupassword. Note: After a certain number of failed attempts to connect, the cn=orcladmin account becomes locked. In this case, you must unlock the account.
The cn=orcladmin account becomes locked (Oracle Internet Directory user repository only).	The cn=orcladmin account becomes locked, by default, after 10 failed attempts to connect. This setting is controlled by the password policy.	If you know the cn=orcladmin password, you can unlock the account by running the following command from the OracleAS Infrastructure Oracle home: <code>ORACLE_HOME/bin/oidpasswd connect=db_SID unlock_su_acct=true</code> In the preceding command, <code>db_SID</code> is the SID for the database. For example: <code>ORACLE_HOME/bin/oidpasswd connect=orcl unlock_su_acct=true</code> OID DB user password: my_ODS_password OID superuser account unlocked successfully. The command prompts for the password of the ODS schema. By default, the ODS password is the same as for the cn=orcladmin account, which was set during OracleAS Infrastructure installation. See Also: <i>Oracle Internet Directory Administrator's Guide</i> for information about changing the password policy for the allowed number of failed attempts to connect
Users are experiencing problems logging in through the Web client after logging out.	The user did not close all browser windows after logging out of Oracle Content DB.	Because of JAZN limitations, to fully log out of Oracle Content DB, users must close all browser windows associated with the browser they used to log in to Oracle Content DB. For example, if users logged in using Microsoft Internet Explorer, they must close all Internet Explorer windows after they log out.

Table A-1 (Cont.) General Administration Issues

Problem	Probable Cause	Corrective Action
The password for the <code>cn=orcladmin</code> account has expired, and you want to change the default password expiration time.	The default password expiration time is 60 days.	<p>To change the default expiration time for the <code>cn=orcladmin</code> password:</p> <ol style="list-style-type: none"> If the <code>cn=orcladmin</code> account is locked, you must unlock the account before you can modify the password policy. See the preceding item in this table for more information. Log in to Oracle Directory Manager and go to Password Policy Management. Look for the following two attributes: <ul style="list-style-type: none"> The <code>PasswordExpiryTime</code> attribute under the <code>cn=PwdPolicyEntry</code> (for example, <code>password_policy_entry, dc=mycompany, dc=com</code>) The <code>pwdmaxage</code> attribute under Entry Management (for example, <code>cn=PwdPolicyEntry, cn=common, cn=products, cn=OracleContext, dc=mycompany, dc=com</code>) Change the <code>pwdmaxage</code> attribute in each password policy to an appropriate value. For example: <ul style="list-style-type: none"> 5184000 = 60 days (default) 7776000 = 90 days 10368000 = 120 days 15552000 = 180 days 31536000 = 1 year <p>Note: It is very important to change this value in both places.</p> Still in Oracle Directory Manager, go to the realm-specific <code>orcladmin</code> account. Find the <code>userpassword</code> attribute and assign a new value. You can then start any Oracle component that uses Oracle Single Sign-On and log in as <code>orcladmin</code>. Run the <code>oidsrvreg</code> utility to reset the randomly generated password for Oracle Directory Integration and Provisioning. For example: <pre>oidsrvreg -D cn=orcladmin -w mypassword -p 3060 Already Registered...Updating DIS password... DIS registration successful.</pre> <p>See Also: <i>Oracle Identity Management Integration Guide</i> for more information</p>
An out-of-memory exception occurs when running Oracle Content DB.	The maximum Java heap size is too low.	Increase the heap size by modifying the <code>-Xmx</code> setting for that node configuration. See "Modifying Node Configurations" on page 8-5 for more information.
Content queries through the Web and Windows return no rows.	Oracle Text indexing of the documents has not occurred.	See "Maintaining the IFS_TEXT Index by Using the Oracle Text PL/SQL Packages" on page C-2 for more information.
In the Application Server Control, cannot view the Oracle Content DB Web services in the Web Services tab of the OC4J_Content page.	The Oracle Content DB Web services do not use the Oracle Application Server Web Services framework	The Oracle Content DB Web services use the Axis framework, not the Oracle Application Server Web Services framework. Because of this, in the Application Server Control, the Oracle Content DB Web services do not appear in the Web Services tab for OC4J_Content.
When using the Search Logs function in the Application Server Control, cannot find OC4J_Content logs.	The log search criteria include message types that do not apply.	On the Search Logs page in the Application Server Control, be sure to select Unknown in the Message Types section. Oracle Content DB logs are not categorized by the other message types listed (Internal Error, Warning, Trace, Error, and Notification).

Solving Performance Problems

Table A-2 provides information about how to troubleshoot problems with Oracle Content DB performance.

Table A-2 Performance Issues

Problem	Probable Cause	Corrective Action
Server is generally slow for read and write activity (case #1).	Server memory is overcommitted. The server is excessively swapping memory blocks to disk.	Run system monitoring tools, such as <code>vmstat</code> (UNIX) and look for excessive page swapping to verify the problem. Adjust the following parameters in the <code>init.ora</code> file for the database: <ul style="list-style-type: none"> ■ Reduce <code>processes</code>. ■ Reduce <code>open_cursors</code>. ■ Reduce <code>db_block_buffers</code>. Stop unneeded Java VMs or other unneeded processes. You may also need to add memory to your server or, if you are running a single-tier configuration, reconfigure your Oracle Content DB server into a two-tier configuration.
Server is generally slow for read and write activity (case #2).	CTXHX is using 100 percent of your CPU.	See Appendix C, "Managing the Oracle Text Index" .
Server is slow only on read or search activity.	Large volumes of data have been loaded but the CBO statistics were not updated.	If the Cost-Based Optimizer is using out-of-date statistics data, performance suffers. Run the <code>analyze.sql</code> script located in the <code>ORACLE_HOME/content/admin/sql</code> directory to refresh the statistics.
Server is slow only on content-based search activity (case #1).	Oracle Text tablespaces are on the same disk as other database files.	Move the Oracle Text tablespaces to other disks. See <i>Oracle Database Administrator's Guide</i> for more information about moving tablespaces.
Server is slow only on content-based search activity (case #2).	Oracle Text indexes have become fragmented.	Regularly optimize the Oracle Text Oracle index <code>IFS_TEXT</code> . See "Maintaining the IFS_TEXT Index by Using the Oracle Text PL/SQL Packages" on page C-2 for more information.
Server is slow only on write activity (case #1).	Large amounts of documents are being loaded and the Redo logs are too small.	Add two or more 100 MB or larger Redo logs. See <i>Oracle Database Administrator's Guide</i> for more information. In general, Redo logs should be switching every hour or less frequently. See the <code>ORACLE_HOME/rdbms/sid/bdump</code> directory for the latest logs which indicate the frequency of Redo log switching.
Server is slow only on write activity (case #2).	Large amounts of documents are being loaded and the Redo logs are on the same disk as the database files.	Place the Redo logs on a separate disk from the database files. See <i>Oracle Database Administrator's Guide</i> and <i>Oracle Database Performance Tuning Guide</i> for more information. For optimal performance, dedicate one or more disks (and, if possible, a disk controller) exclusively to the Redo logs, and optimize the disks for sequential write activity. For example, on Solaris Operating System (SPARC), you may choose raw partitions or UNIX file systems for the disks. If you choose UNIX file systems on Solaris 2.6 or later, use the "forcedirection" option when mounting the file systems. These options should only be used if the file systems are dedicated exclusively to the Redo logs.

Migrating Content to Oracle Content DB

This chapter provides information about how to migrate content and users from legacy systems to Oracle Content DB. Oracle Content DB migration is applicable to customers migrating from the following systems:

- Oracle Content Management SDK
- Third-party applications, such as Novell

Oracle Content DB does not currently offer a migration toolkit. You must migrate your files manually. If you are migrating a very large number of files and require assistance, contact Oracle Support Services.

This appendix provides information about the following topics:

- [Migration Tasks](#)
- [Migrating Oracle Content DB Users](#)
- [Creating Oracle Content DB Libraries](#)
- [Migrating Oracle Content DB Content](#)

Migration Tasks

Consolidating users, folder hierarchy, content, and access privileges from other file server systems to Oracle Content DB involves the following tasks:

- [Migrating Oracle Content DB Users](#): You need to move the user list from the old file system to the new one. In other words, you need to re-create each user in the Oracle Content DB user repository.
- [Creating Oracle Content DB Libraries](#): If you have folders grouped into logical structures with specific security, you can create corresponding Libraries in Oracle Content DB with the same membership and access permissions.
- [Migrating Oracle Content DB Content](#): You must copy the actual files and folders from the old system to the new one.

Migrating Oracle Content DB Users

The first task in moving to a new Oracle Content DB server is creating the user list.

For each user you want to migrate to Oracle Content DB, create a user in your Oracle Content DB user repository. See [Chapter 5, "Managing Oracle Content DB Users"](#) for more information.

Creating Oracle Content DB Libraries

To migrate user groups into Oracle Content DB, you must create or update corresponding Libraries and member roles in Oracle Content DB.

Scripted Library Creation

If your management tools let you export group information to a file, you can write a translation script to convert the groups into XML format. Then, you can use the Library Creation tool to create corresponding Libraries in Oracle Content DB. See the developer documentation for more information about the Library Creation tool.

Migrating Oracle Content DB Content

After creating users and Libraries, the next step is to move files and folders into Oracle Content DB. However, if your old file system had application-specific metadata, this information cannot be automatically copied.

How to Copy the Data

Use one of the following methods to copy your files:

- **Web-based Distributed Authoring and Versioning (WebDAV):** WebDAV, a protocol designed for Internet and intranet collaboration on files, enables you to drag and drop data from one system to another. If you want to retain the file structure, click and drag the entire directory structure from the original file system into Oracle Content DB, or drag different parts of the directory tree separately, confirming that each part of the tree has been copied before copying the next one.

See "[Using WebDAV with Oracle Content DB](#)" on page 1-11 for more information about using WebDAV.
- **Oracle Drive:** Oracle Drive is a desktop client that uses the WebDAV protocol to access Oracle Content DB. After it is installed, Oracle Drive appears as a mapped drive in your Windows Explorer. Oracle Drive also provides file synchronization capabilities between your local computer and Oracle Content DB. See "[Using Oracle Drive with Oracle Content DB](#)" on page 4-10 for more information.

Managing the Oracle Text Index

Oracle Content DB uses Oracle Text to facilitate full-text search and other advanced capabilities. The speed with which results are returned depends on several factors, including the quality of the Oracle Text index used with Oracle Content DB (IFS_TEXT). The performance of the search can also depend on how much time you let elapse before a search times out.

Oracle Content DB uses an additional index, the IFS_LYKE index, to speed up substring searches on known items. For example, the IFS_LYKE index facilitates searches such as "*planning*" or "*.doc." The IFS_LYKE index is automatically created and maintained and does not normally require any administration. If you are having problems related to the IFS_LYKE index, contact Oracle Support Services for troubleshooting information.

This appendix provides information about how to maintain the Oracle Text index to ensure optimal Oracle Content DB performance, and includes these topics:

- [Oracle Text Tablespaces and Disk Utilization](#)
- [Creating and Maintaining the Oracle Text Index](#)
- [Modifying the Search Timeout Parameter](#)
- [Troubleshooting Oracle Text Problems](#)

Previous names for Oracle Text include Oracle Context and Oracle *interMedia* Text. Many of the underlying indexes, views, tables, and various PL/SQL packages referred to in much of the administrator and application developer documentation still use Context or *interMedia*-related terminology.

For detailed information about Oracle Text, visit the Oracle Technology Network at <http://www.oracle.com/technology/products/text>.

Oracle Text Tablespaces and Disk Utilization

Disk space for Oracle Text is divided among three distinct tablespaces:

- The **Oracle Text Tokens** tablespace contains tables that hold text tokens (separate words) that exist within the various indexed documents. The storage for these text tokens is roughly proportional to the ASCII content of the document. The ASCII content percentage will vary depending on the format of the original document. Text files only have white space as their non-ASCII content and, therefore, will incur a greater per-document percentage overhead. Document types such as Microsoft Word or PowerPoint contain large amounts of data required for formatting that does not qualify as text tokens. The per-document percentage on these types of documents will, therefore, be lower. On a system with diverse

content types, the expected overhead is approximately 8 percent of the sum of the original sizes of the indexed documents.

- The **Oracle Text Index** tablespace contains the B*tree database index that is used against the text token information stored in the Oracle Text Tokens tablespace. This will grow as a function of the ASCII content, just as the Oracle Text Tokens tablespace does. On a system with diverse content types, the expected overhead is approximately 4 percent of the sum of the ASCII content of the documents, or approximately 1 percent of the sum of the total sizes of the indexed documents.
- The **Oracle Text Other** tablespace contains the tables and indexes required to translate from the Oracle Content DB locator of a document (the Oracle Content DB DocID) to the Oracle Text locator of that same document (the Oracle Text DocID). The expected space utilization for this tablespace is approximately 70 bytes for each indexed document.

Use this information to estimate and plan disk storage needs for your Oracle Content DB instance.

Creating and Maintaining the Oracle Text Index

The configuration process for Oracle Content DB uses the SQL scripts shown in [Table C-1](#) to create and populate the IFS_TEXT index.

These scripts are located in the following directory:

`ORACLE_HOME/content/admin/sql`

Table C-1 SQL Scripts for Creating Oracle Text Index

Script	Usage	Log In As	Arguments
CreateContext FunnelProcedure.sql	Creates the procedure used by USER_DATASTORE.	CONTENT	None
GrantContext ToIFS.sql	Grants the Oracle Content DB user (schema) privileges on the Oracle Text-specific commands required to maintain the index.	SYS	CONTENT
CreateContext Preferences.sql	Tablespace and other text preferences are created by the Oracle Content DB user.	CONTENT	<i>OracleText_index_</i> <i>tablespace</i> <i>OracleText_keymap_</i> <i>tablespace</i> <i>OracleText_data_</i> <i>tablespace</i> CONTENT (the Oracle Content DB schema name)
CreateContext Index.sql	Creates the IFS_TEXT index based on the text preferences.	CONTENT	None

Maintaining the IFS_TEXT Index by Using the Oracle Text PL/SQL Packages

Two PL/SQL procedures are provided with Oracle Text for maintaining the index. Unlike a regular database index, the Oracle Text index is not dynamically updated with each insert or update of information. Rather, the index must be refreshed (or synchronized) periodically, using the Oracle Text stored procedure `ctx_ddl.sync_index`.

The `ctx_ddl.sync_index` procedure does not rebuild the entire index; it adds and deletes records that have changed since the last synchronization. Because the changes are incremental, the more frequently this procedure is run, the faster it runs. Over the course of time, however, the index can become fragmented, so a companion procedure (`ctx_ddl.optimize_index`) is provided to optimize the index.

During Oracle Content DB configuration, the procedures to synchronize and optimize the `IFS_TEXT` index are automatically set up to run periodically in the background, using the `DBMS_JOBS` package of Oracle Database. `DBMS_JOBS` procedures, which are similar to `cron jobs` on UNIX systems, are portable across all platforms on which Oracle Database runs.

When the Oracle Content DB schema is created during configuration, two `DBMS_JOBS` are set up: Sync Job and Optimize Job. The name of the Oracle Content DB schema is `CONTENT`.

Sync Job

Sync Job will periodically call the `ctx_ddl.sync_index()` method. This method indexes the documents that were created or updated since the last run. By default, this job runs every 30 minutes.

Optimize Job

Optimize Job will periodically call the `ctx_ddl.optimize_index()` method. The goal of this job is to optimize the `IFS_TEXT` index by defragmenting it. By default, this job is run in `FULL` mode, with a maximum of 1 hour allocated for the optimization task. The job runs every 24 hours, starting at midnight.

Monitoring DBMS_JOBS

`DBMS_JOB` logs can be found under the Oracle home that hosts Oracle Database, in the directory that holds the background process logs. This directory is pointed to by the `BACKGROUND_DUMP_DEST` configuration parameter of the database server. You can recognize the log trace files by their name pattern, `DBNAME_j###_process-id.trc`.

Another database configuration parameter, `JOB_QUEUE_PROCESSES`, determines how many processes are available to run all background tasks. You may need to increase the value of this parameter if not enough processes are available to run Sync Job and Optimize Job. The default value is 10.

You can also look at the `USER_JOBS` view to see a list of all the jobs set up by the current schema user. The `USER_JOBS` view shows details such as the PL/SQL being run by each job, the last time each job was run, and when the jobs are scheduled to be run next. To see the `USER_JOBS` view, log on to the Oracle Content DB schema (`CONTENT`) using `SQL*Plus`.

Changing or Removing the Default DBMS_JOBS

Two SQL files are used to set up and clear the `DBMS_JOBS` in Oracle Content DB: `SetupContextJobs.sql` and `ClearContextJobs.sql`. These files are located in the following directory:

```
ORACLE_HOME/content/admin/sql
```

`SetupContextJobs.sql` is used by the system during configuration to set up Sync Job and Optimize Job. `ClearContextJobs.sql` is provided to remove Sync Job and Optimize Job, in case you want to set up your own `DBMS_JOBS`.

See *Oracle Database Administrator's Guide* for information about setting up your own DBMS_JOBS. You can also look at Sync Job and Optimize Job as examples.

Manually Synchronizing and Optimizing IFS_TEXT

To synchronize an existing IFS_TEXT index, use SQL*Plus to connect as the Oracle Content DB schema user (CONTENT), and enter:

```
exec ctx_ddl.sync_index('ifs_text');
```

You can also run the SyncContextIndex.sql script from the ORACLE_HOME/content/admin/sql directory. In addition to synchronizing the IFS_TEXT index, this script will display extra log information on the console.

To optimize an existing IFS_TEXT index, use SQL*Plus to connect as the Oracle Content DB schema user (typically CONTENT), and enter:

```
exec ctx_ddl.optimize_index('ifs_text', 'FAST');
```

or

```
exec ctx_ddl.optimize_index('ifs_text', 'FULL', maxtime);
```

Monitoring Oracle Text Indexing of Oracle Content DB Documents

Oracle Content DB provides some utility-type SQL scripts to facilitate interaction with Oracle Text. Read each .sql file for additional usage details. All scripts are available in:

ORACLE_HOME/content/admin/sql

Table C-2 lists the SQL scripts provided by Oracle Content DB to monitor Oracle Text.

Table C-2 SQL Scripts for Monitoring Oracle Text Indexing

Script	Usage
ViewContextErrors.sql	Script that decodes the operating system-specific errors that were generated during Oracle Text indexing.
SyncContextIndex.sql	Script that synchronizes the Oracle Text index and enables you to monitor the Oracle Text synchronization process. Uncomment the first two lines in the script, which includes a call to ctx_output.add_event(), to monitor on a row ID by row ID basis.
ViewDocumentByRowID.sql	Script that enables you to view additional information about a document that is indexed by Oracle Text. Use the docid from the Oracle Text log with this script.

Indexing Non-Standard Content Types

Oracle Content DB does not, by default, index every file that is moved into the system, but you can configure it to index any type of content you choose. To do this, designate the MIME type as Indexed on the New Format page (or Edit Format page, if the format already exists) in the Application Server Control. The MIME type of a document is determined by its extension.

For example, you may want to index all your C# (.cs) source code files. To do so:

1. Use the Application Server Control to add the .cs MIME type, and designate it as **Indexed** on the New Format page.
2. Upload the files into the repository.
3. Synchronize the index using the procedure discussed in ["Manually Synchronizing and Optimizing IFS_TEXT"](#) on page C-4.

See ["Default Formats"](#) on page 10-4 for a list of formats that are indexed by default in Oracle Content DB.

Modifying the Search Timeout Parameter

The `IFS.SERVICE.SESSION.DefaultSearchTimeoutPeriod` service configuration parameter specifies the timeout period for a running search that has not yet returned results. The default setting for this parameter (in the default service configurations) is 60 seconds. If you increase this value, users will wait longer than a minute before a search times out; decrease the value to shorten the time in which a running search will time out.

See ["Modifying Service Configurations"](#) on page 8-10 for information about how to modify service configuration parameters.

Troubleshooting Oracle Text Problems

[Table C-3](#) provides Oracle Text troubleshooting information.

Table C-3 Troubleshooting Oracle Text Problems

Problem	Probable Cause	Corrective Action
Cannot search on contents of any documents.	Documents have not been indexed.	Start the database instance and ensure that the Oracle Text indexing jobs are running. See "Creating and Maintaining the Oracle Text Index" on page C-2 for more information.
Server is slow only on content-based search activity (case #1).	Oracle Text tablespaces are on the same disk as other database files.	Move the Oracle Text tablespaces to other disks. See <i>Oracle Database Administrator's Guide</i> for more information about moving tablespaces.
Server is slow only on content-based search activity (case #2).	Oracle Text indexes have become fragmented.	Regularly optimize the Oracle Text index GLOBALINDEXEDBLOB_I. See "Manually Synchronizing and Optimizing IFS_TEXT" on page C-4 for more information.
Searching on the contents of new documents stops working.	A recent document has caused Oracle Text server to fail.	<ol style="list-style-type: none"> 1. Log in to SQL*Plus as <code>content_db_schema/schema_password</code>, and enter the following command: <pre>select count(*) from ctx_user_pending;</pre> The name of the Oracle Content DB schema is CONTENT. 2. If there are any rows in that view and the rows are not changing, then a recent document has caused Oracle Text to stop indexing. To determine which Oracle Content DB documents these rows refer to, see the problem "Oracle Content DB rows show up in the Oracle Text view ctx_user_index_errors." 3. Check again to see if there are any rows in <code>ctx_user_pending</code> and, if so, that the rows are changing. 4. If this does not resolve the issue, contact your Oracle Support Services representative for further assistance.

Table C-3 (Cont.) Troubleshooting Oracle Text Problems

Problem	Probable Cause	Corrective Action
<p>Oracle Content DB rows show up in the Oracle Text view <code>ctx_user_index_errors</code>.</p>	<p>Oracle Content DB documents are corrupt or do not have the correct extension.</p>	<ol style="list-style-type: none"> 1. Determine which Oracle Content DB document is being referred to, based on the <code>err_textkey</code> from <code>ctx_user_index_errors</code>. <pre>sqlplus content_db_schema/schema_password select du.uniqueid, vd.name, co.contentsize, cs.id, vd.id from odm_document vd, odm_contentobject co, odmm_contentstore cs, odm_document od, odm_directoryuser du where vd.id = od.id and od.contentobject = co.id and co.content = cs.id and du.id = vd.owner and cs.id in (select distinct od.id from ctx_user_index_errors cp, odmm_ contentstore od where od.rowid = err_textkey) order by cs.id;</pre> 2. Log in to Oracle Content DB as a user with the Content Administrator role and switch to Administration Mode. 3. Search on the document name <code>vd.id</code>, where <code>vd.id</code> is the <code>vd.id</code> returned from the <code>SELECT</code> statement provided in Step 1. 4. Check document attributes, such as document size, to ensure that it is the correct document. 5. Examine this document, and consider these questions: Is the file damaged in any way? Is the file name extension correct for this document? Is the character set of the document correct? 6. If no obvious problems are found, send the document to your Oracle Support Services representative for further diagnosis.
<p>Oracle Content DB rows never get processed and never leave the Oracle Text view <code>ctx_user_pending</code>.</p>	<p>Oracle Content DB documents are corrupt or do not have the correct extension.</p>	<ol style="list-style-type: none"> 1. Follow the steps in "Oracle Content DB rows show up in the Oracle Text view <code>ctx_user_index_errors</code>." to determine which Oracle Content DB documents are being referred to, substituting <code>ctx_user_pending</code> for <code>ctx_user_index_errors</code> and <code>pnd_rowid</code> for <code>err_textkey</code>. 2. Examine this document, and consider these questions: Is the file damaged in any way? Is the file name extension correct for this document? Is the character set of the document correct? 3. If no obvious problems are found, send the document to your Oracle Support Services representative for further diagnosis. 4. Delete the document from Oracle Content DB.

Service Configuration Properties

An Oracle Content DB service comprises a Java runtime environment for the protocol servers and agents that it supports. A service also manages connections to the database through JDBC. There are three default service configuration objects you can use to create new services on nodes:

- SmallServiceConfiguration
- MediumServiceConfiguration
- LargeServiceConfiguration

The differences among the three configuration templates are in the number of connections and sessions supported.

This appendix lists the service configuration properties and their default values.

Note: Do not use spaces to separate alternate values of a property. Instead, use a comma as a delimiter.

Table D-1 IFS.SERVICE.* Properties

Property	Description and Usage Notes	Default	Required?
IFS.SERVICE.ACLCACHE.EmergencyTrigger	The cache size, in ACLs, at which the service ACL cache performs an immediate purge of data that has not been recently used. Must be greater than IFS.SERVICE.ACLCACHE.UrgentTrigger but less than IFS.SERVICE.ACLCACHE.Size.	600 - Small 2400 - Medium 6000 - Large	No
IFS.SERVICE.ACLCACHE.NormalTrigger	The cache size, in ACLs, at which the service ACL cache schedules a low-priority purge of data that has not been recently used.	500 - Small 2000 - Medium 5000 - Large	No
IFS.SERVICE.ACLCACHE.PurgeTarget	The target cache size, in ACLs, on completion of a purge cycle. Must be less than IFS.SERVICE.ACLCACHE.NormalTrigger.	400 - Small 1600 - Medium 4000 - Large	No
IFS.SERVICE.ACLCACHE.Size	The absolute maximum size of the service's ACL cache, in ACLs. The service ACL cache holds resolved access levels of ACLs.	750 - Small 3000 - Medium 7500 - Large	No
IFS.SERVICE.ACLCACHE.UrgentTrigger	The cache size, in ACLs, at which the service ACL cache schedules a high-priority purge of data that has not been recently used. Must be greater than IFS.SERVICE.ACLCACHE.NormalTrigger.	550 - Small 2200 - Medium 5500 - Large	No

Table D-1 (Cont.) IFS.SERVICE.* Properties

Property	Description and Usage Notes	Default	Required?
IFS.SERVICE. CaseSensitiveAuthentication	Whether, in performing Cleartext authentication, passwords are case-sensitive.	false	No
IFS.SERVICE. CheckForOrphanSessionsPeriod	Number of seconds between checks for orphan sessions. (Active sessions generate heartbeats. An orphan session is one that no longer generates session heartbeats. When the service detects an orphan session, it disconnects the session and releases the resources for the session.) Default is 60 seconds between checks. Set to 0 to disable the checking.	60	No
IFS.SERVICE.CONNECTIONPOOL. READONLY.MaximumSize	The absolute maximum number of database connections in the read-only connection pool. Must be greater than or equal to IFS.SERVICE.CONNECTIONPOOL.READONLY.TargetSize.	20 - Small 40 - Medium 60 - Large	No
IFS.SERVICE.CONNECTIONPOOL. READONLY.MaximumSizeTimeout	The maximum period, in milliseconds, that a service will postpone a connection allocation request when there are no unallocated connections, if the current size of the read-only connection pool is equal to its maximum size. If a database connection does not become available within this period, the allocation request will fail and an exception will occur.	10000	No
IFS.SERVICE.CONNECTIONPOOL. READONLY.MinimumSize	The initial number of database connections in the read-only connection pool.	2 - Small 4 - Medium 6 - Large	No
IFS.SERVICE.CONNECTIONPOOL. READONLY.StatementCacheSizeTrigger	The cache size, in number of statements, at which the statement cache schedules a purge.	150	No
IFS.SERVICE.CONNECTIONPOOL. READONLY.StatementCacheTarget	The target cache size, in number of statements, for the statement cache upon completion of a purge cycle. Must be less than IFS.SERVICE.CONNECTIONPOOL.READONLY.StatementCacheSizeTrigger.	120	No
IFS.SERVICE.CONNECTIONPOOL. READONLY.TargetSize	The target maximum number of database connections in the read-only connection pool. Must be greater than or equal to IFS.SERVICE.CONNECTIONPOOL.READONLY.MinimumSize.	10 - Small 20 - Medium 30 - Large	No
IFS.SERVICE.CONNECTIONPOOL. READONLY.TargetSizeTimeout	The maximum period, in milliseconds, that the service will postpone a connection allocation request when there are no unallocated connections, if the current size of the read-only connection pool is greater than or equal to its target size, but less than the maximum size. If a database connection does not become available within this period, a new connection will be created.	1000	No

Table D-1 (Cont.) IFS.SERVICE.* Properties

Property	Description and Usage Notes	Default	Required?
IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSize	The absolute maximum number of database connections in the writeable connection pool. Must be greater than or equal to IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSize.	20 - Small 40 - Medium 60 - Large	No
IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MaximumSizeTimeout	The maximum period, in milliseconds, that a service will postpone a connection allocation request when there are no unallocated connections, if the current size of the writeable connection pool is equal to its maximum size. If a database connection does not become available within this period, the allocation request will fail and an exception will occur.	10000	No
IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MinimumSize	The initial number of database connections in the writeable connection pool.	2 - Small 4 - Medium 6 - Large	No
IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheSizeTrigger	The cache size, in number of statements, at which the statement cache schedules a purge.	200	No
IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheTarget	The target cache size, in number of statements, for the statement cache upon completion of a purge cycle. Must be less than IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.StatementCacheSizeTrigger.	160	No
IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSize	The target maximum number of database connections in the writeable connection pool. Must be greater than or equal to IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.MinimumSize.	10 - Small 20 - Medium 30 - Large	No
IFS.SERVICE.CONNECTIONPOOL.WRITEABLE.TargetSizeTimeout	The maximum period, in milliseconds, that the service will postpone a connection allocation request when there are no unallocated connections, if the current size of the writeable connection pool is greater than or equal to its target size, but less than the maximum size. If a database connection does not become available within this period, a new connection will be created.	1000	No
IFS.SERVICE.CREDENTIALMANAGER.*	The configuration of credential managers for the service. These properties are set during installation. Do not change these values.	Not applicable	Not applicable
IFS.SERVICE.DATACACHE.Size	The absolute maximum size of the service's data cache, in LibraryObjects. The service data cache holds the attribute values of recently used LibraryObjects.	7500 - Small 30000 - Medium 75000 - Large	No
IFS.SERVICE.DATACACHE.NormalTrigger	The cache size, in LibraryObjects, at which the service data cache schedules a low-priority purge of data that has not been recently used.	5000 - Small 20000 - Medium 50000 - Large	No

Table D-1 (Cont.) IFS.SERVICE.* Properties

Property	Description and Usage Notes	Default	Required?
IFS.SERVICE.DATACACHE.UrgentTrigger	The cache size, in LibraryObjects, at which the service data cache schedules a high-priority purge of data that has not been recently used. Must be greater than IFS.SERVICE.DATACACHE.NormalTrigger.	5500 - Small 22000 - Medium 55000 - Large	No
IFS.SERVICE.DATACACHE.EmergencyTrigger	The cache size, in LibraryObjects, at which the service data cache performs an immediate purge of data that has not been recently used. Must be greater than IFS.SERVICE.DATACACHE.UrgentTrigger but less than IFS.SERVICE.DATACACHE.Size.	6000 - Small 24000 - Medium 60000 - Large	No
IFS.SERVICE.DATACACHE.PurgeTarget	The target cache size, in LibraryObjects, on completion of a purge cycle. Must be less than IFS.SERVICE.DATACACHE.NormalTrigger.	4000 - Small 16000 - Medium 40000 - Large	No
IFS.SERVICE.DefaultCharacterSet	This property is not used.	Not applicable	No
IFS.SERVICE.DefaultLanguage	This property is not used.	Not applicable	No
IFS.SERVICE.HSM.PrimaryDevice	This property is not used.	Not applicable	Not applicable
IFS.SERVICE.JDBC.DefaultRowPrefetch	Number of result set rows prefetched. If set to null or 0, prefetches 10 rows. Do not change.	0	No
IFS.SERVICE.JDBC.DriverType	Specifies the JDBC driver type. Do not change.	oci8	No
IFS.SERVICE.JDBC.TracingEnabled	Sends JDBC debugging information to the standard output. Do not change.	false	No
IFS.SERVICE.SESSION.TransactionStackSize	The maximum number of nested transactions by the session.	100	No
IFS.SERVICE.LockTimeoutPeriod	The time period (in seconds) for a session to wait when attempting to lock database resources when performing an update operation. If unable to lock the required database resources within the time period indicated, the update operation will time out, and an exception will occur.	10	No
IFS.SERVICE.MaximumConcurrentSessions	Maximum number of Library sessions the service can support concurrently. Default of 0 means unlimited. This value determines how many Library sessions are available for outstanding user requests, across all users. It does not limit the number of users who can log in.	40 - Small 70 - Medium 200 - Large	No
IFS.SERVICE.OrphanSessionTimeoutPeriod	Number of seconds after which a session that no longer generates a heartbeat becomes an orphan. Set to 0 to disable orphan session timeout.	600	No
IFS.SERVICE.PollForEventsFromOtherServicesPeriod	Seconds between checks for incoming events from other services. Set to 0 to disable interservice event polling.	2	No

Table D-1 (Cont.) IFS.SERVICE.* Properties

Property	Description and Usage Notes	Default	Required?
IFS.SERVICE. ServiceKeepAliveEventPeriod	Seconds between service heartbeats. The Service Watchdog Agent detects services that cease to have a heartbeat, and cleans up information associated with the failed service in the Oracle Content DB repository. Set to 0 to disable the heartbeat.	60	No
IFS.SERVICE.SESSION.EventPoller	The event poller used by a session to generate the heartbeat of the session. Must be either oracle.ifs.beans.LibrarySessionEventPollerThreadPerProcess (recommended) or oracle.ifs.beans.LibrarySessionEventPollerThreadPerSession.	oracle.ifs.beans.LibrarySessionEventPollerThreadPerProcess	No
IFS.SERVICE.SESSION. EventPollerPeriod	The period, in milliseconds, of the session's heartbeat. In addition to indicating the health of the session to the service, the heartbeat allows an idle session to process events generated by other sessions or services.	2500	No
IFS.SERVICE.SESSION. DefaultSearchTimeoutPeriod	The period, in seconds, after which a search API call is terminated, even if incomplete. If a search times out in this manner, it is terminated and an exception occurs. The session performing the search remains valid. A value of 0 disables search timeouts.	60	No
IFS.SERVICE.SESSION. BEANSOBJECTCACHE.Size	The target maximum size of the bean-side session object cache, in LibraryObjects. The bean-side session object cache holds instances of oracle.ifs.beans.LibraryObject. If IFS.SERVICE.SESSION.SERVEROBJECTCACHE.IsUnbounded is false, this value is ignored and implicitly equal to IFS.SERVICE.SESSION.SERVEROBJECTCACHE.Size.	750	No
IFS.SERVICE.SESSION. FOLDERPATHCACHE.Enabled	Whether the session caches the resolution of folder paths.	true	No
IFS.SERVICE.SESSION. FOLDERPATHCACHE.Size	The absolute maximum size of the folder path cache of the session, in cached folder paths.	150	No
IFS.SERVICE.SESSION. FOLDERPATHCACHE.NormalTrigger	The cache size, in folder paths, at which the session's folder path cache schedules a low-priority purge of data that has not been recently used.	100	No
IFS.SERVICE.SESSION. FOLDERPATHCACHE.UrgentTrigger	The cache size, in folder paths, at which the folder path cache of the session schedules a high-priority purge of data that has not been recently used. Must be greater than IFS.SERVICE.SESSION.FOLDERPATHCACHE.NormalTrigger and less than IFS.SERVICE.SESSION.FOLDERPATHCACHE.Size.	110	No
IFS.SERVICE.SESSION. FOLDERPATHCACHE.PurgeTarget	The target cache size, in folder paths, on completion of a purge cycle. Must be less than IFS.SERVICE.SESSION.FOLDERPATHCACHE.NormalTrigger.	80	No

Table D-1 (Cont.) IFS.SERVICE.* Properties

Property	Description and Usage Notes	Default	Required?
IFS.SERVICE.SESSION.SERVEROBJECTCACHE.Size	The absolute maximum size of the server-side session object cache, in LibraryObjects. The server-side session object cache holds instances of oracle.ifs.server.S_LibraryObject and oracle.ifs.beans.LibraryObject.	750	No
IFS.SERVICE.SESSION.SERVEROBJECTCACHE.NormalTrigger	The cache size, in LibraryObjects, at which the session data caches schedule a low-priority purge of data that has not been recently used.	500	No
IFS.SERVICE.SESSION.SERVEROBJECTCACHE.UrgentTrigger	The cache size, in LibraryObjects, at which the session data caches schedule a high-priority purge of data that has not been recently used. Must be greater than IFS.SERVICE.SESSION.SERVEROBJECTCACHE.NormalTrigger.	550	No
IFS.SERVICE.SESSION.SERVEROBJECTCACHE.EmergencyTrigger	The cache size, in LibraryObjects, at which the session data caches perform an immediate purge of data that has not been recently used. Must be greater than IFS.SERVICE.SESSION.SERVEROBJECTCACHE.UrgentTrigger but less than IFS.SERVICE.SESSION.SERVEROBJECTCACHE.Size.	600	No
IFS.SERVICE.SESSION.SERVEROBJECTCACHE.PurgeTarget	The target cache size, in LibraryObjects, on completion of a purge cycle. Must be less than IFS.SERVICE.SESSION.SERVEROBJECTCACHE.NormalTrigger.	400	No
IFS.SERVICE.SessionOperationTimeoutPeriod	Number of seconds after which certain Oracle Content DB API calls are terminated, even if incomplete. If an operation times out in this manner, it is terminated, its transaction is terminated, and an exception occurs. The session performing the operation remains valid. Set to 0 to disable session operation timeout.	300	No
IFS.SERVICE.TRACING.ChannelCount	The number of trace logger channels. Oracle reserves channels 0 to TraceLogger.LAST_RESERVED_CHANNEL. See the Javadoc for class oracle.ifs.common.TraceLogger for a list of Oracle-defined channels.	50	No
IFS.SERVICE.TRACING.ServiceTraceType	The destination of trace data generated by a service. Must be TRACETYPE_NONE (disabled) or TRACETYPE_LOCAL (writes to a file on the local file system).	TRACETYPE_NONE	No
IFS.SERVICE.TRACING.ServerSessionTraceType	The destination of trace data generated by a server-side session. Must be TRACETYPE_NONE (disabled), TRACETYPE_LOCAL (writes to a file on the local file system), TRACETYPE_REMOTE (routes to the service's trace logger), or TRACETYPE_BOTH (writes to a file on the local file system and routes to the service's trace logger).	TRACETYPE_NONE	No

Table D-1 (Cont.) IFS.SERVICE.* Properties

Property	Description and Usage Notes	Default	Required?
IFS.SERVICE.TRACING. BeansSessionTraceType	The destination of trace data generated by a bean-side session. Must be TRACETYPE_NONE (disabled), TRACETYPE_LOCAL (writes to a file on the local file system), TRACETYPE_REMOTE (routes to the server-side session's trace logger), or TRACETYPE_BOTH (writes to a file on the local file system and routes to the server-side session's trace logger).	TRACETYPE_NONE	No
IFS.SERVICE.TRACING. TraceLevelChannel <i>n</i>	Tracing verbosity for trace channel <i>n</i> . Refer to the Javadoc for class <code>oracle.ifs.common.TraceLogger</code> for a list of Oracle-defined trace levels.	None	No
IFS.SERVICE.TRACING. DefaultTraceLevel	Default tracing verbosity for all trace channels. See <code>oracle.ifs.common.TraceLogger</code> Javadoc for a list of trace levels.	None	No
IFS.SERVICE. TransportEventsToOtherServices Period	Maximum length of time (seconds) that outgoing events are buffered before sending. Set to 0 to disable outgoing event buffer.	2	No

Server Configuration Properties

Each Oracle Content DB node can support multiple **servers**. These servers can be either protocol servers or agents:

- The protocol servers listen for requests from clients on a specific port and respond to requests according to the rules of the protocol specification.
- Agents perform operations periodically (time-based) or in response to events generated by other Oracle Content DB servers or processes (event-based). Although different agents can run on different nodes, each agent must run only on a single node, except the Service Warmup Agent and the Statistics Agent. These agents must be running on all nodes. Typically, most of the agents that come with the software must be run to ensure a stable system.

Each server is based on a particular **server configuration** that holds the default values used when the server is started for an Oracle Content DB node.

The properties listed in this appendix are all required for a protocol server or agent to run properly. When you install and configure an Oracle Content DB instance, the properties are configured using the default values shown in this appendix.

This appendix provides information about the following topics:

- [Shared Properties](#)
- [Background Request Agent](#)
- [Cleanup Agent](#)
- [Content Agent](#)
- [Content Garbage Collection Agent](#)
- [Dangling Object AV Cleanup Agent](#)
- [Event Exchanger Agent](#)
- [Expiration Agent](#)
- [Folder Index Agent](#)
- [Folder Index Analyzer Agent](#)
- [Garbage Collection Agent](#)
- [HTTP Server](#)
- [Inbound Queue Listener Agent](#)
- [Lock Expiration Agent](#)
- [Most Recent Doc Agent](#)

- [Quota Agent](#)
- [Read Document Agent](#)
- [Reassign Quota Agent](#)
- [Refresh Security Agent](#)
- [Service Warmup Agent](#)
- [Service Watchdog Agent](#)
- [Statistics Agent](#)
- [User Connect Agent](#)
- [Version Purge Agent](#)
- [Virus Repair Agent](#)

Shared Properties

Table E-1 defines server configuration properties that are shared among more than one server or agent.

Table E-1 Shared Properties

Property	Description and Usage Notes	Default
IFS.SERVER.Class	The class used to instantiate the server.	Default varies from server to server.
IFS.SERVER.SESSION.LOCALE.Country	Default country to be used in session localizer.	US
IFS.SERVER.SESSION.LOCALE.Language	Default language to be used in session localizer.	en
IFS.SERVER.SESSION.User	User name for server session. Must be a user with Oracle Content DB administrator privileges.	system
IFS.SERVER.TIMER.ActivationPeriod	Time interval for when the agent runs again. Specified as a number followed by a time unit, such as 4h to indicate a 4-hour interval. Time units are: h=hours, m=minutes, s=seconds	Default varies from server to server.
IFS.SERVER.TIMER.InitialDelay	The delay before the first time interval, relative to when the server is started. This property is ignored if a value is specified for IFS.SERVER.TIMER.InitialTimeOfDay.	Default varies from server to server.
IFS.SERVER.TIMER.InitialTimeOfDay	The first timer event. Set time based on a 24-hour clock.	00:15:00

Background Request Agent

The Background Request Agent is an event-based agent that reacts to requests placed by users for operations that take a long time to perform, such as modifying the Sharing properties for the Oracle Content DB Site. The agent asynchronously performs the requested operations to avoid performance problems.

The default name for this server configuration is:

BackgroundRequestAgentConfiguration

Table E-2 lists the properties for the Background Request Agent.

Table E–2 Background Request Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.BACKGROUNDREQUESTAGENT.EventBatchSize	The maximum number of events processed in a single iteration of this agent.	5000

Cleanup Agent

The Cleanup Agent performs a variety of cleaning tasks on a periodic basis, such as deleting content in the Archive that has passed the expiration period set by the Content Administrator. Each of these tasks has a corresponding property called an Activation Multiplier that controls how often the task is performed.

The Activation Multiplier works in conjunction with the IFS.SERVER.TIMER.ActivationPeriod property. For example, if IFS.SERVER.TIMER.ActivationPeriod is set to 1h, and ECM.AGENT.CLEANUPAGENT.EMPTYARCHIVE.ActivationMultiplier is set to 8, then the Cleanup Agent will delete expired content in the Archive every 8 hours.

The descriptions and notes provided in [Table E–3](#) assume an ActivationPeriod of 1 hour, which is the default for this agent.

The default name for this server configuration is:

CleanupAgentConfiguration

Table E–3 Cleanup Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.CLEANUPAGENT.ARCHIVETOBFILE.ActivationMultiplier	Controls how often content in the Archive is moved to a BFILE. This action is only performed when BFILE archiving has been enabled. See "Setting Up Data Archiving" on page 4-6 for more information.	24
ECM.AGENT.CLEANUPAGENT.BaseTimeOfDay	The time of day from which all intervals for this agent are based. This property determines the time at which tasks will be run that perform only once every 24 hours, and the relative time for tasks performed only a few times in a 24-hour period. For example, if a task has an ActivationMultiplier of 8 and the BaseTimeOfDay is set to 20:15:00, that task will run at 20:15, 4:15, and 12:15.	20:15:00
ECM.AGENT.CLEANUPAGENT.CALCULATEARCHIVEQUOTA.ActivationMultiplier	Controls how often the quota used by files in the Archive for the Site is recalculated.	4
ECM.AGENT.CLEANUPAGENT.CALCULATEDOMAINQUOTA.ActivationMultiplier	Controls how often the total quota used by all files located in Libraries for the Site is recalculated.	1
ECM.AGENT.CLEANUPAGENT.CLEARLINKREFERENCE.ActivationMultiplier	Controls how often links that reference inaccessible items have their internal representation optimized.	12
ECM.AGENT.CLEANUPAGENT.DELETEDOMAINADMINUSER.ActivationMultiplier	Controls how often the administration mode representation for users is removed from the system, for users whose application administration access has been disabled for a sufficient period of time. This time period is controlled by the ECM.AGENT.CLEANUPAGENT.DELETEDOMAINADMINUSER.InactivityPeriod property.	12
ECM.AGENT.CLEANUPAGENT.DELETEDOMAINADMINUSER.InactivityPeriod	The amount of time the administration representation for a user remains after the user loses all application administration rights, before that user is removed from the system.	24h

Table E-3 (Cont.) Cleanup Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.CLEANUPAGENT.DELETEGRANT.ActivationMultiplier	Controls how often security configurations are optimized to reflect users or groups that have been removed from the system.	24
ECM.AGENT.CLEANUPAGENT.DELETETRASHACL.ActivationMultiplier	Controls how often unused security configurations for items in Trash folders are removed from the system.	24
ECM.AGENT.CLEANUPAGENT.DELETETWORKFLOWUSER.ActivationMultiplier	Controls how often workflow components are optimized with respect to users that have been removed from the system.	12
ECM.AGENT.CLEANUPAGENT.DISABLEDOMAINADMINUSER.ActivationMultiplier	Controls how often verification is performed for administrative users to ensure that the users still have administration mode access. For users that have lost all administration mode access, the administration representation of the user is disabled, and remains disabled until the user is again granted application administration access, or is removed from the system.	1
ECM.AGENT.CLEANUPAGENT.EMPTYARCHIVE.ActivationMultiplier	Controls how often content that has passed the expiration period set by the Content Administrator is deleted from the Archive.	24
ECM.AGENT.CLEANUPAGENT.EMPTYTRASH.ActivationMultiplier	Controls how often Trash folders are emptied if they were configured to be automatically emptied.	4
ECM.AGENT.CLEANUPAGENT.ISSUEDOMAINQUOTAWARNING.ActivationMultiplier	Controls how often e-mail notification warnings are sent when the quota used by the Site is at or near the allocated quota limit for that Site. E-mail notifications are sent to any users of the Site with the Quota Administrator role, as well as to the administrator e-mail address specified in the IFS.DOMAIN.EMAIL.AdministratorAddress domain property.	12
ECM.AGENT.CLEANUPAGENT.ISSUEDOMAINQUOTAWARNING.ConsumptionPercentageThreshold	Specifies how close the used quota for the Site needs to be to the allocation limit for a Site quota warning to be issued. The value is specified as a percentage of the Site quota allocation.	95
ECM.AGENT.CLEANUPAGENT.ISSUEDOMAINQUOTAWARNING.IncludeArchiveConsumption	Specifies whether documents in the Archive for the Site are considered to count against the quota used for the Site.	true
ECM.AGENT.CLEANUPAGENT.PURGEDELETEDWORKSPACE.ActivationMultiplier	Controls how often Libraries that have been deleted and that are unreferenced in the Archive are permanently removed from the system.	24

Content Agent

The Content Agent controls the management of document content when BFILE aging has been set up. When BFILE aging has been enabled, the Content Agent moves content to a BFILE if it has not been accessed after the retention period.

The Content Agent is one of the few agents that does not run by default. If you want to use BFILE aging in Oracle Content DB, you must first enable BFILE aging, then activate this agent by modifying the node configuration for the node where you want the agent to run. See "[Managing Storage Options](#)" on page 4-5 for information about setting up BFILE aging and activating the Content Agent.

The default name for this server configuration is:

ContentAgentConfiguration

Table E-4 lists the properties for the Content Agent.

Table E-4 Content Agent Configuration Properties

Property	Description and Usage Notes	Default
<code>IFS.SERVER.AGENT.CONTENTAGENT.ContentToBfileManager</code>	The fully qualified classname of the <code>ContentToBfileManager</code> interface.	<code>oracle.ifs.management.servers.content.IfsContentToBfileManager</code>
<code>IFS.SERVER.AGENT.CONTENTAGENT.MaxFilesPerFolder</code>	For every relative path created, the maximum number of files that can be moved to a folder.	500
<code>IFS.SERVER.AGENT.CONTENTAGENT.MaxFoldersPerActivationPeriod</code>	The maximum number of folders created when the Content Agent runs.	20
<code>IFS.SERVER.AGENT.CONTENTAGENT.RetentionPeriod</code>	How long a file may be kept in the database as a LOB if it is not accessed.	30d

Content Garbage Collection Agent

File attributes and content are stored separately. For performance reasons, the content of a document is not deleted when the document is deleted. The Content Garbage Collection Agent deletes the unreferenced content. Like many agents, this agent runs at a specific time that is specified in the `IFS.SERVER.TIMER.InitialTimeOfDay` and `IFS.SERVER.TIMER.ActivationPeriod` properties.

The default name for this server configuration is:

`ContentGarbageCollectionAgentConfiguration`

Table E-5 lists the properties for the Content Garbage Collection Agent.

Table E-5 Content Garbage Collection Agent Configuration Properties

Property	Description and Usage Notes	Default
<code>IFS.SERVER.AGENT.CONTENTGARBAGECOLLECTIONAGENT.FilteredContentRemovalPeriod</code>	Amount of time filtered content is kept in the system before it is deleted. HTML-generated rendition of content is an example of filtered content. Unit of measure is seconds.	3600
<code>IFS.SERVER.AGENT.CONTENTGARBAGECOLLECTIONAGENT.FreedContentBatchSize</code>	The maximum number of unreferenced <code>ContentObjects</code> that are freed in a single iteration of this agent.	10000

Dangling Object AV Cleanup Agent

Similar to the Garbage Collection Agent, the Dangling Object AV Cleanup Agent removes orphaned object type references and identifies all invalid object references, such as references to objects that no longer exist, and sets these references to null for array type attributes and zero for scalar attributes. For example, this agent cleans up the owner attribute of a document pointing to a directory object that was deleted and is no longer valid.

The default name for this server configuration is:

`DanglingObjectAVCleanupAgentConfiguration`

Table E-6 lists the properties for the Dangling Object AV Cleanup Agent.

Table E–6 Dangling Object AV Cleanup Agent Configuration Properties

Property	Description and Usage Notes	Default
IFS.SERVICE.AGENTS.DANGLINGOBJECTAVCLEANUPAGENT.ExcludedAttributeList	A list of attributes for which invalid references to LibraryObjects are not cleaned up. Do not delete the default values, so the Garbage Collection Agent can handle deleted users correctly. Add additional attributes as needed.	AUDITENTRY PUBLICOBJECT:OWNER PUBLICOBJECT:DELETOR PUBLICOBJECT:CREATOR PUBLICOBJECT:LASTMODIFIER VERSIONSERIES:RESERVOR

Event Exchanger Agent

The Event Exchanger Agent periodically purges expired events from the event queue.

The default name for this server configuration is:

EventExchangerAgentConfiguration

[Table E–7](#) lists the properties for the Event Exchanger Agent.

Table E–7 Event Exchanger Agent Configuration Properties

Property	Description and Usage Note	Default
IFS.SERVICE.EventLifespan	The time, in seconds, after which an event is assumed to have been delivered and become eligible for purging.	1800

Expiration Agent

All public objects have an attribute called ExpirationDate. When this date passes, the public objects are automatically deleted. This is handled by the Expiration Agent, which periodically deletes expired objects. If the expiration date of a public object passes, the agent deletes the public object. Like many agents, this agent runs at a specific time that is specified in the IFS.SERVICE.TIMER.InitialTimeOfDay and IFS.SERVICE.TIMER.ActivationPeriod properties.

The default name for this server configuration is:

ExpirationAgentConfiguration

Folder Index Agent

The Folder Index Agent handles additional folder index functions not covered by the Folder Index Analyzer Agent. See the following section for more information about the Folder Index Analyzer Agent.

The default name for this server configuration is:

FolderIndexAgentConfiguration

[Table E–8](#) lists the properties for the Folder Index Agent.

Table E–8 Folder Index Agent Configuration Properties

Property	Description and Usage Notes	Default
IFS.SERVICE.AGENTS.FOLDERINDEXAGENT.MaxDeferredUpdates	The maximum number of deferred updates processed in a single iteration of this agent.	5000

Folder Index Analyzer Agent

Oracle Content DB uses an internal mechanism called the folder index to speed up folder-restricted queries. This index is modified every time the folder hierarchy gets changed, to reflect the up-to-date folder hierarchy. However, certain forms of file links may leave the folder index in a less than optimal state. The Folder Index Analyzer Agent runs periodically to detect and correct these states, and returns the folder index to an optimal state.

The default name for this server configuration is:

FolderIndexAnalyzerAgentConfiguration

[Table E-9](#) lists the properties for the Folder Index Analyzer Agent. Never modify these values.

Table E-9 Folder Index Analyzer Agent Configuration Properties

Property	Description and Usage Notes	Default
IFS.SERVER.AGENTS.FOLDERINDEXANALYZERAGENT.MaxParentsThreshold	The threshold for the maximum number of parents after which the folder index is considered less than optimal. This condition is ANDed with the MaxChildrenThreshold.	10
IFS.SERVER.AGENTS.FOLDERINDEXANALYZERAGENT.MaxChildrenThreshold	The threshold for the maximum number of children after which the folder index is considered less than optimal. This condition is ANDed with the MaxParentsThreshold.	10

Garbage Collection Agent

The Garbage Collection Agent fixes invalid public object owners, creators, and modifiers. For example, a document is created and modified by jsmith. The creator, owner, and last modifier attribute of document are set to the object ID of jsmith. If jsmith is deleted, then the attribute value becomes invalid. The agent replaces these invalid attribute values with the ID of the replacement owner, creator, or modifier specified in the server configuration properties.

The default name for this server configuration is:

GarbageCollectionAgentConfiguration

[Table E-10](#) lists the properties for the Garbage Collection Agent.

Table E-10 Garbage Collection Agent Configuration Properties

Property	Description and Usage Notes	Default
IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementOwner	User to be replaced as owner. Modify as needed.	system
IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementCreator	User to be replaced as creator. Modify as needed.	system
IFS.SERVER.AGENT.GARBAGECOLLECTIONAGENT.ReplacementModifier	User to be replaced as modifier. Modify as needed.	system

HTTP Server

The Oracle Content DB HTTP server lets users access the Oracle Content DB Web client. It also contains properties for [WebDAV](#) access.

The default name of this server configuration is:

EcmHttpServerConfiguration

Table E-11 lists the properties for the Oracle Content DB HTTP server.

Table E-11 HTTP Server Configuration Properties

Property	Description and Usage Notes	Default
IFS.SERVER.PROTOCOL.DAV.Browse.Enabled	If set to true, WebDAV will return a directory listing when a user tries to GET a folder through the WebDAV servlet. If set to false, the user is redirected to the Web interface.	true
IFS.SERVER.PROTOCOL.DAV.DigestNonceTimeout	Nonce refers to the challenge used by WebDAV in digest authentication. After using a nonce to authenticate, the client can continue accessing the server until the timeout period is reached, at which point the server sends another challenge and the client must authenticate again. Unit of measure is minutes.	10
IFS.SERVER.PROTOCOL.DAV.Locks.Timeout.Min	The minimum timeout value, in seconds, that a client can request when acquiring a lock. This value prevents clients from asking for short timeouts, then refreshing frequently, which increases server load.	601
IFS.SERVER.PROTOCOL.DAV.Propfind.Infinity.Enabled	Whether to allow depth-infinity PROPFIND requests on collections, which can be extremely resource-intensive.	true
IFS.SERVER.PROTOCOL.DAV.Propfind.Infinity.MaxResponses	The maximum number of results to collect for a depth-infinity PROPFIND on a collection before rejecting the request. This limit only applies to depth-infinity PROPFIND requests; depth-one requests are not affected. Set to -1 to collect unlimited results. This property is ignored if IFS.SERVER.PROTOCOL.DAV.Propfind.Infinity.Enabled is set to false.	1001
IFS.SERVER.PROTOCOL.DAV.Welcome	The array of welcome document names that are served up if a GET is done on a directory containing one of these documents. Typically used so that index.html will be served automatically when the directory is requested. To disable this feature, set to an empty array.	index.html index.htm

Renaming the Oracle Content DB HTTP Server

Do not change the name of the `EcmHttpServer`. If you change the server name, you will not be able to access Oracle Content DB through the Web client.

If you must change the server name, you must also change the name in the `web.xml` configuration file. To change the server name:

1. Rename the server using the Application Server Control.
2. Edit `web.xml`, located in the following directory:

`ORACLE_HOME/j2ee/OC4J_Content/applications/content/content/WEB-INF`

Look for the following lines of code, and replace the value for `<param-value>`:

```
<init-param>
  <param-name>IFS.SERVER.PROTOCOL.DAV.IfsServer.Name</param-name>
  <param-value>EcmHttpServer</param-value>
</init-param>
```

3. Save the file.
4. Restart the OC4J instance.

Inbound Queue Listener Agent

The Inbound Queue Listener Agent is a time-based agent that polls all of the inbound queues periodically so that Oracle Content DB can act upon the messages placed on inbound queues. The Inbound Queue Listener Agent can dequeue a message and delegate the work of processing to the message object itself.

The default name for this server configuration is:

`InboundQueueListenerAgentConfiguration`

[Table E-12](#) lists the properties for the Inbound Queue Listener Agent.

Table E-12 Inbound Queue Listener Agent Configuration Properties

Property	Description and Usage Notes	Default
<code>IFS.SERVER.AGENT.INBOUNDQUEUELISTENERAGENT.Queues</code>	Holds a list of queues on which the agent will listen.	<code>IFS_IN</code> <code>IFS_BPEL_IN</code>

Lock Expiration Agent

The Lock Expiration Agent is a time-based agent that releases locks that are timed out. The agent needs to be running at all times for the automatic expiration function of the lock to work.

The default name for this server configuration is:

`LockExpirationAgentConfiguration`

Most Recent Doc Agent

The Most Recent Doc Agent is an event-based agent that reacts to documents that have been uploaded or accessed by each user. The information provided by the agent is used whenever a user accesses My Recent Documents.

The default name for this server configuration is:

`MostRecentDocAgentConfiguration`

[Table E-13](#) lists the properties for the Most Recent Doc Agent.

Table E-13 Most Recent Doc Agent Configuration Properties

Property	Description and Usage Notes	Default
<code>ECM.AGENT.MOSTRECENTDOCAGENT.EventBatchSize</code>	The maximum number of events processed in a single iteration of this agent.	5000

Quota Agent

The Quota Agent is triggered by an event to compute the quota used for Libraries. This agent also checks all active Libraries periodically, according to a specified timer period. The agent updates the storage used by the Library. When the storage used is over the allocated quota, users of the Library will not be able to add any more documents to that Library. Documents in Trash count toward the quota for a Library.

The quota for a Library is calculated based on the content already used. This means that a Library will go over quota when a user of that Library adds the final file that pushes the storage used over the storage limit. When you set the allocated quota for a Library, remember that the last file the user puts in the Library must go over quota before being denied.

Quotas will not be enforced if:

- The Quota Agent has not been started or is not running.
- The quota for a Library has not been enabled.

The default name for this server configuration is:

QuotaAgentConfiguration

Read Document Agent

The Read Document Agent is an event-based agent that reacts to documents read by users, by triggering a custom workflow if one is configured for the document that is read.

If no custom workflow is configured for the Read Document operation on the folders where the documents are read, the agent takes the action of moving the **BFILE** content of any recently read document back into a **LOB**. Documents are moved to BFILES by the Content Agent; see "[Content Agent](#)" on page E-4 for more information.

The default name for this server configuration is:

ReadDocumentAgentConfiguration

[Table E-14](#) lists the properties for the Read Document Agent.

Table E-14 Read Document Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.READDOCUMENTAGENT.EventBatchSize	The maximum number of events processed in a single iteration of this agent.	5000

Reassign Quota Agent

The Reassign Quota agent is an event-based agent that adjusts the quota charged for content in the system when content is moved between Libraries, often a time-consuming task.

The default name for this server configuration is:

ReassignQuotaAgentConfiguration

[Table E-15](#) lists the properties for the Reassign Quota Agent.

Table E-15 Reassign Quota Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.REASSIGNQUOTAAGENT.EventBatchSize	The maximum number of events processed in a single iteration of this agent.	5000

Refresh Security Agent

The Refresh Security Agent is an event-based agent that reacts to changes in grants applied at the Site or Container level, and modifies the security applied lower in the folder hierarchy accordingly, if necessary.

The default name for this server configuration is:

RefreshSecurityAgentConfiguration

[Table E-16](#) lists the properties for the Refresh Security Agent.

Table E-16 Refresh Security Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.REFRESHSECURITYAGENT.EventBatchSize	The maximum number of events processed in a single iteration of this agent.	5000

Service Warmup Agent

When a node is started, the Service Warmup Agent automatically preloads the data cache of the service. All properties for this agent are required. Unlike most other agents, this agent is configured to run separately on each node.

The default name for this server configuration is:

ServiceWarmupAgentConfiguration

[Table E-17](#) lists the properties for the Service Warmup Agent.

Table E-17 Service Warmup Agent Configuration Properties

Property	Description and Usage Notes	Default
IFS.SERVER.AGENT.SERVICEWARMUP.WarmupAcls	If set to true, preloads ACL collection.	false
IFS.SERVER.AGENT.SERVICEWARMUP.WarmupFormats	If set to true, preloads format collection.	true
IFS.SERVER.AGENT.SERVICEWARMUP.WarmupMedias	If set to true, preloads Media collection.	true
IFS.SERVER.AGENT.SERVICEWARMUP.WarmupSetAdmin	Whether the preloading is done in administration mode.	true
IFS.SERVER.AGENT.SERVICEWARMUP.WarmupUsers	If set to true, preloads user collection.	false

Service Watchdog Agent

The Service Watchdog Agent cleans up after Oracle Content DB services that do not shut down cleanly.

The default name for this server configuration is:

ServiceWatchdogAgentConfiguration

[Table E-18](#) lists the properties for the Service Watchdog Agent.

Table E-18 Service Watchdog Agent Configuration Properties

Property	Description and Usage Notes	Default
IFS.SERVER.AGENT.SERVICEWATCHDOGAGENT.ServiceTimeoutPeriod	The number of seconds after which a service is considered inactive. When a service becomes inactive, it is eligible for cleanup by the Service Watchdog Agent.	120

Statistics Agent

The Statistics agent is a time-based agent that gathers statistics pertaining to service activity on the node where the agent is running. Unlike most other agents, this agent is configured to run separately on each node, so that statistics are gathered independently for each node. The properties of the agent determine whether the statistics are logged, and whether they are written to a document stored in the Oracle Content DB repository.

The default name for this server configuration is:

StatisticsAgentConfiguration

Table E-19 lists the properties for the Statistics Agent.

Table E-19 Statistics Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.STATISTICSAGENT.CreateStatisticsDocument	Specifies whether an HTML document should be created, whose content is the currently gathered statistics. The name for this file is automatically generated and appears as <i>node_name_log.html</i> .	false
ECM.AGENT.STATISTICSAGENT.LogStatistics	If set to true, the currently gathered statistics are sent to the node or application log.	true
ECM.AGENT.STATISTICSAGENT.StatisticsFolderPath	The path within the Oracle Content DB folder hierarchy where the statistics document should be created. The path must refer to a Library or a folder within a Library. Do not include a file name as part of this path; the statistics document file name is autogenerated. If the folder where the statistics file resides does not have a versioning policy set on it, the file will be overwritten every time the agent logs statistics. You should set the folder versioning policy to Auto Versioning or Manual Versioning so that a new version is generated each time the agent logs statistics. When you set the versioning policy, set the Maximum number of versions to keep to a high number to ensure that statistics are kept for an adequate time period. For example, if you keep the activation period for this agent at 15 minutes (the default), you would need 96 versions in order to retain statistics for a 24-hour period.	Not applicable

User Connect Agent

The User Connect Agent is an event-based agent that updates the user preferences of active users. A user is considered active if they logged in to Oracle Content DB during the last Activation Period.

The default name for this server configuration is:

UserConnectAgentConfiguration

Table E-20 lists the properties for the User Connect Agent.

Table E-20 User Connect Agent Configuration Properties

Property	Description and Usage Notes	Default
ECM.AGENT.USERCONNECTAGENT.EventBatchSize	The maximum number of events processed in a single iteration of this agent.	5000

Version Purge Agent

The Version Purge agent is an event-based agent that purges versioned documents that have exceeded the version limit specified by the Versioning Configuration in effect for the documents. The purged versions are moved to the associated Trash folder.

The default name for this server configuration is:

VersionPurgeAgentConfiguration

[Table E-21](#) lists the properties for the Version Purge Agent.

Table E-21 *Version Purge Agent Configuration Properties*

Property	Description and Usage Notes	Default
ECM.AGENT.VERSIONPURGEAGENT.EventBatchSize	The maximum number of events processed in a single iteration of this agent.	5000

Virus Repair Agent

The Virus Repair Agent is responsible for repairing files that have been infected with a virus, and for retrieving the latest virus definitions. Whenever the agent becomes active, it will poll the SAVSE server for updated virus definitions, and then attempt to repair the quarantined files. The agent will not try to repair the following files:

- Files that have exceeded the maximum number of repair attempts
- Files that have already experienced repair attempts using the current virus definitions

The default name for this server configuration is:

VirusRepairAgentConfiguration

Oracle Content DB Globalization Support

Oracle Content DB globalization support lets users store and search documents of heterogeneous character sets and languages in a single Oracle Content DB instance. The globalization infrastructure ensures that the resource strings, error messages, sort order, date, time, numeric, and calendar conventions adapt automatically to any native language and locale.

Globalization support is provided in the Oracle Content DB repository so that the other dependent processes, such as the protocol servers, can share and use this support. The major globalization goal for the repository is to ensure efficient storage of documents of heterogeneous character sets and languages, and to allow effective update, retrieval, and search operations on these documents.

This appendix provides information about the following topics:

- [How to Choose the Database Character Set for Oracle Content DB](#)
- [How to Ensure Documents Are Properly Indexed in Oracle Content DB](#)
- [Globalization and the Oracle Content DB Protocols](#)
- [Character Sets Supported in Oracle Content DB](#)
- [Document Languages Supported in Oracle Content DB](#)

How to Choose the Database Character Set for Oracle Content DB

In the repository, all metadata strings, such as the name of the document or the description, are stored in the VARCHAR2 data type of Oracle Database. Strings stored in this data type are encoded in the database character set specified when a database is created. The document itself, however, is unstructured data and stored in one of the large object data types of Oracle Database, particularly the BLOB data type. The BLOB data type stores content as is, avoiding any character set conversion on document content. The LONG and CLOB data types store content in the database character set, which requires character set conversion. Conversions can compromise the data integrity and have the potential to convert incorrectly or lose characters.

The full-text search index built on the document content is encoded in the database character set. When the content of a document is indexed, the BLOB data is converted from the character set of the content to the database character set for creation of the index text tokens. If the character set of the content is not a subset of the database character set, then the conversion will yield garbage tokens. For example, a database character set of ISO-8859-1 (Western European languages) will not be able to index correctly a Shift-JIS (Japanese) document. To be able to search content effectively, the character set of the documents stored by the users must be considered when selecting the database character set.

If your Oracle Content DB instance will contain multilingual documents, AL32UTF-8 is the recommended database character set. AL32UTF-8 supports characters defined in the Unicode standard. The Unicode standard solves the problem of many different languages in the same application or database. Unicode is a single, global character set that contains all major living scripts and conforms to international standards. Unicode provides a unique code value for every character, regardless of the platform, program, or language. AL32UTF-8 is the 8-bit encoding of Unicode. It is a variable-width encoding and a strict superset of ASCII. One Unicode character can be 1 byte, 2 bytes, 3 bytes, or 4 bytes in AL32UTF-8 encoding. Characters from the European scripts are represented in either 1 or 2 bytes. Characters from most Asian scripts are represented in 3 bytes. Supplementary characters are represented in 4 bytes. By using a Unicode-based file system, document content and metadata of different languages can be shared by users with different language preferences in one system.

How to Ensure Documents Are Properly Indexed in Oracle Content DB

To support documents in different character sets and languages in a single file system, the repository associates two globalization attributes with each document. They are the character set and language attributes.

Character Set

The character set of a document is used in several situations. When the document content is rendered to a file, the character set of the document is used as the character encoding of the file. When the document is displayed in the browser, the character set of the document is set in the HTTP content-type header. Finally, when a full-text search is built on a text document, Oracle Text uses the character set of the document to convert the data into the database character set before building the index. When a character set is updated, the content is reindexed.

If no character set is specified when a document is inserted, the repository determines a default character set by using the character set of the user's LibrarySession stored in the Localizer object. This is obtained from the PrimaryUserProfile information of the user when the LibrarySession of the user is initialized.

Language

The language of a document is used as a criterion to limit the search for documents of a particular language. It is also used to build a full-text search index on the document with Oracle Text. The multilexer feature of Oracle Text uses the language to identify the specific lexer to parse the document for searchable words. The language-specific lexers need to be defined and associated with a language before the index is built.

[Table F-1](#) describes the language-specific lexers.

Table F-1 Language-Specific Lexers

Language	Lexer	Lexer Option
Brazilian Portuguese	BASIC_LEXER	BASE LETTER
Canadian French	BASIC_LEXER	BASE LETTER INDEX THEME
Danish	BASIC_LEXER	BASE LETTER DANISH ALTERNATE SPELLING
Dutch	BASIC_LEXER	BASE LETTER
Finnish	BASIC_LEXER	BASE LETTER

Table F-1 (Cont.) Language-Specific Lexers

Language	Lexer	Lexer Option
French	BASIC_LEXER	BASE LETTER INDEX THEME THEME LANGUAGE=FRENCH
German	BASIC_LEXER	BASE LETTER GERMAN ALTERNATE SPELLING
Italian	BASIC_LEXER	BASE LETTER
Japanese	JAPANESE_VGRAM_LEXER	Not applicable
Korean	KOREAN_LEXER	Not applicable
Latin American	BASIC_LEXER	BASE LETTER
Spanish Portuguese	BASIC_LEXER	BASE LETTER
Simplified Chinese	CHINES_VGRAM_LEXER	Not applicable
Swedish	BASIC_LEXER	BASE LETTER SWEDISH ALTERNATE SPELLING
Tradition Chinese	CHINESE_VGRAM_LEXER	Not applicable
Others	BASIC_LEXER	INDEX THEME THEME LANGUAGE=ENGLISH INDEX TEXT

The BASIC_LEXER is used for single-byte languages using white space as a word separator. Asian language lexers cannot use white space as word separators. Instead, they use a V-gram algorithm to parse the documents for searchable keys. Languages that are not supported by Oracle Text are parsed as English. Oracle Content DB uses the multilexer feature of Oracle Text. It is a global lexer that contains German, Danish, Swedish, Japanese, Simplified Chinese, Traditional Chinese, and Korean sublexers.

If no language is specified when a document is inserted, the repository determines a default language as follows:

1. If the character set has been set, the language can most likely be obtained from a best-guess algorithm based on the character set value. For example, a document with a character set of Shift-JIS will most likely be in Japanese.
2. The default language is obtained from the Localizer of the user's LibrarySession. During initialization of the LibrarySession, the default language is obtained from the PrimaryUserProfile of the user.
3. The default language and default character set are specified when a new user is created in Oracle Internet Directory.

Oracle Content DB identifies languages using Oracle Globalization Support language abbreviations. See "[Document Languages Supported in Oracle Content DB](#)" on page F-6 for a list of Oracle Content DB-supported languages.

Globalization and the Oracle Content DB Protocols

Some protocols do not support multibyte user names. Access through WebDAV and HTTP is not available for user names that contain multibyte characters. In addition, some protocols require that user passwords be in ASCII format.

Character Sets Supported in Oracle Content DB

Table F–2 is a summary of the character sets supported in Oracle Content DB.

Table F–2 Character Sets Supported in Oracle Content DB

Language	IANA Preferred MIME Character Set	IANA Additional Aliases	Java Encodings	Oracle Character Set
Arabic (ISO)	iso-8859-6	ISO_8859-6:1987, iso-ir-127, ISO_8859-6, ECMA-114, ASMO-708, arabic, csISOLatinArabic	ISO8859_6	AR8ISO8859P6
Arabic (Windows)	windows-1256	none	Cp1256	AR8MSWIN1256
Baltic (ISO)	iso-8859-4	csISOLatin4, iso-ir-110, ISO_8859-4, ISO_8859-4:1988, I4, latin4	ISO8859_4	NEE8ISO8859P4
Baltic (Windows)	windows-1257	none	Cp1257	BLT8MSWIN1257
Central European (DOS)	ibm852	cp852, 852, csPcp852	Cp852	EE8PC852
Central European (ISO)	iso-8859-2	csISOLatin2, iso-ir-101, iso8859-2, iso_8859-2, iso_8859-2:1987, I2, latin2	ISO8859_2	EE8ISO8859P2
Central European (Windows)	windows-1250	x-cp1250	Cp1250	EE8MSWIN1250
Chinese	iso-2022-cn It is not defined in IANA, but use in MIME documents.	csISO2022CN	ISO2022CN	ISO2022-CN
Chinese Simplified (GB2312)	gb2312	chinese, csGB2312, csISO58GB231280, GB2312, GB_2312-80, iso-ir-58	EUC_CN	ZHS16CGB231280
Chinese Simplified (GB18030)	GB18030	none	GB18030	ZHS32GB18030
Chinese Simplified (Windows)	GBK	windows-936	GBK	ZHS16GBK
Chinese Traditional	big5	csbig5, x-x-big5	Big5	ZHT16BIG5
Chinese Traditional	windows-950	none	MS950	ZHT16MSWIN950
Chinese Traditional (EUC-TW)	EUC-TW	none	EUC_TW	ZHT32EUC
Chinese Traditional (Big5-HKSCS)	Big5-HKSCS	none	Big5_HKSCS	ZHT16HKSCS
Cyrillic (DOS)	ibm866	cp866, 866, csIBM866	Cp866	RU8PC866
Cyrillic (ISO)	iso-8859-5	csISOLatinCyrillic, cyrillic, iso-ir-144, ISO_8859-5, ISO_8859-5:1988	ISO8859_5	CL8ISO8859P5

Table F–2 (Cont.) Character Sets Supported in Oracle Content DB

Language	IANA Preferred MIME Character Set	IANA Additional Aliases	Java Encodings	Oracle Character Set
Cyrillic (KOI8-R)	koi8-r	csKOI8R, koi	KOI8_R	CL8KOI8R
Cyrillic Alphabet (Windows)	windows-1251	x-cp1251	Cp1251	CL8MSWIN1251
Greek (ISO)	iso-8859-7	csISOLatinGreek, ECMA-118, ELOT_928, greek, greek8, iso-ir-126, ISO_8859-7, ISO_8859-7:1987, csISOLatinGreek	ISO8859_7	EL8ISO8859P7
Greek (Windows)	windows-1253	none	Cp1253	EL8MSWIN1253
Hebrew (ISO)	iso-8859-8	csISOLatinHebrew, hebrew, iso-ir-138, ISO_8859-8, visual, ISO-8859-8 Visual, ISO_8859-8:1988	ISO8859_8	IW8ISO8859P8
Hebrew (Windows)	windows-1255	none	Cp1255	IW8MSWIN1255
Japanese (JIS)	iso-2022-jp	csISO2022JP	ISO2022JP	ISO2022-JP
Japanese (EUC)	euc-jp	csEUCPkdFmtJapanese, Extended_UNIX_Code_Packed_Format_for_Japanese, x-euc, x-euc-jp	EUC_JP	JA16EUC
Japanese (Shift-JIS)	shift_jis	csShiftJIS, csWindows31J, ms_Kanji, shift-jis, x-ms-cp932, x-sjis	MS932	JA16SJIS
Korean	ks_c_5601-1987	csKSC56011987, korean, ks_c_5601, euc-kr, csEUCKR	EUC_KR	KO16KSC5601
Korean (ISO)	iso-2022-kr	csISO2022KR	ISO2022KR	ISO2022-KR
Korean (Windows)	windows-949	none	MS949	KO16MSWIN949
South European (ISO)	iso-8859-3	ISO_8859-3, ISO_8859-3:1988, iso-ir-109, latin3, l3, csISOLatin3	ISO8859_3	SE8ISO8859P3
Thai	TIS-620	windows-874	TIS620	TH8TISASCII
Turkish (Windows)	windows-1254	none	Cp1254	TR8MSWIN1254
Turkish (ISO)	iso-8859-9	latin5, l5, csISOLatin5, ISO_8859-9, iso-ir-148, ISO_8859-9:1989	ISO8859_9	WE8ISO8859P9
Universal (UTF-8)	utf-8	unicode-1-1-utf-8, unicode-2-0-utf-8, x-unicode-2-0-utf-8	UTF8	UTF8
Unicode (UTF-16BE)	UTF-16BE	none	UTF-16BE	AL16UTF16
Unicode (UTF-16LE)	UTF16LE	none	UTF-16LE	AL16UTF16LE
Vietnamese (Windows)	windows-1258	none	Cp1258	VN8MSWIN1258

Table F–2 (Cont.) Character Sets Supported in Oracle Content DB

Language	IANA Preferred MIME Character Set	IANA Additional Aliases	Java Encodings	Oracle Character Set
Western Alphabet	iso-8859-1	cp819, ibm819, iso-ir-100, iso8859-1, iso_8859-1, iso_8859-1:1987, latin1, l1, csISOLatin1	ISO8859_1	WE8ISO8859P1
Western Alphabet (DOS)	ibm850	cp850, 850, csIBM850	Cp850	WE38PC850
Western Alphabet (Windows)	windows-1252	x-ansi	Cp1252	WE8MSWIN1252

Document Languages Supported in Oracle Content DB

Table F–3 is a summary of the document languages supported in Oracle Content DB. Note that the supported document languages are different from the languages supported in the Oracle Content DB application.

Table F–3 Document Languages Supported in Oracle Content DB

Oracle Language Name	Java Locale	ISO Locale
Arabic	ar	ar
Bengali	bn	bn
Brazilian Portuguese	pt_BR	pt-br
Bulgarian	bg	bg
Canadian French	fr_CA	fr-CA
Catalan	ca	ca
Croatian	hr	hr
Czech	cs	cs
Danish	da	da
Dutch	nl	nl
Egyptian	ar_EG	ar-eg
American English	en	en
English	en_GB	en-gb
Estonian	et	et
Finnish	fi	fi
French	fr	fr
German	de	de
Greek	el	el
Hebrew	he	he
Hungarian	hu	hu
Icelandic	is	is
Indonesian	id	in
Italian	it	it

Table F-3 (Cont.) Document Languages Supported in Oracle Content DB

Oracle Language Name	Java Locale	ISO Locale
Japanese	ja	ja
Korean	ko	ko
Latin American Spanish	es	es
Latvian	lv	lv
Lithuanian	lt	lv
Malay	ms	ms
Mexican Spanish	es_MX	es-mx
Norwegian	no	no
Polish	pl	pl
Portuguese	pt	pt
Romanian	ro	ro
Russian	ru	ru
Simplified Chinese	zh_CN	zh-cn
Slovak	sk	sk
Slovenian	sl	sl
Spanish	es_ES	es-es
Swedish	sv	sv
Thai	th	th
Traditional Chinese	zh_TW	zh-tw
Turkish	tr	tr
Ukrainian	uk	uk
Vietnamese	vi	vi

Glossary

administrator

One of two types of administrators in Oracle Content DB: [system administrators](#) or [application administrators](#).

Administration Mode

Provides access to Oracle Content DB application administration functions such as allocating quota and assigning roles.

Advanced Queuing (AQ)

Provides an infrastructure for distributed applications to communicate asynchronously using messages. Advanced Queuing is built into Oracle Database and supports sophisticated queuing features, including subscriptions, inter-queue message propagation, message latency, message expiration, structured payloads, and exception queues. Full name: Oracle Streams Advanced Queueing.

agents

Processes that perform operations periodically (time-based) or in response to events generated by other Oracle Content DB servers or processes (event-based). An agent is a type of Oracle Content DB [server](#).

application administrators

Administrators who are responsible for tasks related to the Oracle Content DB [Site](#), such as managing users, quotas, categories, and content. There are a variety of application administration roles, including User Administrator, Category Administrator, Container Administrator, Content Administrator, and Quota Administrator. See *Oracle Content Database Application Administrator's Guide for Oracle WebCenter Suite* for more information about application administration roles and tasks.

Application Server Control

A Web-based management interface used to manage Oracle Application Server middle-tier hosts. Oracle Content DB system administrators can use the Application Server Control to operate and monitor system processes associated with the Oracle Content DB [domain](#) and [nodes](#). Full name: Oracle Enterprise Manager 10g Application Server Control.

Archive

Location in the [Site](#) where items are stored that have been deleted from user or Library trash. Depending on how the Site has been configured, items in the Archive may be automatically deleted after a specified period of time. Files and folders in the Archive can be restored by the Content Administrator of the Site.

BFILE

A read-only Oracle data type consisting of a directory object and a file name. Oracle Content DB provides transparent access to content stored as either a **BLOB** (online storage) or a BFILE (near-line storage). If BFILES are enabled for your Oracle Content DB **domain**, you can configure content archiving or content aging.

BLOB

A type of large object (**LOB**) provided by the database. All documents in Oracle Content DB are stored as BLOBs. Full name: binary large object.

BPEL

An XML-based markup language for composing a set of discrete Web services into an end-to-end process flow. Full name: Business Process Execution Language. See also [Oracle BPEL Process Manager](#).

Committed Data Cache

A feature that provides caching of the attribute values of frequently used objects without a database request, greatly improving performance and scalability.

custom workflow

A customized workflow process created in the BPEL Designer (a component of [Oracle BPEL Process Manager](#)). Custom workflows must be registered with Oracle Content DB before they can be used.

domain

A logical grouping of Oracle Content DB **nodes**, and an Oracle Database instance that contains the Oracle Content DB data.

domain properties

Settings that apply to the entire Oracle Content DB **domain**. For example, the domain property `IFS.DOMAIN.SEARCH.AttemptContextSearchRewrite` determines whether or not Oracle Content DB tries to generate fast-response SQL for text searches.

formats

Attributes that indicate document file type (for example, `.doc` or `.zip`). The format of a document determines how its content is indexed. Also known as MIME types.

HTTP

One of two **protocols** supported by Oracle Content DB, used for Web-based access. HTTP has been extended with [WebDAV](#), a protocol designed for wide area networks such as the Internet. Full name: Hypertext Transfer Protocol.

identity management

The process by which various components in an identity management system manage the security life cycle for network entities in an organization. Most commonly refers to the management of application users in an enterprise organization. See also [Oracle Identity Management](#).

JAZN

An Oracle implementation of Java Authentication and Authorization Service (JAAS), a Java package that enables services and applications to authenticate and enforce access controls on users. The OC4J JAZN provider provides application developers with user

authentication, authorization, and delegation services to integrate into their application environments. It also supports JAAS policies.

Libraries

Configurable folders for storing and sharing content with an allocated quota. Libraries were known as Workspaces in previous releases.

LDAP

An Internet protocol that applications use to look up contact information from a server, such as a central directory. LDAP servers index all the data in their entries, and filters can be used to select just the person or group you want, and return just the information you want. Full name: Lightweight Directory Access Protocol.

LOB

The majority of data stored in Oracle Content DB is stored as LOBs in database tablespaces. Full name: large object.

nodes

The application software that comprises the product, along with the underlying Java Virtual Machine (JVM) required to support the software at runtime. Each node is based on a particular **node configuration**.

The Oracle Content DB node runs as part of an **OC4J** process called `OC4J_Content`. Through servlets that are configured to work with OC4J, the node supports the Oracle Content DB Web client, Web services, and **WebDAV**.

node configuration

A configuration object that specifies the run-time behavior of a particular **node**. Each node has its own corresponding node configuration. If you want to make permanent changes to a node, such as changing **servers** or **services**, modify the node configuration for the node. If you want to make temporary (run-time) changes to a node, modify the node itself. Changes made at run time are lost when the node is restarted.

node manager

The actual process that gets started when a **node** is started. It is responsible for starting the default **service** and **servers** for a node. It also provides an administrative API for the node that lets you to find information about node log levels, locale information, available free memory, and the Oracle home of the node.

OC4J

A complete set of J2EE containers written entirely in Java that run on the Java Virtual Machine (JVM) of the standard Java Development Kit (JDK). OC4J supplies the following J2EE containers: a servlet container that complies with the servlet 2.3 specification, and a JSP container that complies with the Sun JSP 1.2 specification. Full name: Oracle Containers for J2EE.

OPMN

Manages all the components within an application server instance, including **Oracle HTTP Server** and **OC4J** processes. It channels all events from different components to all components interested in receiving them. Use OPMN to manage Oracle Content DB **nodes**. Full name: Oracle Process Manager and Notification Server.

OracleAS Infrastructure

An application server installation type that provides centralized product metadata and security services, configuration information, and data repositories for Oracle Application Server middle tiers. OracleAS Infrastructure includes [Oracle Identity Management](#).

Oracle BPEL Process Manager

A component of Oracle Application Server. It includes the BPEL Server, the BPEL Console, the BPEL Worklist application for human-centric workflows, and the BPEL Designer. You can use the BPEL Designer, an Oracle JDeveloper-based design tool, to graphically create custom workflows for use in Oracle Content DB. See also [BPEL](#).

Oracle Content Management SDK

A robust development platform for content management applications that was used to build Oracle Content DB. Oracle CM SDK provides a set of Java APIs that expose file system functionality such as file storage and searching, as well as document delete, move, and rename operations. The APIs also provide content management features unique to Oracle CM SDK, such as document versioning, controlling access to documents, and advanced queuing to facilitate communication between applications.

Oracle Drive

Oracle Drive is a native Windows application that lets users use Windows Explorer, Microsoft Office, and other Windows applications to access content in Oracle Content DB. Oracle Drive displays files and folders in Oracle Content DB as a mapped drive in Windows Explorer. Oracle Drive also provides an effective offline solution that lets users edit files on their computers when offline, and then synchronize with the server when they reconnect.

Oracle Enterprise Manager

A systems management software application that enables you to manage and monitor Oracle Application Server instances and other Oracle server products. See also [Application Server Control](#).

Oracle HTTP Server

The Web server component of Oracle Application Server, based on the Apache HTTP Server, version 1.3.28. Do not confuse with the Oracle Content DB HTTP protocol server (`EcmHttpServer`).

Oracle Identity Management

An integrated set of components that provide distributed security to Oracle products and make it possible to centrally and securely manage enterprise identities and their access to applications in the enterprise. It includes the following components: [Oracle Internet Directory](#), Oracle Directory Integration and Provisioning, Oracle Delegated Administration Services, Oracle Single Sign-On, and Oracle Application Server Certificate Authority.

Oracle Internet Directory

An [LDAP](#) service that combines Oracle Database technology with the LDAP v3 directory standard. Oracle Internet Directory is a component of [Oracle Identity Management](#). It is also closely integrated with Oracle Database.

Oracle RAC

Two or more computers configured to interact to provide the appearance of a single Oracle Database. These two or more nodes are linked by an interconnect. The

interconnect serves as the communication path between each node in the cluster database. Each Oracle instance uses the interconnect for the messaging that synchronizes each instance's use of shared resources. Oracle also uses the interconnect to transmit data blocks that are shared by the multiple instances. The datafiles accessed by all the nodes are the primary type of shared resource. Oracle RAC requires that all nodes have simultaneous access to the shared disks to give the instances concurrent access to the database. Full name: Oracle Real Application Cluster.

Oracle Text

A full-text retrieval technology built into Oracle Database for indexing and searching text and documents. Oracle Text supports mixed languages and character sets in the same index. Oracle Content DB uses the text indexing and retrieval features of Oracle Text. To enable content-based searching, Oracle Text indexes each file you store in Oracle Content DB.

Oracle Workflow

A system that supports business process definition, automation, and integration. Its technology enables automation and continuous improvement to business processes, by routing information of any type according to user-defined rules. The internal Oracle Content DB workflows, such as Request for Quota, were created in Oracle Workflow. The two default approvals workflow processes, Parallel Vote and Serial Approval, were also created in Oracle Workflow.

OUI

The installation wizard through which you can install Oracle products, including Oracle Database and Oracle Application Server. Full name: Oracle Universal Installer.

Portal

A component of Oracle Application Server that is used for the development, deployment, administration, and configuration of enterprise class portals. OracleAS Portal incorporates a portal building framework with self-service publishing features to enable you to create and manage information accessed within your portal. Full name: Oracle Application Server Portal.

protocols

Means by which users can connect to Oracle Content DB. Oracle Content DB supports two protocols: [HTTP](#) and [WebDAV](#). The Oracle Content DB protocol servers listen for requests from clients on a specific port and respond to requests according to the rules of the protocol specification. Each protocol may interact with Oracle Content DB in a different way. A protocol server is a type of Oracle Content DB [server](#).

Read-Only Connection Pool

A set of database connections shared by the [sessions](#) to perform database read operations. A minimum number of connections are created when the [service](#) is started. Depending on the number of concurrent operations performed by the sessions, and the nature of these operations, additional connections may be added to the pool, up to a specified maximum. See also [Writable Connection Pool](#).

realms

A collection of identities and associated policies that is typically used when enterprises want to isolate user populations and enforce different identity management policies for each population. Also known as identity management realms.

SAVSE

A partner solution that provides options to verify that content is virusfree and to clean files that are found to be infected. After antivirus integration has been enabled and configured, files are scanned for viruses whenever they are opened for read access, using the latest available virus definitions. Full name: Symantec AntiVirus Scan Engine.

schema

A collection of database objects, including logical structures such as tables, views, sequences, stored procedures, synonyms, indexes, clusters, and database links. A schema has the name of the database user who controls it. The Oracle Content DB schema is created in an Oracle database during the configuration process. The schema owns all database objects, including metadata about Oracle Content DB and configuration information.

servers

Processes that support protocol access to Oracle Content DB (protocol servers) or that perform important internal functions (**agents**). Each Oracle Content DB **node** can support multiple servers. Each server is based on a particular **server configuration**.

server configuration

A configuration object that holds the default values used when a **server** is started for an Oracle Content DB **node**. In addition to the server type, each server configuration specifies values for parameters relevant to that type. If you want to make permanent changes to a server, modify its server configuration. If you want to make temporary (run-time) changes to a server, modify the server itself. Changes made to servers at run time are lost when the node is restarted.

services

Processes that manage user **sessions** and that allow those sessions to access data in the Oracle Content DB repository. Each **node** must have at least one active service. A node can support multiple services, but typically you require only one for each node. Each service is based on a particular **service configuration**.

service configuration

A configuration object that holds the default values used when a **service** is started for an Oracle Content DB **node**. There are three default service configurations, named to reflect the size of their data caches: SmallServiceConfiguration, MediumServiceConfiguration, and LargeServiceConfiguration. If you want to make permanent changes to a service, modify its service configuration. If you want to make temporary (run-time) changes to a service, modify the service itself. Changes made to services at runtime are lost when the node is restarted.

sessions

There are two types of sessions in Oracle Content DB: user sessions, and Library sessions.

User sessions are specific connections of a user to Oracle Content DB through a user process. A user session is not always initiated by a user; for example, a user session could be started by an agent acting on behalf of a user, or a user being logged in through a persistent cookie. A user session lasts from the time the user logs in until the time the user logs out, or until the session times out. User sessions are subject to limits based on the Maximum Sessions Per User set for each node.

Library sessions manage user transactions and are supported by Oracle Content DB [services](#). Library sessions are subject to limits based on the Maximum Concurrent Requests Per User set for each node, as well as the service configuration property `IFS.SERVICE.MaximumConcurrentSessions`, which limits Library sessions across all users for a particular service.

Site

An organizational entity that is used to manage settings for all Oracle Content DB users. The Site has an allocated quota that specifies the amount of content (in MB, GB, or TB) that can be stored in the Site.

system administrators

Administrators in Oracle Content DB that are typically responsible for the following tasks:

- Installing and configuring Oracle Content DB
- Customizing their Oracle Content DB deployment by enabling virus checking, BFILE storage, or other options
- Managing the Oracle Content DB domain, nodes, services, and servers
- Managing the user repository for Oracle Content DB
- Performing system tuning and troubleshooting
- Managing Site settings
- Registering custom workflows

tablespace

A database storage unit that groups related logical structures together.

Web Folders

The Microsoft operating system extension that supports the [WebDAV](#) protocol. Using Web Folders, you can drag and drop files into Oracle Content DB and browse your files through Windows Explorer. On Microsoft Windows 2000 and Microsoft Windows XP, Web Folders appears in Network Places.

WebDAV

One of three [protocols](#) supported by Oracle Content DB. It lets clients browse and edit files on Oracle Content DB as if they were on the local machine. WebDAV is designed for wide area networks such as the Internet. Currently, the most widespread WebDAV client is the [Web Folders](#) extension to Windows Explorer, also known as Network Places in Windows 2000/XP. [Oracle Drive](#) uses WebDAV as its back-end protocol. Oracle Content DB also provides WebDAV support for Macintosh users. Full name: Web-based Distributed Authoring and Versioning.

workflow designer

A person with the necessary skills to design a workflow process in Oracle BPEL Process Manager. The workflow designer creates the [custom workflow](#) process, then the system administrator registers the custom workflow process with Oracle Content DB.

Writable Connection Pool

A set of database connections shared by the [sessions](#) to perform database read and write operations within a database transaction. A minimum number of connections are created when the [service](#) is started. Depending on the number of concurrent

operations performed by the sessions, and the nature of these operations, additional connections may be added to the pool up to a specified maximum. See also [Read-Only Connection Pool](#).

WS-Security

A mechanism for incorporating security information into Web Services.

Index

A

ACL cache, D-1
administration tools
 about, 1-2
 accessing, 1-6
 Administration Mode, 1-5
 Application Server Control, 1-3, 1-13
 Oracle Directory Manager, 1-5
 Oracle Internet Directory Self-Service
 Console, 1-2, 1-5, 5-2
 OracleAS JAAS Provider Admintool, 1-2, 1-5, 5-4
administrative accounts
 contentadmin, 1-2, 5-3
 oc4jadmin, 1-2
 orcladmin, 1-2, 5-1
 third-party LDAP server, 1-2, 5-2
administrators
 application, 1-1
 system, 1-1
Advanced Queueing
 See Oracle Streams Advanced Queueing
agents
 about, 1-9
 Background Processing, E-2
 Cleanup, E-3
 configuring, 8-15
 Content, E-4
 Content Garbage Collection, E-5
 Dangling Object AV Cleanup, E-5
 Event Exchanger, E-6
 Expiration, E-6
 Folder Index, E-6
 Folder Index Analyzer, E-7
 Garbage Collection, E-7
 in a high-availability environment, 2-3
 Inbound Queue Listener, E-9
 Lock, E-9
 Most Recent Doc, E-9
 Quota, E-9
 Read Document, E-10
 Reassign Quota, E-10
 Refresh Security, E-11
 requirements for, 1-9
 Service Warmup, E-11
 Service Watchdog, D-5, E-11

 Statistics, 9-4, E-12
 User Connect, E-12
 Version Purge, E-13
 Virus Repair, 4-2, E-13
AggreSpy, 9-4
analyze.sql script, 12-3, A-4
Anonymous SSL, 3-5
antivirus integration, setting up, 4-2
application administrators, 1-1
Application Server Control
 about, 1-3
 accessing, 1-6
 accessing Oracle Content DB Home page, 1-3
 URL, 1-3
architecture, 1-7
Archive, 4-5, 11-1
archiving data, 4-5
ASCII content, 2-13
authentication
 as a trusted application, 3-7
 case-sensitive, D-2
 digest, 3-11
 modes, 3-2
 user, 3-6
automation, 1-6
Axis framework, 1-7

B

B*tree database index, 2-14
Background Processing Agent, E-2
BACKGROUND_DUMP_DEST parameter, C-3
backups, 12-1
BFILEs
 about, 4-5
 archiving, 4-5
 backing up, 12-1
 definition, 4-5
binary large object
 See BLOB
BLOB, about, 2-11, 4-5
BlockOverhead, 2-11
BPEL, 1-14, 6-2
browser-based access, 1-10

C

- caches
 - ACL, D-1
 - Committed Data, 7-6, 9-3
 - maximum size, D-3
- calculating Xmx settings, 12-2
- Cancel Event, for custom workflows, 6-2
- certificates, 3-7
- certification information, 1-6
- changehostname script, 4-10
- changepassword script, 3-7
- chunks, 2-11
- Cleanup Agent, E-3
- ClearContextJobs.sql, C-3
- client
 - certification information, 1-6, 1-10
 - platforms, 1-10
 - public key, importing, 3-9
 - session timeout period, 3-12
- clients
 - about, 1-10
 - HTTP, 1-11
 - WebDAV, 1-10, 1-11
 - Windows, 4-10
- cluster, 1-12
- command-line tools
 - changehostname, 4-10
 - changepassword, 3-3, 3-9, 3-10, 3-11
 - deleteuser, 5-5
 - opmncnt, 1-5, 7-16
- Committed Data Cache
 - about, 7-6
 - dynamically changing, 7-7
 - service configuration properties, 7-8
 - statistics, 9-3
- concurrent sessions
 - See sessions
- configuration
 - domain properties, 8-1
 - node, 8-4
 - server, 8-11
 - service, 8-8
- configuration assistant log, 9-4
- connection pools
 - read-only, 7-8
 - statistics, 9-3
 - writable, 7-8
- connections, minimum number of, 7-9
- content
 - accessing offline, 4-10
 - accessing with Microsoft Office applications, 4-10
 - accessing with Windows Explorer, 4-10
 - of deleted users, 5-6
- Content Agent, E-4
- Content Garbage Collection Agent, A-1, E-5
- CONTENT_IFS_CTX_I tablespace, 2-13, 2-14
- CONTENT_IFS_CTX_K tablespace, 2-14
- CONTENT_IFS_CTX_X tablespace, 2-14
- CONTENT_IFS_LOB_I tablespaces, 2-11
- CONTENT_IFS_LOB_N tablespaces, 2-11

- CONTENT_IFS_MAIN tablespace, 2-13
- contentadmin account, 1-2, 5-3
- Cost-Based Optimizer, 12-3
- CPU, 2-4
- CreateContextFunnelProcedure.SQL, C-2
- CreateContextIndex.sql, C-2
- CreateContextPreferences.sql, C-2
- credential manager, service configuration
 - properties, D-3
- credentials, user, 3-6
- Critical Patch Updates, 3-12
- ctx_ddl.optimize_index, C-3
- ctx_ddl.sync_index, C-2
- custom applications, building, 1-6
- custom workflows
 - about, 1-14, 6-1
 - building, 1-6
 - Cancel Event, 6-2
 - deleting, 6-4
 - Launch Event, 6-2
 - registering, 6-2
- customization, 1-6

D

- Dangling Object AV Cleanup Agent, E-5
- data
 - archiving, 4-5
 - backing up, 12-1
- data cache, maximum size, D-3
- data types
 - Oracle Content DB, 2-10
 - standard, 1-12
- database
 - backing up, 12-1
 - clustering, 1-12
 - tables, 1-12
- database buffer cache, 2-9
- DB_BLOCK_SIZE parameter, 2-11
- DBMS_JOBS
 - about, C-3
 - changing or removing, C-3
 - monitoring, C-3
- DCPromo.exe utility, 4-15
- default service configurations, 12-1
- deinstalling Oracle Content DB, 2-3
- deleteuser script, 5-5
- deployment
 - multiple-computer, 2-2
 - single-computer, 2-1
- DHCP, 1-10, 1-11, A-2
- digest authentication, 3-11
- disk
 - size, 2-5
 - throughput, 2-5
- DMS metrics, 9-4
- dmstool, 9-4
- documents
 - associating formats with, 10-1
 - designating to be indexed, C-4

- overhead, 2-13
- domain
 - about, 7-1
 - diagram, 1-7
 - performance monitoring, 9-1
 - properties, 8-1
 - restarting, 7-2, 7-17
 - starting, 7-2, 7-17
 - starting from command line, 7-16
 - stopping, 7-2, 7-17
- domain properties
 - about, 8-1
 - changing, 8-1
 - editable, 8-2
- drives, mapped, 4-10

E

- .EAR file, 1-13
- eDirectory, 5-2
- e-mail
 - notifications, 4-1
 - servers, 4-1
 - Site quota notifications, 11-1
- Event Exchanger Agent, E-6
- Expiration Agent, E-6
- Explain Plan, 12-4

F

- file-based user repository
 - and multiple middle tiers, 5-3
 - default user for, 5-3
 - jazn-data.xml file, 5-3
 - managing users, 5-4
 - using with Oracle Content DB, 5-3
- files
 - designating to be indexed, C-4
 - .EAR, 1-13
 - .Jar, 1-13
 - limiting size of, 3-11
 - migrating, B-1
 - quarantined, 4-2
 - .RAR, 1-13
 - synchronizing, 4-10
 - uploading and downloading multiple, 4-11
 - .WAR, 1-13
- firewall
 - interference with Oracle Drive, 4-19
 - opening ports, 4-8
 - sample configuration, 4-9
 - timeout periods, 4-9
- Folder Index Agent, E-6
- Folder Index Analyzer Agent, E-7
- formats
 - about, 10-1
 - adding, 10-1
 - default, 10-4
 - deleting, 10-3
 - excluding from virus scans, 4-4

- modifying, 10-2

G

- garbage collection, 12-5
- Garbage Collection Agent, E-7
- GrantContextToIFS.sql, C-2
- guest users, 2-7

H

- hardware requirements, 2-4
- headroom parameter, 2-8
- high availability considerations, 2-3
- host name, changing, 4-9
- HTTP
 - about, 1-10
 - access, 1-10
 - security issues, 3-11
 - server configuration parameters, E-7
- HTTP/DAV, 3-11
- Hypertext Transfer Protocol
 - See HTTP

I

- ICAP, 4-3
- IExpress utility, 4-18
- IFS_LYKE index
 - maintaining, C-1
- IFS_TEXT index
 - about, C-1
 - maintaining, C-2
 - optimizing, C-2
 - refreshing, C-2
- IFS.SERVICE.DATACACHE.Size, 2-7
- IFS.SERVICE.MaximumConcurrentSessions, 2-7
- Inbound Queue Listener Agent, E-9
- indexing
 - setting up, 10-1, C-4
 - troubleshooting, C-5
 - with Oracle Text, C-1
- installing Oracle Content DB, 1-6
- interconnect, 1-12
- interMedia Text, C-1
- IP address, changing, 4-9
- iPlanet, 5-2

J

- .JAR files, 1-13
- Java
 - API layer, 1-7
 - cache statistics, 12-5
 - heap size, 8-8, A-3
 - object cache, 2-7
 - servlets, 1-13
 - Xmx setting, 12-1
 - Xmx settings, 12-5
- Java Server Pages (JSPs), 1-13
- Java SSO, 3-7

- java.lang.OutOfMemory errors, 12-2
- JAZN, 3-7, A-2
- JCR Adapter
 - about, 1-7
 - configuring, 1-6, 1-7
- JDBC, D-4
- JOB_QUEUE_PROCESSES parameter, C-3
- JSR-170, 1-7
- JVM memory usage, chart for, 9-2
- JVM threads, chart for, 9-2

K

keystores

- changing passwords for, 3-9
- LDAP, 3-2
- listing keys, 3-8
- server, 3-7
- WS-Security, 3-7

keytool, 3-2, 3-7

L

languages, supported, F-6

large objects

See LOBs

Launch Event, for custom workflows, 6-2

launch page, 4-20

LDAP keystore, 3-2

LDAP server certificate, 3-2

LDAP servers, supported third-party, 5-2

ldapadd, 1-5, 5-2

ldapmodify, 1-5, 5-2

Library sessions

about, Glossary-7

limiting, 12-1

LIBRARYOBJECTS, D-3

load balancer, setting up, 1-6

LOB index, 2-12

LOBs, 1-12, 2-11

Lock Agent, E-9

loggers, for Oracle Content DB, 9-6

logging out, 3-7

logging service performance information, 9-4

logs

application, 9-4

changehostname.log, 9-5

changing log level, 9-5

ContentConfig.log, 9-4

for changehostname script, 4-10

for Oracle Content DB, 9-4

viewing, 9-5

M

Macintosh clients, 1-10

malicious uploads, preventing, 3-11

mapped drives, 4-10

maximum number of repair attempts, 4-2

memory, 2-4

metadata storage, 1-11

metrics, DMS, 9-4

Microsoft Active Directory, 4-15, 5-2

Microsoft .NET Framework, 4-11

middle tier, backing up, 12-1

migrating files, B-1

MIME types, 10-1, C-4

monitoring

domain performance, 9-1

vmstat tool, A-4

Most Recent Doc Agent, E-9

multiple-computer deployment, 2-2

N

near-line storage, 4-5

network channel encryption, 3-11

New User Orientation

about, 4-19

customizing, 4-20

node configurations

about, 8-4

adding servers, 8-7

adding services, 8-7

changing, 8-5

nodes, 1-8

about, 7-1

checking status, 7-16

diagram, 1-8

Java parameters, 8-7

logs, 9-4

manager, 1-8

modifying at run time, 7-4

Oracle RAC, 1-12

restarting, 7-4, 7-17

starting, 7-3, 7-17

starting from command line, 7-16

stopping, 7-3, 7-17

number of CPUs

database computer, 2-8

middle tier computer, 2-6

O

OC4J

about, 1-13

managing, 7-16

OC4J_Content, 7-1

checking status, 7-16

logs, 9-4

modifying, 7-4

restarting, 7-4, 7-17

starting, 7-3, 7-17

stopping, 7-3, 7-17

oc4jadmin account, 1-2

ODriveSetup.msi file, extracting, 4-15

offline storage, 4-5

on-demand provisioning, 5-5

OpenLDAP, 5-2

OPMN

See Oracle Process Management and Notification

- Server
 - opmnctl script, 1-5, 7-16
 - Optimize Job, C-3
 - Oracle Application Server, 1-12
 - Oracle BPEL Process Manager
 - about, 6-1
 - creating workflows in, 6-2
 - integration with, 1-14
 - Oracle Content DB
 - application architecture, 1-7
 - application host property, 8-2
 - application port property, 8-2
 - architecture, 1-6
 - changing the port number, 4-8
 - configuring for SSL, 3-1
 - Data Control, 1-7
 - data types, 2-10
 - deinstalling, 2-3
 - deploying, 2-1
 - domain, 1-7, 7-1
 - extending, 1-6
 - getting started after installation, 1-6
 - high availability considerations, 2-3
 - installing, 1-6
 - JCR Adapter, 1-6
 - loggers, 9-6
 - logs, 9-4
 - migrating files to, B-1
 - New User Orientation, 4-19
 - nodes, 1-8
 - options, 4-1
 - processes, 7-1
 - protocols, 1-10
 - related documentation, 1-6
 - running on Windows, 1-14
 - schema, 1-8, 1-11
 - security architecture, 3-1
 - service configuration, 12-1
 - sizing guidelines, 2-4
 - starting, 7-1
 - URL, 1-10
 - user provisioning, 5-5
 - Web services, 1-6
 - Oracle Database
 - Oracle Content DB integration with, 1-11
 - schema password, 3-10
 - URL, 4-10
 - Oracle Directory Manager, 1-5, 5-2
 - Oracle Drive
 - about, 4-10
 - administrator-configured installation, 4-11
 - and firewall software, 4-19
 - config.xml file parameters, 4-12
 - downloading, 4-10
 - drive letter, 4-13
 - extracting ODriveSetup.msi file, 4-15
 - installed files, 4-16
 - installing, 4-18
 - odrive.ini file parameters, 4-14
 - preconfiguring service details, 4-17
 - redeploying, 4-16
 - Report a Problem e-mail address, 4-12
 - .SED file parameters, 4-18
 - update.xml file parameters, 4-14
 - Oracle Enterprise Manager, 1-13
 - Oracle Identity Management, 1-10, 5-1
 - Oracle Internet Directory
 - administration tools, 5-2
 - managing users, 5-2
 - required user attributes, A-1
 - using with Oracle Content DB, 5-1
 - Oracle Internet Directory Self-Service Console, 1-2, 1-5, 5-2
 - Oracle Process Management and Notification Server
 - about, 1-13
 - running on Windows, 1-13
 - Oracle Real Application Clusters
 - about, 1-12
 - changing to, 4-10
 - Oracle Streams Advanced Queuing, 1-12
 - Oracle Text
 - about, 1-12, C-1
 - and Oracle Content DB searches, 2-13
 - maintaining the IFS_TEXT index, C-2
 - tablespaces, C-1
 - troubleshooting, C-5
 - Oracle Text Index tablespace, C-2
 - Oracle Text Other tablespace, C-2
 - Oracle Text Tokens tablespace, C-1
 - Oracle Workflow
 - about, 1-14
 - backing up, 12-1
 - OracleAS Containers for J2EE
 - See* OC4J
 - OracleAS Infrastructure, installing, 5-1
 - OracleAS JAAS Provider Admin tool, 1-2, 1-5, 5-4
 - oraInventory directory, 12-1
 - orcladmin account, 1-2, 5-1
 - orphan session, D-2
 - out-of-memory exception, A-3
 - OWF_MGR, 12-1
- ## P
-
- Parallel Vote workflow process, 6-1
 - passwords
 - case-sensitive, D-2
 - schema, 1-2
 - PCCU, 12-2
 - PCTVERSION parameter, 2-12
 - peak concurrent connected users, 2-6, 2-8
 - performance
 - monitoring server, 9-4
 - troubleshooting, 12-4
 - tuning, 12-3
 - pop-up blockers, disabling, A-1
 - ports, changing, 4-8
 - processes, node, 7-1
 - properties
 - application host, 8-2

- application port, 8-2
- domain, 8-1
- protocol servers
 - about, 1-10
 - HTTP, 1-10, E-7
 - WebDAV, 1-10, 1-11
- protocols
 - and DHCP, 1-10
 - supported, 1-10
- provisioning
 - troubleshooting, A-1
 - users, 5-5

Q

- quarantined files, 4-2
- Quota Agent, E-9
- quota e-mail notifications, 11-1
- quotas
 - Library, E-10
 - Site, 11-1, Glossary-7

R

- .RAR file, 1-13
- Read Document Agent, E-10
- Read-Only Connection Pool
 - about, 7-8
 - dynamically changing, 7-8
 - parameters, D-2
 - statistics, 9-3
- Reassign Quota Agent, E-10
- Redo log size, 2-8, A-4
- Refresh Security Agent, E-11
- related documents, xii
- remote processes, managing, 7-17
- requests, maximum number per user, 8-6
- required usable disk space
 - database computer, 2-8
 - middle tier computer, 2-6
- roles, application administrator, 1-2, 11-3
- run time
 - changes to Committed Data Cache, 7-7
 - changes to Connection Pools, 7-8
 - changes to nodes, 7-4
 - changes to servers, 7-11
 - changes to services, 7-4

S

- SAVSE
 - about, 4-2
 - setting up, 4-3
- schema
 - \$CM, 1-12, 12-1
 - Oracle Content DB, 1-8, 1-11
 - password, 1-2, 3-10
 - tables, 1-12
- scripts
 - analyze.sql, 12-3
 - changehostname, 4-10

- changepassword, 3-7
- deleteuser, 5-5
- opmnctl, 1-5, 7-16
- SQL, C-2, C-3, C-4
- searching
 - for users, 5-5, A-2
 - specifying search timeout period, C-5
 - troubleshooting, C-5
- security
 - about, 3-1
 - issues with HTTP, 3-11
 - issues with WebDAV, 3-11
 - network channel encryption, 3-11
- Security Administrator role, granting, 11-3
- Security Alerts, 3-12
- Serial Approval workflow process, 6-1
- server configurations
 - about, 8-11
 - abstract and non-abstract, 8-12
 - creating, 8-13
 - deleting, 8-16
 - modifying, 8-15
 - properties, E-1
 - viewing inherited properties, 8-13
- server keystore, 3-7
- Server Only SSL, 3-2
- server public key, exporting, 3-8
- servers
 - about, 1-9
 - adding to node, 8-7
 - changing at run time, 7-14
 - creating, 7-12
 - managing at run time, 7-11
 - monitoring performance, 9-4
 - protocol, 1-10
 - reloading, 7-15
 - setting Initially Started, 7-14, 8-7
 - shared properties, E-2
 - slow read and write activity, A-4
 - SMTP, 4-1
 - stopping and starting, 7-13
 - suspending and resuming, 7-13
- service configurations
 - about, 8-8
 - and library sessions, 12-1
 - changing, 8-10
 - creating, 8-9
 - default, 8-3
 - deleting, 8-11
 - properties, D-1
 - types, 8-8
- Service Warmup Agent, E-11
- Service Watchdog Agent, D-5, E-11
- services
 - about, 1-9
 - adding to node, 8-7
 - changing at run time, 7-5
 - creating, 7-5
 - deleting, 7-11
 - failed, D-5

- logging performance information, 9-4
- managing at run time, 7-4
- specifying automatic shutdown, 7-6
- servlets, Java, 1-13
- sessions
 - about, Glossary-6
 - chart, 9-2
 - enabling and disabling acceptance of, 7-6
 - maximum number per user, 8-6
 - number of concurrent, 7-6, D-4
 - operation timeout period, D-6
 - orphan, D-2
 - service configuration properties, D-4
- SetupContextJobs.sql, C-3
- single-computer deployment, 2-1
- Site
 - about, 1-10, 11-1
 - administrators, 11-1
 - modifying, 11-1
 - quota, 11-1
 - quota warning notifications, 4-1
- Sites
 - quota, Glossary-7
- sizing
 - formulas for database computer, 2-8
 - formulas for middle-tier computer, 2-5
 - guidelines, 2-4
- SMTP servers, configuring, 4-1
- SOAP, 6-2
- SQL scripts
 - ClearContextJobs.sql, C-3
 - CreateContextFunnelProcedure.SQL, C-2
 - CreateContextIndex.sql, C-2
 - CreateContextPreferences.sql, C-2
 - GrantContextToIFS.sql, C-2
 - SetupContextJobs.sql, C-3
 - SyncContextIndex.sql, C-4
 - ViewContextErrors.sql, C-4
 - ViewDocumentByRowID.sql, C-4
- SSL
 - Anonymous, 3-5
 - for client connections to Oracle Content DB, 3-1
 - for user repository, 3-2
 - Server Only, 3-2
 - supported authentication modes, 3-2
- statement cache, 7-8
- statistics
 - Committed Data Cache, 9-3
 - connection pool, 9-3
 - data distribution, 12-3
 - Java cache, 12-5
 - resetting, 9-3
- Statistics Agent, 9-4, E-12
- Statspack utility, 12-4
- storage
 - calculating, 2-11
 - management options, 4-5
 - metadata, 2-13
 - near-line, 4-5
 - offline, 4-5

- optimized, 1-12
- Sun Directory Server, 5-2
- support calls, reducing, 4-11
- Sync Job, C-3
- SyncContextIndex.sql, C-4
- system administrator, 1-1
- System MBean Browser, 9-5

T

- tables, database, 1-12
- tablespace
 - definitions, 2-10
 - storage requirements, 2-10
- tablespaces
 - CONTENT_IFS_CTX_I, 2-13, 2-14
 - CONTENT_IFS_CTX_K, 2-14
 - CONTENT_IFS_CTX_X, 2-14
 - CONTENT_IFS_LOB_I, 2-11
 - CONTENT_IFS_LOB_N, 2-11
 - CONTENT_IFS_MAIN, 2-13
 - Oracle Text Index, C-2
 - oracle Text Other, C-2
 - Oracle Text Tokens, C-1
 - WORKFLOW_IFS_MAIN, 2-10
- text
 - analyzing, 1-12
 - indexing, 1-12
 - searching, 1-12
- total computer memory
 - database computer, 2-9
 - middle tier computer, 2-6
- trusted application, 3-7

U

- URLs
 - Oracle Content DB, 1-10
 - Oracle Database, 4-10
 - WebDAV, 1-11
- User Connect Agent, E-12
- user names, limitations, 1-11
- user preferences information, 5-6, A-2
- user profile information, 5-6
- user profiles for hardware sizing, 2-5
- user provisioning, 5-5
- user repository
 - about, 1-10
 - file-based, 5-3
 - Oracle Internet Directory, 5-1
 - setting up SSL, 3-2
 - supported types, 5-1
 - third-party, 5-2
- user sessions, about, Glossary-6
- users
 - authenticating, 3-6
 - deleting, 5-5
 - guest, 2-7
 - managing in a file-based user repository, 5-4
 - managing in a third-party LDAP server, 5-3

managing in Oracle Internet Directory, 5-2
peak concurrent connected, 2-6, 2-8
searching for, 5-5, A-2

modifying, A-3

V

verbosegc, 12-5
Version Purge Agent, E-13
ViewContextErrors.sql, C-4
ViewDocumentByRowID.sql, C-4
virus definitions, 4-3
Virus Repair Agent, 4-2, E-13
virus scanning
 exclusions, 4-2
 performance implications, 4-4
 policy, 4-3
vmstat, A-4

W

.WAR file, 1-13
Web client error reports, 4-1
Web services, 1-6
 service descriptions, 1-7
 URL, 1-7
 wsdl files, 1-7
WebDAV
 about, 1-10
 access, 1-11
 clients, 1-10
 limitations, 1-11
 security issues, 3-11
 URL, 1-11
web.xml file, E-8
Windows clients, 4-10
Windows users, information for, 1-14
WORKFLOW_IFS_MAIN tablespace, 2-10
workflows
 blocking, 6-1
 custom, 1-14
 default, 6-1
 Parallel Vote, 6-1
 registering, 6-2
 Serial Approval, 6-1
Writable Connection Pool
 about, 7-8
 dynamically changing, 7-8
 parameters, D-3
 statistics, 9-3
WSDL, 1-7, 6-2
WS-Security
 about, 3-7
 keystore, 3-7

X

XML Schema, 6-2
Xmx settings
 about, 12-1, 12-5
 calculating, 12-2
 changing, 8-7