

Oracle® Content Database

Application Administrator's Guide

10g Release 1 (10.2)

B31265-02

September 2006

Oracle Content Database Application Administrator's Guide, 10g Release 1 (10.2)

B31265-02

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

Primary Author: Ginger Tabora

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

Audience.....	v
Documentation Accessibility	v
Related Documents	vi
Conventions	vii
1 Oracle Content DB Overview	
1.1 What Is Content Management?	1-1
1.2 Oracle Content Database	1-1
1.3 Oracle Content DB Administration.....	1-1
1.4 Oracle Content DB Default Folder Structure	1-2
1.5 Signing In to Oracle Content DB for the First Time.....	1-2
2 Oracle Content DB Site Level Administration	
2.1 Oracle Content DB Site Administration	2-1
2.1.1 Assigning an Administrator Role to a User.....	2-1
2.2 Oracle Content DB Role Administration.....	2-1
2.3 Oracle Content DB User Administration.....	2-2
2.3.1 Managing Oracle Content DB Users.....	2-3
2.3.2 Managing Oracle Content DB Groups.....	2-3
2.4 Oracle Content DB Category Administration.....	2-3
2.4.1 Managing Oracle Content DB Category Properties	2-3
2.5 Oracle Records Database Administration	2-4
3 Oracle Content DB Site-Level and Container-Level Administration	
3.1 Oracle Content DB Container Administration	3-1
3.1.1 Managing Oracle Content DB Containers.....	3-1
3.2 Oracle Content DB Security Administration	3-2
3.2.1 Managing Oracle Content DB Administrator Roles.....	3-2
3.2.2 Managing Oracle Content DB User Roles	3-3
3.3 Oracle Content DB Library Administration.....	3-7
3.4 Oracle Content DB Configuration Administration.....	3-7
3.4.1 Managing Auditing Tasks	3-7
3.4.2 Managing Workflow Processes	3-7
3.4.3 Setting Oracle Content DB Library Defaults	3-8
3.5 Oracle Content DB Content Administration.....	3-8

3.5.1	Managing Oracle Content DB Content.....	3-9
3.5.2	Managing the Oracle Content DB Archive	3-9
3.6	Oracle Content DB Quota Administration.....	3-9
3.6.1	Managing Oracle Content DB Library Quota.....	3-9
3.7	Other Oracle Content DB Roles	3-10

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 life cycle management. Oracle Content DB integrates with OracleAS Portal, E-Business applications, and other environments.

Oracle Content DB runs with Oracle Application Server and an Oracle database, and provides a highly scalable content management repository. This guide describes application administration functions for Oracle Content DB.

Audience

Oracle Content Database Application Administrator's Guide is intended for Oracle Content DB application administrators, such as User, Category, or Quota Administrators. Oracle Content DB system administrators should refer to *Oracle Content Database Administrator's Guide* for information about system 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 Database and Oracle Records DB

- *Oracle Content Database Administrator's Guide*
- *Oracle Records Database Application Administrator's Guide*

Oracle Collaboration Suite

- *Oracle Collaboration Suite Administrator's Guide*
- *Oracle Collaboration Suite Release Notes*
- *Oracle Collaboration Suite Installation Guide*
- *Oracle Collaboration Suite Upgrade Guide*
- *Oracle Collaboration Suite Concepts Guide*
- *Oracle Collaboration Suite Deployment Guide*
- *Oracle Collaboration Suite Security Guide*
- *Oracle Collaboration Suite Licensing Information*
- *Oracle Collaboration Suite Migration and Coexistence Guide*

Oracle Application Server

- *Oracle Application Server Concepts*
- *Oracle Application Server Installation Guide*
- *Oracle Application Server Administrator's Guide*
- *Oracle Internet Directory Administrator's Guide*
- *Oracle HTTP Server Administrator's Guide*
- *Oracle Application Server Single Sign-On Administrator's Guide*
- *Oracle BPEL Process Manager Developer's Guide*

Oracle Database 10g

- *Oracle Database Administrator's Guide*
- *Oracle Database Backup and Recovery Basics*
- *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*

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 Overview

This chapter provides an overview of the Oracle Content DB application. This chapter contains the following topics:

- [What Is Content Management?](#)
- [Oracle Content Database](#)
- [Oracle Content DB Administration](#)
- [Oracle Content DB Default Folder Structure](#)
- [Signing In to Oracle Content DB for the First Time](#)

1.1 What Is Content Management?

Content management systems enable organizations to support the life cycle of content. The life cycle of content typically consists of creating, editing, publishing, and archiving. For example, content is created by one or more authors. Over time, that content may be edited and approved for publication. Once the content has been published, it may be replaced by another form of content and archived or removed from use.

Content management can improve an organization's knowledge sharing and communication capability. Content management systems improve users' efficiency by making content readily available.

In addition, content management systems may include version control, workflow, security, and more.

1.2 Oracle Content Database

Oracle Content DB is a consolidated, database-centric content management system that provides a comprehensive, integrated solution for file and document life cycle management. Oracle Content DB enables enterprise customers to use one highly scalable, manageable, and usable application to manage all of their unstructured information.

1.3 Oracle Content DB Administration

There are two types of administration for Oracle Content DB: system administration and application administration.

- System administration involves managing the Oracle Content DB instance by starting and stopping the nodes, services, and servers, tuning the system to ensure reliability and performance, creating, modifying, and deleting **Sites**, as well as

registering custom workflow processes. System administration uses Oracle Enterprise Manager 10g Application Server Control to manage Oracle Content DB.

- Application administration involves managing users, **quota**, Libraries, categories, content, and records at the Site and **Container** levels. Application administration is divided into multiple administrator roles that can be assigned at the Site level only or at both the Site and Container levels.

A single user can act in multiple roles. In addition, each role has a different set of access privileges.

1.4 Oracle Content DB Default Folder Structure

When Oracle Content DB is installed, and the personal library is enabled, a default folder structure is automatically created with the following folders:

- Private Documents
- Published Documents
- Shared Folders

1.5 Signing In to Oracle Content DB for the First Time

Initially, when Oracle Content DB is installed, a default user is chosen.

When first signing in to Oracle Content DB, use the `orcladmin` user for the default realm. This user has all the Oracle Content DB administrative roles.

The `orcladmin` user can designate the various application administrator roles to other users. A user can have more than one **application administrator** role, and more than one user may be assigned the same application administrator role.

In addition, the `orcladmin` user can designate the Security Administrator role to a user, and in turn, that Security Administrator can designate the remaining application administrator roles to other users.

Once users have been assigned administrator roles, they can sign on to the application as a regular user, and decide whether or not they want to be in administrator mode by selecting **Switch to Administration Mode**.

Oracle Content DB Site Level Administration

This chapter provides conceptual information for Oracle Content Database Site-level administration. This chapter contains the following topics:

- [Oracle Content DB Site Administration](#)
- [Oracle Content DB Role Administration](#)
- [Oracle Content DB User Administration](#)
- [Oracle Content DB Category Administration](#)
- [Oracle Records Database Administration](#)

2.1 Oracle Content DB Site Administration

Site Administrators can provide the ability to grant public access for specific items and **Library** creation request for the Site folder.

2.1.1 Assigning an Administrator Role to a User

Perform the following steps to assign an administrator role to a user:

1. Sign in to Oracle Content DB as an administrator.
2. Click on Switch to Administration Mode.
3. In the Folders pane, select the Site.
4. From the File menu, select Properties to open the Properties window.
5. Open the Sharing tab.
6. Enter the username of the person to which you want to add. The selected user's current administrative roles are displayed under the list of users and groups.
7. Select a role to assign from the Roles list.
8. Click Grant to assign the role to the selected user.
9. Click OK.

2.2 Oracle Content DB Role Administration

Role Administrators can perform the following tasks:

- View and modify permissions associated with default and custom roles
- Create custom roles by combining permissions that are available

- Delete default and custom roles
- Hide default and custom roles

A default role is a role that ships with Oracle Content DB. A custom role is a role created by the Role Administrator.

In addition, Role Administrators can change the order of the roles that are available to users on the Library, folder, and file levels.

Users assigned this role will be able to see the Role Administration link when they switch to Administration Mode in the Web client.

See "[Oracle Content DB Security Administration](#)" in Chapter 3 for a list of the various roles.

2.3 Oracle Content DB User Administration

All Oracle Content DB users are **Oracle Internet Directory** users. Users are synchronized from Oracle Internet Directory into Oracle Content DB through the Oracle Internet Directory Credential Manager Agent.

The Oracle Internet Directory Credential Manager Agent is a time-based agent that polls for changes to Oracle Internet Directory users. If a user has been added, modified, or deleted in Oracle Internet Directory, the Oracle Internet Directory Credential Manager Agent makes the change in Oracle Content DB.

After users have been created in Oracle Internet Directory, users are automatically provisioned in Oracle Content DB by the Oracle Internet Directory Credential Manager Agent.

Once a user has been provisioned into Oracle Content DB, they can sign on to the application.

User Administrators manage all users and groups within a Site. User Administrators can perform the following tasks:

- Set and modify user preference defaults
- Enable edit -in-place for documents
- Allow users to have a Personal Library
- Search for all users in a Site
- Add and remove members of a group
- Assign a group member the Group Manager role
- Create and delete groups
- Restrict which users have group creation permission

User Administrators can restrict which users can create groups within the Site. By default, all users can create groups.

Group creators can specify who has access to the group membership list. The group creator can specify one of the following access permissions:

- All users
- Members of the group (default)
- Managers of the group

Any group manager of this group or the User Administrator can modify this setting once the group has been created.

2.3.1 Managing Oracle Content DB Users

User Administrators can search for all users in a Site, as well as set and modify the following user default preferences:

- Enable edit-in-place for documents
- Enable each user to have a Personal Library
- Specify the number of files to list in each user's My Recent Files list
- Specify how often each user should be prompted for a password when using a WebDAV client
- Specify the Default Document Language
- Specify file types to be excluded from the My Recent Files list
- Specify which character encoding should be used for multibyte URLs that are not W3C compliant

2.3.2 Managing Oracle Content DB Groups

User Administrators manage all groups in a Site. They have Group Manager access for all groups in a Site, which allows them to add and remove members from a group, and assign the Group Manager role to a group member.

In addition, User Administrators can also restrict which users have group creation permission.

Once a Group Manager is assigned, then the Group Manager can modify and delete existing member properties of the groups they manage.

2.4 Oracle Content DB Category Administration

By associating categories with files and modifying the attributes of a category, users can organize and classify their information. Users can also search for files by category and by a category's attributes.

Users can categorize files by applying categories to them in the File Properties window. Configuration Administrators and administrators of Libraries and folders can exclude or specify required or optional categories for folders. If required, users must enter information for these categories when uploading or checking in files.

Categories can be divided into subcategories, and can have one or more attributes. Categories are created and configured for a Site by the Category Administrator. Categories are listed and sorted by name.

Category Administrators manage categories within a Site. They can create categories for a Site and defines a hierarchy of categories and subcategories available to users in a Site. In addition, Category Administrators modify and delete categories, as well as add additional categories to any point in the category hierarchy.

2.4.1 Managing Oracle Content DB Category Properties

Category Administrators can create, modify, and delete categories within a Site. A name must be provided for each category when it is created.

Category Administrators can also add and remove **category attributes**. The parameters that can be modified for an existing attribute are Prompt, Configurable, Required, Hidden , and Default Value.

2.5 Oracle Records Database Administration

Oracle Records Database (Oracle Records DB) is a records management application that ships with Oracle Content DB. To use Oracle Records DB, it must be enabled through Oracle Enterprise Manager 10g Application Server Control.

Records Administrators can perform the following:

- Create, update, and delete file plans, record categories, record series, and record folders
- Change content that has been declared a record back to regular content
- Freeze record dispositions
- Close record categories for further filings
- Submit failed dispositions
- Manage records management security

The Records Administrator must also have Content Administrator privileges to view and change content that has been declared a record to regular content.

See Also: *Oracle Records Database Application Administrator's Guide* for more information

Oracle Content DB Site-Level and Container-Level Administration

This chapter provides conceptual information for Oracle Content DB Site and Container-level administration. This chapter contains the following topics:

- [Oracle Content DB Container Administration](#)
- [Oracle Content DB Security Administration](#)
- [Oracle Content DB Library Administration](#)
- [Oracle Content DB Configuration Administration](#)
- [Oracle Content DB Content Administration](#)
- [Oracle Content DB Quota Administration](#)
- [Other Oracle Content DB Roles](#)

3.1 Oracle Content DB Container Administration

A **Container** is a special kind of folder that can contain other Containers or Libraries. Containers let Oracle Content DB administrators organize the folder hierarchy in a logical way. For example, Containers could be created for geographical regions or by division. Users can see only the Containers to which they have access.

Note: Folders containing more than 1000 documents are slow in opening through WebDAV or the Web Client.

To avoid this ensure that there are no more than 1000 Libraries in a single Container, and limit folders that will be opened frequently to contain less than 1000 documents.

3.1.1 Managing Oracle Content DB Containers

Container Administrators can create, remove, and modify Container properties, such as the name and description.

Only Container Administrators can create and delete Containers. Containers may have default folder configuration settings that are inherited by Libraries created in the Container. In addition, a Container can be configured to allow or to limit Library creation to users and groups with specific privileges. Container Administrators can also enable Library creation requests through a workflow process.

In addition, Containers have Library defaults for categories, workflow, records management, and version creation. By default, these settings are inherited by all

Libraries created in the Container. There are no default security settings for Libraries in Containers.

Only a Container Administrator can delete a Container.

3.2 Oracle Content DB Security Administration

Security Administrators can add, remove, or modify administrator and user roles. Only Security Administrators can modify Site and Container roles. They can also manage the roles of Libraries, folders, and files within the Container.

3.2.1 Managing Oracle Content DB Administrator Roles

Security Administrators can assign administrative roles to any user in the Site. Each administrative role must be filled by at least one user.

Administration that can be performed only at the Site level is divided into the following roles:

- **Site Administrator**
Provides the ability to grant public access for specific items and Library creation requests for the Site folder.
- **Role Administrator**
Views and modifies permissions associated with default and custom roles; creates custom roles by combining permissions that are available; deletes default and custom roles; hides default and custom roles; adds, removes, and changes the order of the roles that are available to users on the Library, folder, and file levels.
- **User Administrator**
Sets and modifies user preference defaults; searches for all users in a Site; adds and removes members of a group; assigns a group member the Group Manager role; creates and deletes groups; restricts which users can create groups within the Site.
- **Category Administrator**
Creates categories for the Site and define a hierarchy of categories and subcategories available to Site users; can add additional categories anywhere in this hierarchy; and can add or remove attributes for all categories.
- **Records Management Administrator**
Creates, modifies, and deletes file plans; can change content that has been declared a record back to regular content, can freeze record dispositions, close record categories for further filings, and resubmit failed dispositions.

See Also: *Oracle Records Database Application Administrator's Guide* for more information

Administration that can be performed at both the Site and Container levels is divided into the following roles:

- **Quota Administrator**
Manages the quota of allocated disk space for Libraries throughout the Site or Container.
- **Configuration Administrator**

Manages all folders and files, as well as configuration settings. Sets the default and actual configuration of Sites, Containers, Libraries, and folders for categories, version creation, **workflow processes**, and records management.

- **Library Administrator**
Creates and sets the initial configurations and security of Libraries. Can rename and delete libraries, as well as set descriptions. Once the Library is created the Library Administrator cannot update the configuration or security settings.
- **Container Administrator**
Creates and deletes Containers. Enables Library creation requests.
- **Security Administrator**
Manages the security configurations for Sites, Containers, Libraries, folders, and files.
- **Content Administrator**
Manages all Site content; has access to all content in the Site; can unlock files locked by any user; can rename and delete Libraries; and can restore deleted files from the **Archive**.

In addition to administration roles, the following default roles can be assigned at the Site and Container levels:

- **Container Viewer**
Views Containers and their properties. Can also send a request that a Library be created if the option is enabled.
- **Library Creator**
Views Container properties and can create Libraries, as well as view Container properties and create Libraries for sub Containers.

3.2.2 Managing Oracle Content DB User Roles

Security Administrators can assign default and custom roles.

Default roles are sample roles created during the Oracle Content DB installation, and apply to the Site, Container, Library, folder, and file levels. Some default roles can be customized by modifying the permissions.

Custom roles are new roles created by the Role Administrator, and apply to the Library, folder, and file levels.

The following default roles cannot be customized:

- **Administrator**
 - View the properties of a Library, folder, file, or link
 - View the content and category information of a file
 - Add, delete, or modify the category information of a file
 - Update the content of a file that is not version-controlled
 - Rename and update the properties of a Library, file, folder, or link
 - Modify the Library, folder, or file to which a link refers
 - Lock and unlock files
 - Add files to a folder

- Copy, delete, and move folders and files
- Create folders
- Add a version for a version-controlled file
- **Check-in and check-out**
- Add, delete, or modify the security configuration of a Library, folder, or file
- Update and delete Libraries
- Add, delete, or modify any configuration category on a folder or file, except for quota
- Container Viewer
View Containers and their properties. Can also request for Library creation if the option is enabled.
- Discoverer
View the properties of a Library, folder, or file.
- Library Creator
View Container properties and can create Libraries.

The following default roles can be customized:

- Administrative Assistant
 - View the properties of a Library, folder, file, or link
 - Add files to a folder
 - Create folders
 - Add, delete, or modify the security configuration of a folder or file
 - Add, delete, or modify any configuration category on a folder or file, except for quota
 - Modify security settings
- Approver
 - View the properties of a Library, folder, file, or link
 - View the content and category information of a file
 - Add, delete, or modify the category information of a file
 - Update the content of a file that is not version-controlled
 - Rename and update the properties of a file or folder
 - Modify the Library, folder, or file to which a link refers
 - Lock and unlock files
 - Copy folders and files
- Author
 - View the properties of a Library, folder, or file
 - View the content and category information of a file
 - Add, delete, or modify the category information of a file
 - Update the content of a file that is not version-controlled

- Rename and update the properties of a file or folder
- Modify the Library, folder, or file to which a link refers
- Lock and unlock files
- Add files to a folder
- Copy, delete, and move folders and files
- Create folders
- Add a version for a version-controlled file
- Commentator
 - View the properties of a Library, folder, or file
 - View the content and category information of a file
 - Add, delete, or modify the category information of a file
 - Update the content of a file that is not version-controlled
 - Rename and update the properties of a file or folder
 - Modify the Library, folder, or file to which a link refers
 - Lock and unlock files
 - Copy folders and files
- Content Editor
 - View the properties of a Library, folder, or file
 - View the content and category information of a file
 - Add, delete, or modify the category information of a file
 - Update the content of a file that is not version-controlled
 - Rename and update the properties of a file or folder
 - Modify the Library, folder, or file to which a link refers
 - Lock and unlock files
 - Add files to a folder
 - Copy folders and files
 - Create folders
 - Add a version for a version-controlled file
- Custodian
 - View the properties of a Library, folder, or file
 - View the category information of a file
 - Add, delete, or modify the category information of a file
 - Rename and update the properties of a file or folder
 - Modify the Library, folder, or file to which a link refers
 - Lock and unlock files
 - Add files to a folder
 - Copy, delete, and move folders and files

- Create folders
- Limited Author
 - View the properties of a Library, folder, or file
 - View the content and category information of a file
 - Add, delete, or modify the category information of a file
 - Update the content of a file that is not version-controlled
 - Rename and update the properties of a file or folder
 - Modify the Library, folder, or file to which a link refers
 - Lock and unlock files
 - Add files to a folder
 - Create folders
 - Add a version for a version-controlled file
 - Copy folders and files
- Manager
 - View the properties of a Library, folder, or file
 - Add files to a folder
 - Create folders
 - Add, delete, or modify the security configuration of a folder or file
- Organizer
 - View the properties of a Library, folder, or file
 - Add, delete, modify, and view the category information of a file
 - Update the content of a file that is not version-controlled
 - Rename and update the properties of a file or folder
 - Modify the Library, folder, or file to which a link refers
 - Lock and unlock files
 - Copy, delete, and move folders and files
- Reader
 - View the properties of a Library, folder, or file
 - View the content and category information of a file
 - Copy folders and files
- Reviewer
 - View the properties of a Library, folder, or file
 - View the content and category information of a file
 - Copy folders and files

3.3 Oracle Content DB Library Administration

Libraries are the first level in the Oracle Content DB folder hierarchy where content is added. Members must be added to a Library, and a Library is visible only to Site and Container level administrators and members of the Library.

Library Administrators can create and delete Libraries, but they cannot change the configuration settings of the Library after it has been created. Library Administrators can also move Libraries if they have Container Administrator privileges in the target Site or Container. In addition, Library Administrators can rename and set Library descriptions.

3.4 Oracle Content DB Configuration Administration

Configuration Administrators set all the default actions for Libraries, including version creation, categories, workflow, and records management. They can also modify any existing Library or folder settings to which they have access. Configuration Administrators set all the defaults for folders and documents within a Library.

3.4.1 Managing Auditing Tasks

Oracle Content DB provides auditing support through Web Services.

Configuration Administrators can specify the **audit events** that should be captured for **global audit histories** and **object audit histories**. In addition, they can specify the disposition rules for each **audit history**, as well as query against any audit history by specifying criteria from the **primary audit event information**.

See *Oracle Content Database Web Services Java API Reference (Javadoc)* for more information.

3.4.2 Managing Workflow Processes

An Oracle Content DB workflow process defines a set of operations to be executed before or after a particular workflow-enabled action occurs.

A workflow process is triggered as soon as a workflow operation occurs in the target (destination) folder. For example, if the Delete operation is controlled by a workflow process, the workflow process starts automatically when a user deletes an item in the folder.

Oracle Content DB uses Oracle Workflow to manage workflow processes. Oracle Workflow is configured and integrated with Oracle Content DB during Oracle Content DB configuration.

Oracle Content DB comes with two default workflow processes:

- **Parallel vote:** All approvers review the submitted files or request at the same time. The number of approvals or rejections for a completed approval or rejection is set in the Workflow tab of the folder or Library Properties window.
- **Serial approval:** Each approver reviews the submitted files or request in turn, one approver at a time. All reviewers must approve the request to complete the approval process; a single rejection ends the review process, and results in the request being rejected.

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.

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.

3.4.3 Setting Oracle Content DB Library Defaults

Configuration Administrators can set the following default actions for a Library:

- Version creation
 - Set the version model (Automatic, Manual, or No Versioning)
 - Set the maximum number of versions to retain
 - Enable automatic version labeling and select label format
 - Disallow version model selections to be modified
- Categories
 - Select which categories are available
 - Select defaults for all categories available in the system, such as whether a category must be associated with all content, or whether a particular attribute should be required
 - Disallow category selections to be modified
- Workflow process
 - Select which operations are controlled by workflow processes
 - Select the workflow process used to control each workflow-controlled operation
 - Specify if a workflow requires approval
 - Add and remove **approvers**
 - Enable automatic approval of requests sent by approvers
 - Set the number of approvals required to approve
 - Set the number of rejections required to reject
 - Disallow workflow selections to be modified
- Records Management
 - Select the record category to enforce on all content
 - Disallow Records Management selections to be modified

3.5 Oracle Content DB Content Administration

Content Administrators manage all content within a Site. They have access to and can perform various file operations on all Site content. Content Administrators have access to all Libraries, with all permissions except for the ability to set or configure security. Content Administrators can delete Libraries, as well as manage the Archive, and can perform various operations on files within the Archive.

In addition, Content Administrators can view properties of a Site or Container, depending on whether or not they have Site-level or Container-level access.

3.5.1 Managing Oracle Content DB Content

Content Administrators manage and have access to all content in a Site. Content Administrators can perform the following file operations:

- Lock and unlock files
- Set and view content
- Set and view categories
- Add version-controlled files
- Delete Libraries
- Create, copy, and delete folders and files
- Modify Library, folder, and file names and descriptions
- Move files to and from various folders within a Site

Content Administrators can also set virus scanning to detect and repair infected files.

3.5.2 Managing the Oracle Content DB Archive

Content Administrators manage and have access to all content within the Archive. In addition, Content Administrators can restore and remove files from the Archive. However, Content Administrators cannot change the security settings of content in the Archive.

3.6 Oracle Content DB Quota Administration

Quota is the measurement of storage usage in Oracle Content Database. Each Library is allocated a quota by the Quota Administrator. The contents of each Library and Trash folder count against the Library's allocated quota. When the Library's quota is exceeded, Library members cannot store additional content in the Library.

The Quota Administrator can modify the quota of any Library. Approving a quota request automatically changes the quota for the Library.

Quota Administrators can view and change quota through the Library Properties page. Quota Administrators can also browse or search for a Library by name. The Quota Administrator can view the allocated and used quota and change the allocated quota for any Library.

Quota Administrators can view files, folders, and the configuration of all Libraries, but they do not have access to the content.

Quota is also allocated and tracked at the Site level. Site quota is managed by the system administrator.

3.6.1 Managing Oracle Content DB Library Quota

Quota Administrators manage all the quota within a Site, and can perform the following tasks:

- Search for Libraries within a Site
- View the consumed quota for a Site

- Assign the default quota for all newly created Libraries within a Site
- Approve requests for additional Library quota
- Modify allocated Library quota

3.7 Other Oracle Content DB Roles

In addition to administration roles, there are two additional roles that can be assigned at the Site and Container levels: Container Viewer and Library Creator.

Container Viewers can view Containers and their properties. All users are assigned the Container Viewer role on the Site folder.

Library Creators can view Container properties and can create Libraries at the Site or Container level.

These roles can be accessed without being in **Administration Mode**.

Glossary

roles

Oracle Content DB security is based on roles, which specify what kind of access a user has to files, folders, Libraries, Containers, and links in Oracle Content DB. Each role is made up of a set of permissions — a permission represents the ability to perform a specific Oracle Content DB action or operation.

Administration Mode

Oracle Content DB Administration Mode provides access to application administration functions such as allocating quota and assigning roles.

application administration

Oracle Content DB application administration involves managing users, quota, Libraries, security, categories, content, and records.

approver

An approver, in a workflow request, is a specified user who must either approve or reject the request.

archive

Each Oracle Content DB Site contains an Archive folder. When a file or folder is deleted, the item is moved to the Trash folder of the Library containing the file or folder. When an item is deleted from the Trash folder, the item is moved to the Archive folder. Depending on the Site's configuration, items in the Archive folder may be automatically deleted after a specified period of time. Files and folders in the Archive folder can be recovered and restored by the Site's Content Administrator.

audit event

A record of an Oracle Content DB operation that is stored as a record of an operation or operation attempt in the repository. This includes the information selected when discovered through an audit search.

audit history

A set of audit events that can be searched. Audit history can be used to associate a set of audit events with individual objects.

category

A category is a unit of information by which files and folders may be classified. In Oracle Content DB, users associate metadata with a file or folder by assigning one or more categories to it. Users can use categories to create intelligent searches for files and folders. Categories may be divided into subcategories, and may have one or more

category attributes. Categories are created and configured for your Site by the Oracle Content DB Category Administrator.

category attribute

A category attribute is additional information added to define a category in Oracle Content DB.

check-out/check-in

One mechanism for creating a new version of a file is check-out/check-in. A user checks out a document to indicate his intention to create a new version. Each document can be checked out by only one user at a time, enforced by a locking mechanism. Checking in a file creates a new version from the working copy, and then destroys the working copy. The new version becomes the latest version of the document, and like any document version, is immutable and thus cannot be further updated. The lock acquired at check-out is released, allowing other users to check out the document.

Container

A Container is a special type of Oracle Content DB folder. The Container provides users and Administrators with greater flexibility in organizing files and folders. For instance, Containers could be used to organize an Oracle Content DB Site by a company's business divisions or office locations. Only Libraries and Containers can be stored in a Container.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a standard protocol for transferring files between computers over a network.

global audit history

Global audit history contains a wide set of audit events for all objects. It can be searched by Configuration Administrators and is the source of audit events used when generating a global audit report.

Library

A Library is a special type of folder in Oracle Content DB. Unlike Containers and regular folders, each Library has a Trash Folder and an allocated amount of disk space.

metadata

Data that provides information about, or documentation of, other data managed within an application or environment. In Oracle Content DB, users associate metadata with a file or folder by assigning one or more categories to the file or folder.

object audit history

Object audit history contains audit events associated with a specific object.

Oracle Internet Directory

Oracle Internet Directory is an online directory, which is a specialized database that stores information in a hierarchical format for fast lookup and retrieval. It implements Lightweight Directory Access Protocol (LDAP), an industry-standard protocol for accessing online directory services. Oracle Content DB users are created in Oracle Internet Directory.

Oracle Workflow

Oracle Workflow is a system that supports business process definition, automation, and integration.

Personal Library

A Personal Library is a Library that is set up for, and managed by, a single user. Personal Libraries may or may not be available, depending on whether or not the User Administrator has enabled Personal Libraries in your Oracle Content DB Site.

primary audit information

A collection of information present for all audit events. This includes the following:

- Audit event operation type: The specific type of operation that occurred or was attempted
- Audit event date: The time and date the audit event was created
- Audit event creator: The user that initiated the operation to create an audit event
- Audit event target: The primary object of which the audit event was created
- Audit event domain: The Site of the audit event target
- Audit event operation successful: Indicates if the audited operation was successful (true), or merely attempted but failed (false)

quota

Quota is the amount of disk space allocated for a Library or for a user.

Site

In Oracle Content DB, a Site is a discrete organizational entity whose users can collaborate on files and folders. Users in one Site do not have access to the content of users in another Site. Oracle Content DB Sites are based on Identity Management realms.

system administration

Oracle Content DB system administration involves the following tasks:

- Installing and configuring Oracle Content DB
- Customizing Oracle Content DB deployment by enabling virus checking, the FTP server, the OmniPortlet, retention hardware, or other scenarios
- Managing the Oracle Content DB instances, nodes, services, and servers
- Performing system tuning and troubleshooting
- Adding, deleting, and managing Sites
- Registering custom workflow processes

UTF-8

A character encoding format used to represent a sequence of 16-bit Unicode characters with an equivalent sequence of 8-bit characters, no one of which is zero. This sequence of characters can be represented using an ordinary C language string. If your operating system does not support UTF-8, you can enter another Distributed Authoring and Versioning (DAV) character encoding format in user preferences.

version control

A version controlled file has a version history, consisting of a series of versions. Each version has both content and metadata for the document. Updating the document's content or metadata causes a new version to be created. In general, once a version is created it is immutable. If versioning is enabled for a folder or Library, and Manual Versioning is selected for the Versioning Model, users can create a version-controlled document only through explicit check-out and check-in operations. If versioning is enabled for a folder or Library, and Automatic Versioning is selected for the Versioning Model, updates to a file's content or category information will result in the automatic creation of a new version.

version history

Information about the saved versions of a file. Accessible from the Version Properties window for a file, the version history displays the working copy of the file and a table of the file's saved versions.

Web Distributed Authoring and Versioning (WebDAV)

WebDAV is the Internet Engineering Task Force (IETF) standard for collaborative authoring on the World Wide Web. It consists of a set of extensions to the Hypertext Transfer Protocol (HTTP). These extensions facilitate collaborative editing and file management among users located remotely from each other on the Internet.

workflow process

A workflow process defines a series of events that must be achieved before a certain workflow-enabled action takes place. There are two kinds of workflow processes:

- Parallel: In a parallel review workflow process, all approvers review the submitted files or request at the same time. The number of approvals or rejections for a completed approval or rejection is set in the **Workflow** tab of the folder or Library Properties window.
- Serial: In a serial review workflow process, each approver reviews the submitted files or request in turn, one approver at a time. All reviewers must approve the request to complete the approval process; a single rejection ends the review process, and results in the request being rejected.

working copy

A working copy is the editable copy of a file. When a file is checked out, a server-resident working copy is created as a copy of the latest version. Similar to a file version, the working copy has both content and metadata for the document, and can be overwritten by that user any number of times. The working copy is visible only to the user who checked out the document. The user who checked out the document may update the working copy.

Index

A

administration
 Application, 1-2
Administrator Roles
 managing, 3-2
administrators
 System, 1-1
Application Administration, 1-2
Archive
 managing, 3-9

C

Category Administration
 about, 2-3
Category Properties
 managing, 2-3
Configuration Administration
 about, 3-7
Container Administration
 about, 3-1
Container Viewer
 about, 3-10
Containers
 managing, 3-1
Content
 managing, 3-9
Content Administrator
 about, 3-8
Content Management
 about, 1-1

G

Groups
 managing, 2-3

L

Library Administrator
 about, 3-7
Library Creator
 about, 3-10
Library Defaults
 setting, 3-8
Library Quota

managing, 3-9

M

Miscellaneous Roles
 about, 3-10

O

Oracle Content Services
 about, 1-1
 first sign in, 1-2
Oracle Content Services Administration
 about, 1-1
orcladmin
 about, 1-2

Q

Quota Administration
 about, 3-9

R

Role Administration
 about, 2-1

S

Security Administration
 about, 3-2
Site Administration
 about, 2-1
System Administrator, 1-1

U

User Access Roles
 managing, 3-3
Users
 managing, 2-3

