

Oracle® Fusion Middleware

Administering Oracle WebCenter Content



14c (14.1.2.0.0)

F89677-01

December 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Fusion Middleware Administering Oracle WebCenter Content, 14c (14.1.2.0.0)

F89677-01

Copyright © 2010, 2024, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	xxviii
Documentation Accessibility	xxviii
Diversity and Inclusion	xxviii
Related Documents	xxviii
Conventions	xxviii
WebCenter Content Terminology	xxix

Part I Introduction to Oracle WebCenter Content

1 Introduction to Administering Oracle WebCenter Content

1.1 Introduction to Oracle WebCenter Content	1-1
1.1.1 Content Server	1-1
1.1.2 Content Management	1-1
1.2 Basic Tasks for Administering Oracle WebCenter Content	1-2

Part II Getting Started

2 Getting Started Administering Oracle WebCenter Content

2.1 Understanding System Administrator Roles and Responsibilities	2-1
2.2 Understanding System Administrator Interfaces	2-2
2.2.1 About the WebCenter Content Server Administration Interface	2-2
2.2.2 About Oracle Enterprise Manager Fusion Middleware Control	2-5
2.2.3 About the Oracle WebLogic Server Administration Console	2-6
2.3 Understanding WebCenter Content System Administration Tools	2-6
2.3.1 About Content Server Tools	2-7
2.3.1.1 Management Pages	2-7
2.3.1.2 Applications	2-7
2.3.1.3 Utilities	2-8
2.3.1.4 IdcShell Command-Line Tool	2-8

2.3.2	About Oracle WebLogic Scripting Tool (WLST)	2-9
2.4	Accessing Oracle WebCenter Content	2-9
2.4.1	Accessing WebCenter Content Using Fusion Middleware Control	2-9
2.4.1.1	Logging In to Fusion Middleware Control	2-9
2.4.1.2	Navigating to the Content Server Home Page	2-10
2.4.2	Accessing WebCenter Content Instances Using a Web Browser	2-11
2.4.2.1	Accessing a Content Server Instance	2-12
2.4.2.2	Accessing a WebCenter Content: Inbound Refinery Instance	2-12
2.4.2.3	Accessing a WebCenter Content: Imaging Instance	2-12
2.4.2.4	Accessing a WebCenter: Records Instance	2-13
2.5	Configuring WebCenter Content User Interface	2-13
2.5.1	Setting up the Remote Intradoc Client (RIDC)	2-14
2.5.2	Setting Additional Content Server Parameters	2-14
2.5.3	Configuring Application Parameters	2-15
2.5.4	Enabling Full-Text Searching	2-15
2.5.5	Generating Thumbnails and Web-Viewable Renditions	2-16
2.5.6	Configuring Digital Asset Management in Content Server	2-16
2.5.7	Configuring Extended Features in Content Server	2-17
2.5.8	Completing the Workflow Configuration	2-17
2.6	Associating the WebCenter Content User Interface with Content Server	2-18
2.6.1	Configuring a JAX-WS Connection from the WebCenter Content User Interface Server to Content Server	2-18
2.6.2	Configuring a Secured Connection from the WebCenter Content User Interface Server to Content Server	2-22
2.6.3	Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server	2-23
2.6.3.1	Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server With Require Client Authentication	2-23
2.6.3.2	Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server Without Require Client Authentication	2-27
2.6.4	Configuring an IDC Connection from the WebCenter Content User Interface Server to Content Server	2-28
2.6.5	Configuring an HTTP Connection from the WebCenter Content User Interface Server to Content Server	2-28
2.6.5.1	Importing the Certificate from the Oracle WebCenter Content Domain to the WebCenter Content User Interface Domain	2-29
2.6.6	Configuring an HTTPS Connection to Content Server Without a Certificate	2-30

3 Managing System Processes

3.1	Starting and Stopping Content Server and Inbound Refinery	3-1
3.2	Starting and Stopping Content Server and Inbound Refinery Using Fusion Middleware Control	3-2
3.2.1	Starting Content Server or Inbound Refinery Using Fusion Middleware Control	3-2

3.2.2	Stopping Content Server or Inbound Refinery Using Fusion Middleware Control	3-2
3.2.3	Restarting Content Server or Inbound Refinery Using Fusion Middleware Control	3-3
3.3	Starting and Stopping Content Server Using WebLogic Server	3-3
3.3.1	Starting Content Server Using WebLogic Server Administration Console	3-4
3.3.2	Stopping Content Server Using WebLogic Server Administration Console	3-4
3.3.3	Restarting Content Server Using WebLogic Server Administration Console	3-4
3.4	Starting and Stopping Content Server Using Scripts	3-4
3.4.1	Starting Content Server Using Scripts	3-5
3.4.2	Stopping Content Server Using Scripts	3-5
3.4.3	Restarting Content Server Using Scripts	3-6
3.5	Running Content Server Administration Applications	3-6
3.5.1	Running Administration Applications as Applets	3-6
3.5.2	Running Administration Applications via the Oracle WebCenter Content Administration App	3-7
3.5.3	Running Administration Applications in Standalone Mode	3-9
3.5.3.1	Running a Standalone Application on a UNIX System	3-10
3.5.3.2	Running a Standalone Application on a Windows System	3-10
3.5.3.3	Configuring a System Database Provider for Standalone Mode	3-10
3.5.3.4	Configuring a JDBC Database Driver for Standalone Mode	3-11
3.5.3.5	Configuring an External Database Provider for Standalone Mode	3-12
3.6	Using the IdcShell Command-Line Tool to Run Idoc Script	3-12

4 Batch Loading Content

4.1	About Batch Loading	4-1
4.1.1	About Batch Load File Records	4-2
4.1.2	About Batch Load Actions	4-2
4.1.3	About Batch Load Insert Action	4-2
4.1.3.1	Insert Requirements	4-3
4.1.3.2	Insert Example	4-4
4.1.4	About Batch Load Delete Action	4-5
4.1.4.1	Delete Requirements	4-6
4.1.4.2	Delete Example	4-7
4.1.5	About Batch Load Update Action	4-7
4.1.5.1	Update Requirements	4-8
4.1.5.2	Update Example 1	4-9
4.1.5.3	Update Example 2	4-10
4.1.6	About Optional Batch Load File Parameters	4-10
4.1.7	About Custom Metadata Fields	4-13
4.2	Preparing a Batch Load File	4-13
4.2.1	About Preparing a Batch Load File	4-13
4.2.2	Mapping Files	4-14

4.2.2.1	Mapping File Formats	4-14
4.2.2.2	Mapping File Values	4-14
4.2.3	Creating a Batch Load File from the BatchBuilder Window	4-16
4.2.4	Creating a Mapping File	4-16
4.2.5	Creating a Batch Load File from the Command Line	4-17
4.2.5.1	Windows Example	4-18
4.2.5.2	UNIX Example	4-18
4.3	Running the Batch Loader	4-18
4.3.1	About Running the Batch Loader	4-19
4.3.2	Batch Loading from the Batch Loader Window	4-19
4.3.3	Batch Loading from the Command Line	4-19
4.3.3.1	Windows Example	4-20
4.3.3.2	UNIX Example	4-20
4.3.4	Using the IdcCommand Utility and Remote Access	4-20
4.3.4.1	Batch Load Command Files	4-21
4.3.4.2	Preparing for Remote Batch Loading	4-21
4.3.5	Batch Loading Content as Metadata Only	4-25
4.3.6	Batch Loader -console Command Line Switch	4-25
4.3.7	Adding a Redirect	4-26
4.3.8	Correcting Batch Load Errors	4-26
4.4	Optimizing Batch Loader Performance	4-27
4.5	Best Practice Case Study	4-28
4.5.1	Background Information	4-28
4.5.2	Preliminary Troubleshooting	4-28
4.5.3	Solution	4-28

Part III Monitoring Oracle WebCenter Content Server

5 Monitoring Content Server Status

5.1	Viewing Content Server Status	5-1
5.2	Viewing Content Server Console Output	5-1
5.3	Viewing System Configuration Information	5-2
5.4	Viewing System Audit Information	5-3
5.4.1	System Audit General Information	5-3
5.4.2	System Audit Localization Information	5-3
5.4.3	System Audit Tracing Sections Information	5-4
5.4.4	System Audit Cache Information	5-4
5.4.5	System Audit Configuration Entry Information	5-5
5.4.6	System Audit Component Report Information	5-5
5.5	Viewing Server Output	5-5

5.6	Viewing Event Output	5-6
5.7	Checking Schema Cache	5-6
5.8	Viewing Localization Audit Information	5-6
5.9	Monitoring Scheduled Jobs	5-6
5.9.1	Viewing Active Scheduled Jobs	5-7
5.9.2	Viewing Scheduled Jobs History	5-7
5.9.3	Modifying a Scheduled Job	5-7
5.9.4	Canceling or Deleting a Scheduled Job	5-7

6 Monitoring Content Server Log Files

6.1	Introduction to Managing Content Server Log Files	6-1
6.2	About Content Server Log File Characteristics	6-1
6.3	Accessing Content Server Logs	6-2
6.4	Accessing Archiver Logs	6-3
6.5	Accessing Inbound Refinery Logs	6-3

7 Monitoring Content Server and Inbound Refinery Using Fusion Middleware Control

7.1	Managing Log Information Using Fusion Middleware Control	7-1
7.1.1	Viewing Log Information Using Fusion Middleware Control	7-1
7.1.2	Modifying Log Information Using Fusion Middleware Control	7-1
7.2	Viewing Performance Information Using Fusion Middleware Control	7-2
7.3	Viewing MBean Information Using Fusion Middleware Control	7-5

Part IV Administering System Configuration

8 Configuring System Properties

8.1	About System Properties	8-1
8.2	Configuring System Properties Using Fusion Middleware Control	8-2
8.2.1	Modifying Content Security Configuration Using Fusion Middleware Control	8-3
8.2.2	Modifying General Configuration Using Fusion Middleware Control	8-4
8.2.3	Modifying Internet Configuration Using Fusion Middleware Control	8-4
8.2.4	Modifying Email Configuration Using Fusion Middleware Control	8-5
8.3	Configuring General Options	8-6
8.3.1	Revision Label Sequence	8-7
8.3.1.1	Revision Label Ranges	8-7
8.3.1.2	Revision Examples	8-7
8.3.1.3	Revision Configuration Settings	8-8
8.3.2	Chunking Function	8-8

8.3.3	Vertical Clustering and Scale-Up	8-9
8.3.3.1	Extending WebCenter Content: Inbound Refinery Components	8-9
8.3.3.2	WebCenter Content Scaleup and Ports	8-9
8.4	Configuring Content Security	8-9
8.5	Configuring Internet Information Using Content Server	8-10
8.6	Configuring System Database Properties	8-11
8.6.1	About the Content Server System Database	8-12
8.6.2	Configuring Content Server for IBM DB2 Database Searches	8-12
8.7	Configuring Oracle Content Management Integration Settings	8-13
8.8	Configuring Server Properties	8-14
8.9	Configuring Localization Properties	8-15
8.9.1	Configuring Date Format	8-15
8.9.2	Configuring Interface Language	8-16
8.9.2.1	Specifying a Locale	8-16
8.10	Configuring Paths Properties	8-16
8.11	Configuring Trash	8-17

9 Managing Components

9.1	About Components	9-1
9.2	Using the Component Manager	9-7
9.2.1	Viewing Information about a Component Using the Component Manager	9-8
9.2.2	Enabling or Disabling a Component Using the Component Manager	9-8
9.2.3	Installing a Component Using the Component Manager	9-9
9.2.4	Uninstalling a Component Using the Component Manager	9-10
9.2.5	Downloading a Component Using the Component Manager	9-10
9.2.6	Modifying a Component Configuration Using the Component Manager	9-11
9.2.6.1	Modifying a Component Using Component Manager	9-11
9.2.6.2	Modifying a Component Using the Configuration for instance Page	9-11
9.3	Managing Components Using Fusion Middleware Control	9-11
9.3.1	Using the Component Manager	9-12
9.3.1.1	Viewing Component Information Using Fusion Middleware Control	9-12
9.3.1.2	Enabling or Disabling a Component Using Fusion Middleware Control	9-13
9.3.2	Using the Advanced Component Manager	9-14
9.3.2.1	Enabling or Disabling a Component Using Fusion Middleware Control	9-14
9.3.2.2	Installing a Component Using Fusion Middleware Control	9-15
9.3.2.3	Uninstalling a Component Using Fusion Middleware Control	9-15
9.3.2.4	Downloading a Component Using Fusion Middleware Control	9-16
9.3.2.5	Modifying a Component Configuration Using Fusion Middleware Control	9-16
9.4	Managing Components Using the Command Line	9-17
9.5	Updating Component Configurations	9-18
9.5.1	Updating ContentTracker Component Configuration	9-18

9.5.2	Updating DesktopIntegrationSuite Component Configuration	9-19
9.5.2.1	Configuring Windows Explorer Preview Pane	9-20
9.5.3	Updating EmailMetadata Component Configuration	9-20
9.5.4	Updating OCM Component Configuration	9-22
9.5.5	Updating PDFWatermark Component Configuration	9-23
9.5.6	Updating SiteStudio Component Configuration	9-24
9.6	Creating Components Using the Component Wizard	9-24
9.6.1	Component Wizard Overview	9-25
9.6.2	Working with Java Code	9-27
9.6.3	Editing the Readme File	9-27
9.6.4	Creating a Component Using Component Wizard	9-27
9.6.4.1	Creating an Environment Resource for a New Component	9-28
9.6.4.2	Creating a Template Resource	9-29
9.6.4.3	Creating a Query Resource	9-31
9.6.4.4	Creating a Service Resource	9-32
9.6.4.5	Creating a HTML Include	9-34
9.6.4.6	Creating a String Resource	9-35
9.6.4.7	Creating a Dynamic Table Resource	9-36
9.6.4.8	Creating a Static Table Resource	9-37
9.6.4.9	Enabling the Component	9-38
9.6.5	Additional Component Wizard Tasks	9-38
9.6.5.1	Building a Component Zip File	9-38
9.6.5.2	Working with Installation Parameters	9-39
9.6.5.3	Enabling and Disabling a Component	9-40
9.6.5.4	Removing a Component	9-41
9.6.5.5	Opening a Component	9-41
9.6.5.6	Configuring the Default HTML Editor	9-41
9.6.5.7	Unpackaging a Component	9-42
9.6.5.8	Adding an Unpackaged Component	9-43

10 Managing Search Features

10.1	Managing OracleTextSearch	10-1
10.1.1	Considerations for Using OracleTextSearch	10-1
10.1.2	Oracle Text Features and Benefits	10-2
10.1.2.1	Indexing and Query Speeds and Techniques	10-2
10.1.2.2	Fast Rebuild	10-3
10.1.2.3	Query Syntax	10-3
10.1.2.4	OracleTextSearch Operators	10-4
10.1.2.5	Case Sensitivity and Stemming Rules	10-4
10.1.2.6	Search Results Data Clustering	10-5
10.1.2.7	Snippets	10-5

10.1.2.8	Additional Changes	10-5
10.1.3	Configuring OracleTextSearch for Content Server	10-6
10.1.4	Managing OracleTextSearch	10-7
10.1.4.1	Determining Fields to Optimize	10-7
10.1.4.2	Assigning/Editing Optimized Fields	10-7
10.1.4.3	Performing a Fast Rebuild	10-8
10.1.4.4	Modifying the Fields Displayed on Search Results	10-9
10.1.5	Searching with OracleTextSearch	10-9
10.1.6	Using Metadata Wildcards	10-10
10.1.7	Using Internet-Style Search Syntax	10-10
10.1.8	Adjusting the Score on OracleTextSearch Results	10-11
10.1.9	Customizing Search Results with OracleTextSearch	10-12
10.1.9.1	About Batch Load File Records	10-14
10.2	Configuring Full-Text Database Search Index	10-14
10.3	Managing Elasticsearch	10-15
10.3.1	Elasticsearch Features and Benefits	10-15
10.3.1.1	How the Rebuild Feature Works in Elasticsearch?	10-16
10.3.1.2	Fast Rebuild	10-16
10.3.1.3	Full Rebuild	10-16
10.3.1.4	Elasticserver ReIndex	10-16
10.3.1.5	Sorting	10-17
10.3.1.6	Facets	10-17
10.3.1.7	Search Operators and Searching	10-17
10.3.1.8	Stemming	10-18
10.3.1.9	Snippets	10-18
10.3.1.10	Highlighting	10-19
10.3.2	Configuring Elasticsearch	10-19
10.3.2.1	Updating ESnode.properties	10-20
10.3.2.2	Using SecureES.sh on Unix	10-21
10.3.2.3	Using SecureES.cmd on Windows	10-21
10.3.2.4	Securing Elasticsearch	10-22
10.3.2.5	Securing Other Nodes of Cluster	10-23
10.3.2.6	Start Elasticsearch Cluster	10-24
10.3.2.7	Configuring Elasticsearch for WebCenter Content	10-24
10.3.2.8	Monitoring Elasticsearch Cluster Health	10-25
10.3.2.9	Configuring Index Settings	10-25
10.3.3	Migrating Existing Search Indexes to Elasticsearch Server	10-27
10.4	Managing OpenSearch	10-29
10.4.1	OpenSearch Features and Benefits	10-29
10.4.1.1	How the Rebuild Feature Works in OpenSearch?	10-30
10.4.1.2	Fast Rebuild	10-30
10.4.1.3	Full Rebuild	10-30

10.4.1.4	OpenSearch ReIndex	10-30
10.4.1.5	Sorting	10-30
10.4.1.6	Facets	10-31
10.4.1.7	Search Operators and Searching	10-31
10.4.1.8	Stemming	10-32
10.4.1.9	Snippets	10-32
10.4.1.10	Highlighting	10-32
10.4.2	Configuring OpenSearch	10-33
10.4.2.1	Configuring OpenSearch for WebCenter Content with OCI	10-33
10.4.2.2	Configuring OpenSearch for WebCenter Content	10-35
10.4.2.3	Monitoring OpenSearch Cluster Health	10-36
10.4.2.4	Configuring Index Settings	10-36
10.4.3	Migrating Existing Search Indexes to OpenSearch	10-37

11 Configuring the Search Index

11.1	Variances in Indexing Tools and Methods	11-1
11.2	Configuring the Search Index for Databases	11-1
11.2.1	Configuring Metadata Search with All Databases	11-3
11.2.2	Configuring Full-Text Search with SQL Server	11-3
11.2.3	Configuring Full-Text Search with OracleTextSearch	11-4
11.2.4	Optimizing Full Text Search	11-4
11.2.5	Configuring Database-Supported File Formats	11-5
11.2.5.1	FormatMap	11-5
11.2.5.2	ExceptionFormatMap	11-6
11.2.6	Modifying Default Indexing	11-6
11.2.6.1	Indexing Resource Defaults	11-6
11.2.6.2	Indexing Resource Include Example	11-7
11.3	Working with the Search Index	11-8
11.3.1	About the Search Index	11-8
11.3.2	Updating the Search Index	11-8
11.3.3	Rebuilding the Collection	11-8
11.3.4	Configuring the Search Index Update or Collection Rebuild	11-9
11.3.5	Full-Text Indexing	11-9
11.3.6	Disabling Full-Text Indexing	11-10
11.3.7	Indexing Native Files by Default	11-10
11.3.8	Indexing Email and Attachments	11-10
11.4	Managing Zone Text Fields	11-11
11.4.1	About Zone Text Fields	11-11
11.4.2	Enabling and Disabling Zone Text Fields	11-12
11.4.3	Changing the Minimum Length of Text Fields	11-14
11.4.4	Disabling Database Search Contains Operator	11-14

11.5	Searching Content Using Oracle Query Optimizer	11-15
11.5.1	About Oracle Query Optimizer	11-15
11.5.2	Query Optimization Process	11-16
11.5.2.1	Stage 1: Query Analysis	11-17
11.5.2.2	Stage 2: Parsing	11-17
11.5.2.3	Stage 3: Normalization	11-17
11.5.2.4	Stage 4: Select Hint	11-18
11.5.2.5	Stage 5: Reformat Query	11-18
11.5.3	How Reformatted Queries Optimize Searches	11-18
11.5.3.1	Example 1: Reformatting a Query by Adding a Single Hint	11-18
11.5.3.2	Example 2: Reformatting a Query by Adding Multiple Hints	11-19
11.5.4	Types of Recognized Hints	11-19
11.5.5	Query Hints Syntax	11-20
11.5.5.1	Oracle Hint Syntax	11-20
11.5.5.2	Content Server Hint Syntax	11-20
11.5.6	Additional Supported Sort Constructs	11-21
11.5.7	Hint Rules Table	11-21
11.5.7.1	Key	11-22
11.5.7.2	Table	11-23
11.5.7.3	Column	11-23
11.5.7.4	Operators	11-23
11.5.7.5	Index	11-24
11.5.7.6	Order	11-24
11.5.7.7	Values	11-24
11.5.7.8	AllowMultiple	11-25
11.5.7.9	Disabled	11-25
11.5.8	Edit Hint Rules Form	11-26
11.5.9	The Hint Cache	11-26
11.5.9.1	Reusing Hint Cache Entries	11-26
11.5.9.2	Hint Cache Management	11-27
11.5.9.3	Default Capacity Algorithm	11-27
11.5.9.4	Origin of Hint Cache Keys	11-28
11.5.9.5	Hint Cache Persistence	11-28
11.5.10	Using Hint Rules	11-28
11.5.10.1	Adding and Enabling New Hint Rules	11-28
11.5.10.2	Editing Existing Hint Rules	11-29
11.5.10.3	Disabling Hint Rules	11-29
11.5.10.4	Enabling Hint Rules	11-29
11.5.10.5	Removing Hint Rules	11-29
11.5.11	Using the Query Converter	11-30
11.5.11.1	Accessing the Query Converter Page	11-30
11.5.11.2	Converting a Data Source	11-30

11.5.11.3	Converting a Query	11-30
11.5.11.4	Editing a Converted Data Source or Query	11-31
11.5.12	Updating the Hint Cache	11-31
11.5.12.1	Accessing the Hint Cache Updater Page	11-32
11.5.12.2	Checking the Hint Cache from a Data Source	11-32
11.5.12.3	Checking from a Query	11-32
11.5.12.4	Modifying an Existing Hint Cache Query Using Data Source	11-33
11.5.12.5	Modifying an Existing Hint Cache Using a Query	11-34
11.5.12.6	Removing a Hint Cache Data Source Entry	11-34
11.5.12.7	Removing a Hint Cache Query	11-34
11.6	Improving Search Performance	11-35
11.6.1	Improving Database Search on the Title Field	11-35
11.6.2	Reducing Unnecessary SQL Queries	11-35

12 Managing a File Store System

12.1	Introduction to the File Store System	12-1
12.1.1	Data Management	12-2
12.1.1.1	File Management	12-2
12.1.1.2	Metadata Management	12-3
12.1.1.3	File Stores	12-3
12.1.2	File Store Provider Features	12-3
12.2	About the File Store Provider Upgrade	12-3
12.2.1	DefaultFileStore Settings	12-4
12.2.2	Empty Storage Rule	12-4
12.3	Managing the File Store Provider	12-5
12.3.1	Understanding File Store Provider Storage Principles	12-6
12.3.1.1	Using Storage Rules on Renditions to Determine Storage Class	12-7
12.3.1.2	Understanding Path Construction and URL Parsing	12-8
12.3.2	About File Store Provider Modifications to Content Server	12-9
12.3.2.1	Database Options	12-10
12.3.2.2	Content Server Metadata Fields	12-10
12.3.3	File Store Provider Resource Tables	12-11
12.3.3.1	PartitionList Table	12-11
12.3.3.2	StorageRules Table	12-12
12.3.3.3	PathMetaData Table	12-12
12.3.3.4	PathConstruction Table	12-13
12.3.3.5	FileSystemFileStoreAlgorithmFilters Table	12-14
12.3.3.6	FileStorage Table	12-14
12.3.3.7	FileCache Table	12-15
12.3.4	Working with the File Store Provider	12-15
12.3.4.1	Adding or Editing a Partition	12-15

12.3.4.2	Editing the File Store Provider	12-16
12.3.4.3	Adding or Editing a Storage Rule	12-16
12.4	Sample Implementations of File Store Provider	12-17
12.4.1	Example PathMetaData Table Options	12-18
12.4.2	Configuration for Standard File Paths	12-18
12.4.2.1	Defining the Storage Rule	12-18
12.4.2.2	Defining the Path Construction	12-19
12.4.3	Configuration for a Webless or Optional Web Store	12-20
12.4.3.1	Defining the Storage Rule Example	12-20
12.4.3.2	Defining the Path Construction Example	12-21
12.4.4	Configuration for Database Storage	12-21
12.4.5	Configuration for OCI Object Storage	12-22
12.4.6	Configuration for OCI Object Storage Cache	12-23
12.4.7	Managing Object Storage Migration	12-24
12.4.7.1	Configuration Parameters	12-24
12.4.7.2	Accessing Object Storage Migration Tool	12-25
12.4.7.3	Viewing Migration Progress	12-25
12.4.7.4	Previewing Migration	12-26
12.4.7.5	Retrying Failures	12-27
12.4.7.6	Configuring Media Drive Location	12-27
12.4.8	Altered Path Construction and Algorithms	12-27
12.4.8.1	Using Partitioning	12-27
12.4.8.2	Adding a Partition to the Weblayout Path	12-27
12.4.8.3	Limiting the Number Files in a Directory	12-28
12.5	Using Sun Storage Archive Manager	12-28
12.5.1	About SAM-QFS	12-29
12.5.2	Considerations for Using SAM-QFS	12-29
12.5.3	Installing SAM-QFS	12-30
12.5.4	Configuring Content Server and SAM-QFS with WORM	12-30
12.5.4.1	Configuring the Vault Path	12-30
12.5.4.2	Configuring the File Store Provider to Enable WORM	12-30

13 Configuring Providers

13.1	About Content Server Providers	13-1
13.2	Choosing an Appropriate Provider	13-2
13.2.1	When to Use an Outgoing Provider	13-2
13.2.2	When to Use a Database Provider	13-3
13.2.3	When to Use an Incoming Provider	13-3
13.2.4	When to Use a Preview Provider	13-3
13.2.5	When to Use a JpsUser Provider	13-4
13.2.5.1	Retrieving Direct and Indirect Group Membership for Users	13-5

13.2.5.2	Custom Field Mapping from LDAP Server	13-5
13.2.5.3	Single Character Mapping for Accounts	13-6
13.2.5.4	Credential Map for JpsUser Provider	13-6
13.2.6	When to Use a Ldapuser Provider	13-6
13.3	Understanding Content Server Security Providers	13-7
13.3.1	Planning to Use Security Providers	13-8
13.3.1.1	Keepalive Connections	13-9
13.3.1.2	SSL Connections	13-9
13.3.1.3	Additional Security Configuration	13-10
13.3.2	Keystores and Truststore	13-10
13.3.2.1	When to Use Keystores and a Truststore	13-10
13.3.2.2	Specifying Keystore and Truststore Information	13-11
13.3.2.3	Generating a Keystore	13-11
13.3.2.4	Creating a Truststore	13-12
13.4	Managing Providers	13-13
13.4.1	Adding an Outgoing Provider	13-13
13.4.2	Adding a Database Provider	13-14
13.4.3	Adding an Incoming Provider	13-15
13.4.4	Adding a Preview Provider	13-15
13.4.5	Adding an Incoming Security Provider	13-15
13.4.6	Adding an Outgoing Security Provider	13-16
13.4.7	Adding a JpsUser Provider	13-17
13.4.8	Adding a HTTP Outgoing Provider	13-18
13.4.9	Editing Provider Configuration	13-18
13.4.10	Deleting a Provider	13-19

14 Mapping URLs

14.1	WebUrlMapPlugin Component	14-1
14.2	Script Construction	14-1
14.3	Supported Variables for Referencing	14-2
14.4	Add/Edit URL Mapping Entries	14-3
14.5	Mapping Examples	14-3
14.5.1	Info Update Form	14-3
14.5.2	Dynamic Conversion	14-4
14.5.3	CGI parameters	14-4

Part V Administering Security

15 Understanding Security and User Access

15.1	Overview of Content Server Security	15-1
15.2	Security within Content Server	15-2
15.3	Additional Security Options	15-2
15.4	Advanced Security Options	15-3
15.4.1	Enabling Oracle Advanced Security Configurations Page	15-4
15.4.1.1	Specifying Advanced Security Options for Core QueryText	15-5
15.4.1.2	Specifying Advanced Security Options for FrameworkFolders QueryText	15-5

16 Configuring Fusion Middleware Security for Content Server

16.1	LDAP Authentication Providers	16-1
16.2	Configuring Oracle WebCenter Content to Use SSL	16-2
16.2.1	Configuring WebCenter Content for Two-Way SSL Communication	16-2
16.2.2	Invoking References in One-Way SSL Environments in Oracle JDeveloper	16-5
16.2.3	Configuring WebCenter Content, Oracle HTTP Server for SSL Communication	16-5
16.2.4	Switching from Non-SSL to SSL Configurations for WebCenter Content	16-6
16.2.5	Using a Custom Trust Store for One-Way SSL	16-6
16.2.6	Enabling an Asynchronous Process to Invoke an Asynchronous Process	16-7
16.2.7	Configuring RIDC SSL for Valid Certificate Path	16-7
16.3	Configuring WebCenter Content for Single Sign-On	16-9
16.3.1	Configuring Oracle Access Manager 14c with WebCenter Content	16-10
16.3.2	Configuring Oracle Access Manager 12c with WebCenter Content	16-12
16.3.3	Configuring Oracle Access Manager 11g with WebCenter Content	16-15
16.3.4	Configuring Oracle Access Manager 10g with WebCenter Content	16-17
16.3.5	Configuring Oracle Single Sign-On for WebCenter Content	16-20
16.3.6	Configuring the First Authentication Provider	16-23
16.3.7	Configuring the WebCenter Content URL for Single Sign-On	16-24
16.3.8	Configuring WebCenter Content and Single Sign-On for Windows Native Authentication	16-24
16.4	Configuring Oracle Infrastructure Web Services	16-27
16.5	Configuring WebCenter Content for Oracle Identity Cloud Service (IDCS)	16-27
16.5.1	Updating SSL.hostnameVerifier Property	16-27
16.5.2	Configuring IDCS Security Provider	16-28
16.5.2.1	Configuring Oracle Identity Cloud Integrator Provider	16-28
16.5.2.2	Setting Up Trust between IDCS and Weblogic	16-29
16.5.2.3	Creating Admin User in IDCS for WebCenter Content	16-29
16.5.2.4	Managing Group Memberships, Roles, and Accounts	16-30
16.5.3	Configuring WebCenter Content for User Logout	16-31
16.5.3.1	Configuring Logout for WebCenter Content and WebCenter Content: Imaging	16-31
16.5.3.2	Configuring Logout for Enterprise Capture	16-32

16.5.3.3	Configuring Logout for ADFUI	16-32
16.6	Configuring SAML-Based Single Sign-On	16-32
16.6.1	SAML Components	16-32
16.6.2	SAML Single Sign-On Prerequisites	16-33
16.6.2.1	Enabling SSL for Source Services	16-34
16.6.2.2	Enabling SSL for Destination Services	16-34
16.6.2.3	Creating and Exporting Certificates	16-35
16.6.2.4	Hiding Login Area for WebCenter Portal Landing Page	16-35
16.6.3	Configuring SAML 1.1 Source Services	16-36
16.6.3.1	Creating Credential Mapping Providers	16-36
16.6.3.2	Configuring Credential Mapping Providers	16-36
16.6.3.3	Creating Relying Parties	16-37
16.6.3.4	Configuring Relying Parties	16-37
16.6.3.5	Defining Federation Services for Source	16-38
16.6.4	Configuring SAML 1.1 Destination Services	16-39
16.6.4.1	Creating Identity Asserters	16-39
16.6.4.2	Adding Source Certificates	16-39
16.6.4.3	Creating Asserting Parties	16-40
16.6.4.4	Configuring Asserting Parties	16-40
16.6.4.5	Defining Federation Services for Destination	16-40
16.6.5	Configuring SAML 2.0 (IDCS) Single Sign-On	16-41
16.6.5.1	Configuring SAML 2.0 Asserter	16-42
16.6.5.2	Configuring Weblogic Managed Servers as SAML 2.0 SSO Service Providers	16-42
16.6.5.3	Completing SAML 2.0 Identity Asserter Configuration	16-44
16.6.5.4	Creating SAML Applications in IDCS	16-44
16.6.5.5	Assigning Groups to SAML Applications	16-45
16.6.5.6	Modifying Cookie Path	16-46
16.6.5.7	Configuring Oracle HTTP Server	16-47
16.6.5.8	Configuring Desktop Client	16-48

17 Managing User Types, Logins, and Aliases

17.1	Introduction to User Login Types	17-1
17.1.1	External Users	17-1
17.1.2	Local Users	17-3
17.2	Introduction to User Logins and Aliases	17-4
17.3	Managing Logins and Aliases	17-5
17.3.1	Adding a User Login	17-5
17.3.2	Editing a User Login	17-6
17.3.3	Deleting a User Login	17-6
17.3.4	Creating an Alias	17-7

17.3.5	Editing an Alias	17-7
17.3.6	Deleting an Alias	17-7
17.4	User Information Fields	17-8
17.4.1	Adding a New User Information Field	17-8
17.4.2	Editing an Option List	17-8
17.4.3	Editing a User Information Field	17-9

18 Managing Security Groups, Roles, and Permissions

18.1	Introduction to Content Server Security Groups	18-1
18.1.1	Best Practices for Working with Security Groups	18-1
18.1.2	Performance Considerations	18-2
18.1.2.1	Search Performance	18-3
18.1.2.2	User Admin Performance	18-3
18.2	Managing Content Server Groups	18-3
18.2.1	Adding a Security Group on Content Server	18-3
18.2.2	Deleting a Security Group on Content Server	18-4
18.3	Introduction to Content Server Roles and Permissions	18-4
18.3.1	Predefined Roles	18-6
18.3.2	About Permissions	18-6
18.3.3	Predefined Permissions	18-7
18.4	Managing Content Server Roles and Permissions	18-8
18.4.1	Creating a Role in Content Server	18-8
18.4.2	Deleting a Role in Content Server	18-9
18.4.3	Assigning Roles to a User with Oracle WebLogic Server	18-9
18.4.4	Assigning Roles for a Similar User with Oracle WebLogic Server	18-9
18.4.5	Adding and Editing Permissions in Content Server	18-9

19 Managing Accounts

19.1	Introduction to Content Server Accounts	19-1
19.1.1	Accounts and Security Groups	19-2
19.1.2	Hierarchical Accounts	19-3
19.1.3	Performance Considerations	19-4
19.1.4	External Directory Server Considerations	19-5
19.2	Managing Content Server Accounts	19-5
19.2.1	Enabling Accounts in Content Server	19-5
19.2.2	Creating Predefined Accounts in Content Server	19-6
19.2.3	Creating Accounts When Checking In Content in Content Server	19-6
19.2.4	Deleting Predefined Accounts in Content Server	19-6
19.2.5	Assigning Accounts to a User with Oracle WebLogic Server	19-7
19.3	A Content Server Accounts Case Study	19-7

19.3.1	Xalco Security	19-7
19.3.2	Xalco Accounts	19-8
19.3.3	Xalco Roles	19-8
19.3.4	Roles and Permissions Table	19-9
19.3.5	Roles and Users Table	19-9
19.3.6	Accounts and Users Table	19-10

20 Managing Access Control List Security

20.1	Introduction to Access Control List Security	20-1
20.2	Configuring Access Control List Security	20-2
20.3	Metadata Fields	20-3
20.3.1	xClbraUserList Metadata Field	20-3
20.3.2	xClbraAliasList Metadata Field	20-4
20.3.3	xClbraRoleList Metadata Field	20-4
20.4	Access Control List Permissions	20-4
20.4.1	Empty Access Control List Fields	20-5

21 Managing Additional Content Server Security Connections

21.1	Proxy Connections	21-1
21.2	Credential Mapping	21-2
21.2.1	About Credential Mapping	21-2
21.2.2	Credential Values	21-3
21.2.3	Matching Accounts and Roles	21-4
21.2.3.1	Reference Input Value	21-4
21.2.3.2	Privilege Levels	21-4
21.2.3.3	Substitution	21-5
21.2.3.4	Special Characters	21-5
21.2.4	Proxy Credentials Map	21-5
21.2.5	Creating a Credential Map	21-5
21.3	Secured Connections to Content Server	21-6
21.3.1	About Named Password Connections	21-6
21.3.2	Guidelines for Proxy Connections Data	21-7
21.3.3	Creating a Proxy Connection	21-7
21.4	Connections Using the HTTP Protocol	21-8
21.4.1	Using HTTP Protocol for Content Server Connection	21-8
21.4.2	Configuring the HTTP Provider	21-8

22 Customizing Content Server Communication

22.1	Login/Logout Customization	22-1
22.2	Browser URL Customization	22-1
22.2.1	About BrowserUrlPath Customization	22-1
22.2.2	Affected Idoc Script Variables and Functions	22-2
22.2.3	Determining the URL Path	22-3
22.2.4	Changing Absolute Full Path Computation	22-4
22.3	Extended User Attributes	22-4
22.3.1	ExtUserAttribInfo ResultSet	22-5
22.3.2	Configuration Variable for Extended User Attributes	22-6

Part VI Administering System Migration and Archiving

23 Understanding System Migration and Archiving

23.1	Introduction to Migration Tools and Components	23-1
23.2	Configuration Migration Utility	23-1
23.3	Archiver Application	23-2
23.4	Folder Archiving Application	23-4
23.5	ArchiveReplicationExceptions Application	23-4
23.6	Archive Tool Summary and Comparison	23-5

24 Migrating System Configurations

24.1	Understanding the Configuration Migration Utility	24-1
24.1.1	Migration Structure	24-1
24.1.2	About Migration Templates and Bundles	24-3
24.2	Managing Configuration Migration	24-3
24.2.1	Creating a Configuration Migration Template	24-4
24.2.2	Editing a Configuration Template	24-5
24.2.3	Importing a Template	24-6
24.2.4	Creating a One-Time Export	24-6
24.2.5	Exporting a Configuration	24-7
24.2.6	Uploading a Bundle	24-7
24.2.7	Importing a Bundle	24-8
24.2.8	Downloading a Bundle	24-9
24.2.9	Viewing Action Status	24-9
24.2.10	Viewing Action History	24-9
24.3	Migration Tips	24-9
24.3.1	Limitations	24-10

25 Managing Archives, Collections, and Batch Files

25.1	Understanding How the Archiver Works	25-1
25.1.1	Archive Structure	25-1
25.1.2	Collections	25-2
25.1.3	Batch Files	25-3
25.1.4	Archive Targets	25-4
25.1.5	Using Archive Logs	25-5
25.2	Managing Archives	25-6
25.2.1	Creating a New Archive	25-6
25.2.2	Copying an Existing Archive	25-7
25.2.3	Creating a New Archive by Copying	25-7
25.2.4	Deleting an Archive	25-8
25.2.5	Running Archiver as a Standalone Application	25-8
25.2.5.1	Running the Archiver in Windows	25-8
25.2.5.2	Running the Archiver in UNIX	25-8
25.3	Managing Collections	25-9
25.3.1	Opening a Collection	25-9
25.3.2	Creating a Collection	25-9
25.3.3	Removing a Collection	25-10
25.3.4	Moving the Default Archive Collection	25-11
25.4	Managing Batch Files	25-11
25.4.1	Removing Revisions from a Batch File	25-11
25.4.2	Deleting a Batch File	25-12

26 Exporting Data in Archives

26.1	Understanding Exporting Data	26-1
26.1.1	Export Uses	26-1
26.1.2	Export Methods	26-1
26.2	Managing Exports	26-2
26.2.1	Manually Exporting	26-2
26.2.2	Creating a Content Item Export Query	26-2
26.2.3	Exporting Configuration Information	26-4
26.2.4	Adding a Table to an Archive	26-5
26.2.5	Editing the Archive Properties of a Table	26-5
26.2.6	Creating a Table Export Query	26-5
26.2.7	Setting Export Options	26-7
26.2.8	Initiating the Export	26-7

27 Importing Data from Archives

27.1	Understanding Importing Files	27-1
27.1.1	Import Uses	27-2
27.1.2	Import Methods	27-2
27.2	About Import Rules	27-2
27.2.1	Update Import Rule	27-2
27.2.2	Insert Revision Import Rule	27-4
27.2.3	Insert Create Import Rule	27-4
27.2.4	Delete Revision Import Rule	27-5
27.2.5	Delete All Revisions Import Rule	27-6
27.3	Importing Data	27-7
27.3.1	Importing Archived Data Manually	27-7
27.3.2	Setting Field Maps	27-8
27.3.3	Setting Value Maps	27-9
27.3.4	Setting Import Options	27-10
27.3.5	Importing an Individual Revision	27-11
27.3.6	Initiating the Import	27-11

28 Transferring Files

28.1	Introduction to Transferring Files	28-1
28.1.1	Transfer Uses	28-1
28.1.2	Transfer Methods	28-2
28.1.3	Transfer Terms	28-2
28.2	Understanding Transfer Types	28-3
28.2.1	Local Transfer	28-3
28.2.2	Pull Transfer	28-3
28.2.3	Push Transfer	28-4
28.3	How Transferring Batch Files Works	28-5
28.3.1	Transfer Process Actions	28-5
28.3.2	Transfer Rules	28-6
28.4	Managing Transfers	28-7
28.4.1	Transferring Content	28-7
28.4.2	Making an Archive Targetable	28-7
28.4.3	Defining an Outgoing Transfer Provider	28-8
28.4.4	Setting a Transfer Destination (Target)	28-8
28.4.5	Initiating a Manual Transfer	28-9
28.4.6	Deleting a Transfer	28-9
28.4.6.1	Deleting a Transfer	28-9
28.4.6.2	Deleting an Automated Transfer	28-9

29 Replicating Files

29.1	Understanding Replication	29-1
29.1.1	Replication Uses	29-1
29.1.2	Replication Methods	29-2
29.1.3	Single Revision Replications	29-2
29.2	Managing Replication	29-3
29.2.1	Setting Up Automatic Export	29-3
29.2.2	Setting Up Automatic Import	29-3
29.2.3	Setting Up Automatic Transfer	29-4
29.2.4	Disabling Automatic Import	29-4
29.2.4.1	Unregistering an Importer from the Replication Tab	29-4
29.2.4.2	Disabling a Registered Importer from the Automation for Instance Page	29-5
29.2.5	Disabling Automatic Export	29-5
29.2.6	Disabling Automatic Transfer	29-5
29.2.7	Deleting a Registered Exporter	29-5
29.2.7.1	Deleting a Registered Exporter from the Replication Tab	29-5
29.2.7.2	Deleting a Registered Exporter from the Automation for Instance Window	29-6

30 Migrating the Folders Structure

30.1	About Migrating Folders Structure	30-1
30.2	Exporting Folders Structure Data	30-1
30.3	Importing Folders Structure Data	30-2

31 Archive and Migration Strategies

31.1	Export	31-1
31.2	Import	31-2
31.3	Self Export/Import	31-3
31.4	One-to-One Archiving	31-4
31.5	One-to-Many Archiving	31-6
31.6	Many-to-One Archiving	31-11
31.7	Archiver Examples	31-15
31.7.1	Copying a Content Server Instance to a Laptop	31-15
31.7.2	Transferring by Content Type and Author	31-15
31.7.2.1	Setting up an Automated Export	31-16
31.7.2.2	Setting up an Automated Import	31-16
31.7.2.3	Setting up an Automated Pull Transfer	31-16
31.7.3	Changing Metadata Fields	31-17
31.7.4	Adding Content ID Prefixes	31-17
31.7.5	Changing Release Dates	31-17

32 Using Archiver Replication Exceptions

32.1	Understanding Archiver Replication Exceptions	32-1
32.1.1	How Archiver Replication Exceptions Works	32-1
32.1.2	Scenario 1	32-1
32.1.3	Scenario 2	32-2
32.2	Administering and Using Archiver Replication Exceptions	32-2

Part VII Appendixes

A Managing Oracle Fusion Middleware BPEL Component for Content Server

A.1	Introduction	A-1
A.1.1	Hardware Requirements	A-1
A.1.2	Software Requirements	A-1
A.1.3	Software Distribution	A-1
A.2	Installation	A-2
A.2.1	Integration Instructions	A-2
A.2.1.1	Scenario One	A-2
A.2.1.2	Scenario Two	A-2
A.2.1.3	Final Steps	A-3
A.2.2	Enabling the Integration Component	A-3
A.3	Configuring the Integration Component	A-3
A.3.1	Architecture	A-4
A.3.1.1	Connection Configuration	A-4
A.3.2	Process Configurations	A-5
A.3.2.1	Process Properties	A-6
A.3.2.2	Payload Mappings	A-7
A.3.2.3	Preparing BPEL Composites for WebCenter Content Integration	A-9
A.3.3	Process Faults	A-9
A.4	Configuring a Workflow in Content Server	A-10
A.4.1	Configuring a Workflow	A-10
A.4.2	BPEL Process Information	A-15
A.4.3	Troubleshooting Workflows	A-16

B Managing the Need to Know Component

B.1	Introduction	B-1
B.1.1	Features	B-1

B.1.2	Applications	B-2
B.2	Installing the Need to Know Component	B-2
B.2.1	Installing the NTK Component with Component Wizard	B-3
B.2.2	Installing the NTK component with ComponentTool	B-3
B.3	Configuring the Need to Know Component	B-3
B.4	Using the Need to Know Component	B-5
B.4.1	Security Configuration Customization	B-5
B.4.1.1	Content Security	B-5
B.4.1.2	Search Results	B-7
B.4.1.3	Hit List Roles	B-7
B.4.1.4	WHERE Clause Calculation	B-8
B.4.1.5	Content Metadata Security	B-8
B.4.2	Disclosure Query Security Applet	B-8
B.4.3	Query Syntax	B-9
B.4.3.1	Like Operator	B-10
B.4.3.2	Boolean Operators	B-10
B.4.3.3	UserName Variable	B-10
B.4.3.4	stdSecurity Variable	B-11
B.4.3.5	User Attribute Fields	B-11
B.4.3.6	User Roles	B-11
B.4.4	Defining a Content-Level Query	B-11
B.5	Administration Interface	B-12
B.5.1	NTK Configuration Information Page	B-13
B.5.2	Content Security Configuration Information Page	B-15
B.5.3	Search Results Configuration Information Page	B-18
B.5.4	Hit List Roles Configuration Information Page	B-19
B.5.5	Test NTK Content Security Page	B-20
B.6	Security Customization Samples	B-21
B.6.1	Content Security Samples	B-22
B.6.1.1	Simple Idoc Script Function	B-22
B.6.1.2	Using stdSecurityCheck	B-22
B.6.1.3	Using isStrIntersect	B-22
B.6.1.4	Using allStrIntersect	B-23
B.6.1.5	Using includeNTKReadSecurityScript	B-23
B.6.2	Search Result Samples	B-23
B.6.2.1	Disabling Links	B-23
B.6.2.2	Changing Links	B-24
B.6.2.3	Changing Images	B-24
B.6.3	Hit List Roles Samples	B-24
B.6.3.1	Using the Query Hit List Role	B-24
B.6.3.2	Creating a Black Hole Check In	B-24

C Troubleshooting Oracle WebCenter Content

C.1	Introduction to Troubleshooting Oracle WebCenter Content	C-1
C.2	Getting Started with Troubleshooting Basics for Oracle WebCenter Content	C-2
C.2.1	Using Tracing	C-2
C.2.1.1	Server-Wide Tracing	C-2
C.2.1.2	Applet-Specific Tracing	C-5
C.2.2	Using Stack Traces	C-5
C.2.3	Using the Environment Packager	C-6
C.2.4	Using the Content Server Analyzer	C-6
C.2.4.1	Accessing the Content Server Analyzer	C-7
C.2.4.2	Specifying a Custom Analyzer Log Directory	C-7
C.2.4.3	Invoking the Analysis Process	C-7
C.2.4.4	Analyzing the Content Server Database	C-8
C.2.4.5	Analyzing the Content Server Search Index	C-9
C.2.4.6	Viewing the Analysis Progress and Results	C-9
C.2.4.7	Generating a Status Report	C-10
C.2.4.8	Canceling the Status Report	C-10
C.2.5	Using Debug Configuration Variables	C-10
C.2.6	Analyzing HDA Files	C-11
C.3	Troubleshooting Oracle WebCenter Content Archiving	C-11
C.3.1	Importing Issues	C-12
C.3.1.1	File Extension Errors on Import System	C-12
C.3.1.2	Selecting Specific Batch Files for Import	C-13
C.3.1.3	Import Maps Do Not Work After Archive Import	C-13
C.3.1.4	Identifying Imported Content Items From Archive	C-14
C.3.1.5	Duplicate Content Items in Content Server	C-14
C.3.1.6	Importing Archived Content to Proxied Server Fails	C-15
C.3.1.7	No Importing Errors But Documents Are Missing	C-15
C.3.1.8	Errors About Invalid Choice List Values	C-16
C.3.1.9	Import Fails Due to Missing Required Field	C-17
C.3.1.10	Changed Metadata Field Makes the Archiver Freeze During an Import	C-17
C.3.2	Exporting Issues	C-19
C.3.2.1	Total Export Possible with Blank Export Query	C-19
C.3.2.2	New Check-Ins and Batch File Transfers	C-19
C.3.2.3	Exporting User Attributes	C-20
C.3.2.4	Folder Archive Export Doesn't Work If Collections Table Has Many Records	C-20
C.3.3	Transfer Issues	C-21
C.3.3.1	Transfer Stopped When Target Locked Up	C-21
C.3.3.2	Aborting/Deleting a Running Transfer	C-22
C.3.3.3	Verifying the Integrity of Transferred Files	C-23

C.3.3.4	Transfer Process Is Not Working	C-23
C.3.4	Replication Issues	C-24
C.3.4.1	Stopping the Automatic Import Function	C-24
C.3.5	Oracle Database Issues	C-25
C.3.5.1	Allotted Tablespace Exceeded	C-25
C.3.5.2	Slow Oracle WebCenter Content Performance with Oracle Database	C-25
C.3.6	Miscellaneous Issues	C-26
C.3.6.1	Archiving Does Not Work With Shared File System	C-26
C.3.6.2	Archiving Does Not Work Over Outgoing Provider	C-26
C.4	Using My Oracle Support for Additional Troubleshooting Information	C-27

Preface

This guide describes how to administer Oracle WebCenter Content and Oracle WebCenter Content Server. It describes how to start and stop Content Server instances, how to access and use Content Server utilities, how to configure WebCenter Content components and security, and also how to archive, retrieve, and migrate WebCenter Content repository structure and content items.

Audience

This guide is intended for Oracle Fusion Middleware administrators responsible for WebCenter Content installations and Content Server deployments.

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

The complete Oracle WebCenter Content documentation set is available from the Oracle Help Center at the [Oracle WebCenter Content](#) page.

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 window, or text that you enter.

WebCenter Content Terminology

WebCenter Content documentation uses the following terms when referring to variables in the directories associated with the WebCenter Content and Content Server configuration:

- *IdcHomeDir*: This variable refers to the `ucm/idc` directory in the Oracle WebCenter Content home where the Oracle WebCenter Content server media is located. The server media can run Oracle WebCenter Content Server, Oracle WebCenter Content: Inbound Refinery, or Oracle WebCenter Content: Records software. This is essentially a read-only directory. The default location is `WCC_ORACLE_HOME/ucm/idc`. The variable portion of the default location can be changed, but the path cannot be changed from `ucm/idc`.
- *DomainHome*: This variable refers to the user-specified directory where an Oracle WebCenter Content application is deployed to run on an Oracle WebLogic Server application server. The `DomainHome/ucm/short-product-id/bin` directory contains the `intradoc.cfg` file and executables. The default location for *DomainHome* is `MW_HOME/user_projects/domains/base_domain`, but you can change the path and domain name (*base_domain*) during the deployment of an Oracle WebCenter Content application to an application server.
- *short-product-id*: This variable refers to the type of Oracle WebCenter Content server deployed to an application server. This name is used as the context root (default `HttpRelativeWebRoot` configuration value). Possible values include:
 - `cs` (Oracle WebCenter Content Server)
 - `ibr` (Oracle WebCenter Content: Inbound Refinery)
- *IntradocDir*: This variable refers to the root directory for configuration and data files specific to an Oracle WebCenter Content instance that is part of an Oracle WebCenter Content application deployed to an application server. This `Idoc Script` variable is configured for one type of Oracle WebCenter Content instance: Content Server (`cs`) or Inbound Refinery (`ibr`). This directory can be located elsewhere, but the default location is `DomainHome/ucm/short-product-id`. The specified directory must be an absolute path to the instance directory and must be unique to a particular server or node. The directory includes a `bin/` directory, which contains the startup files (`intradoc.cfg` and executables).

With the introduction and enablement of vertical cluster and scale-up support by default beginning from 12c (12.2.1.1.0) release, a server specific `intradoc.cfg` will be created along with the original `intradoc` file and named as:

```
<server-name>_intradoc.cfg
```

This server specific `intradoc.cfg` file needs to be updated for any configuration changes to take effect.

If the existing instance is scaled-up by adding more scale-up instances, then each scaled-up instance will have its own `intradoc` file, for example:

UCM_server1HA_intradoc.cfg

Part I

Introduction to Oracle WebCenter Content

This part provides an introduction to Oracle WebCenter Content and summarizes the primary tasks for administering the system.

This part contains the following chapters:

- [Introduction to Administering Oracle WebCenter Content](#)

1

Introduction to Administering Oracle WebCenter Content

This chapter provides an introduction to the Oracle WebCenter Content system and to basic system administration tasks.

This chapter covers the following topics:

- [Introduction to Oracle WebCenter Content](#)
- [Basic Tasks for Administering Oracle WebCenter Content](#)

1.1 Introduction to Oracle WebCenter Content

Oracle WebCenter Content enables users to manage documents, images, records, and rich media files with end-to-end content life cycle management from creation to archiving.

The WebCenter Content system by default includes the Oracle WebCenter Content Server, which provides core content management functions and features supporting a wide variety of functionality for managing content, images, digital assets, records, content conversion, and the desktop experience.

For more information about WebCenter Content concepts and applications, see *Overview of Oracle WebCenter Content* in *Understanding Oracle WebCenter Content Concepts*.

1.1.1 Content Server

The Content Server is the foundation for a variety of WebCenter Content management features. It provides a flexible, secure, centralized, web-based repository that manages all phases of the content life cycle from creation and approval to publishing, searching, expiration, and archiving or disposition.

WebCenter Content administration involves configuring and managing the Content Server, including the system database, and other software such as Oracle software for user authentication and authorization, Oracle Fusion Middleware for domain-level system control and monitoring, and other software as needed to maintain optimal system performance.

WebCenter Content administration includes using Content Server components which provide advanced functionality for managing system features. Some components are automatically enabled in the WebCenter Content system and some are available to be enabled after system installation. Content Server also provides software that can be used to create customized components. For details on customizing components, see *Getting Started with Content Server Components* in *Developing with Oracle WebCenter Content*.

1.1.2 Content Management

The content repository is the heart of the WebCenter Content system. Content can take many forms such as documents, records, images, and audio files. All content checked in to the system is stored in the repository, and from there it can be managed by users with the appropriate permissions to that content.

Every contributor throughout an organization can easily contribute content from native desktop applications, efficiently manage business content through use of rich library services, and securely access that content anywhere using a web browser.

All content, regardless of content type, is stored in the web repository or database for management, reuse and access. While stored in the repository, all types of content ranging from email, discussions, documents, reports, spreadsheets, and records to images, multimedia or other digital formats receive the same set of fundamental core services.

WebCenter Content administration involves managing internal features and applications to support content conversion, workflow, metadata, records management, and so forth. See Introduction to Oracle WebCenter Content Features in *Managing Oracle WebCenter Content*.

1.2 Basic Tasks for Administering Oracle WebCenter Content

The roadmap in [Table 1-1](#) outlines typical tasks that a system administrator might perform to manage WebCenter Content after the application has been installed and the initial configuration completed.

For details about installing WebCenter Content, see Installing the Oracle WebCenter Content Software in *Installing and Configuring Oracle WebCenter Content*.

Table 1-1 Roadmap - Administering Oracle WebCenter Content

Task	Documentation
Stop and start the managed server	Restart the Oracle WebLogic Server managed server on which the Oracle WebCenter Content application is deployed to effect configuration changes or for routine maintenance: <ul style="list-style-type: none"> • Starting and Stopping Content Server and Inbound Refinery
Monitor performance	Analyze the performance of the WebCenter Content application and monitor its current status: <ul style="list-style-type: none"> • Monitoring Content Server and Inbound Refinery Using Fusion Middleware Control • Monitoring Content Server Status
View and manage log files	Identify and diagnose problems through log files. WebCenter Content logs record many types of events, including startup and shutdown information, errors, warnings, and other information: <ul style="list-style-type: none"> • Monitoring Content Server Log Files • Troubleshooting Oracle WebCenter Content
Load content into the repository	Load a quantity of content into the Content Server repository using a Content Server application: <ul style="list-style-type: none"> • Batch Loading Content
Backup and migrate data	Archive, restore, and migrate Content Server metadata and content: <ul style="list-style-type: none"> • Migrating System Configurations • Managing Archives, Collections, and Batch Files • Exporting Data in Archives • Importing Data from Archives • Transferring Files • Replicating Files • Migrating the Folders Structure

Table 1-1 (Cont.) Roadmap - Administering Oracle WebCenter Content

Task	Documentation
Tune application properties	Configure or reconfigure performance related settings for the WebCenter Content environment and Content Server: <ul style="list-style-type: none"> • Configuring System Properties • Configuring Providers • Managing Components • Managing Search Features • Configuring the Search Index • Managing a File Store System
Tune security properties	Configure or reconfigure security related settings for the WebCenter Content environment and Content Server: <ul style="list-style-type: none"> • Configuring Fusion Middleware Security for Content Server • Managing User Types, Logins, and Aliases • Managing Security Groups, Roles, and Permissions • Managing Accounts • Managing Access Control List Security • Managing Additional Content Server Security Connections • Customizing Content Server Communication Note that by default users, groups, and accounts are managed through a selected LDAP provider, Oracle WebLogic Server, and other Oracle security software. Some configuration may be performed with Content Server security settings.
Configure related applications	Configure or reconfigure related applications: <ul style="list-style-type: none"> • Managing the Need to Know Component • Managing Oracle Fusion Middleware BPEL Component for Content Server

Part II

Getting Started

This part provides information about using Oracle WebCenter Content administration interfaces and tools, and how to access and control a Content Server instance.

This part contains the following chapters:

- [Getting Started Administering Oracle WebCenter Content](#)
- [Managing System Processes](#)
- [Batch Loading Content](#)

2

Getting Started Administering Oracle WebCenter Content

This chapter provides information on Oracle WebCenter Content system administration responsibilities, interfaces, apps, utilities, and other tools.

This document is written with the assumption that WebCenter Content software is already installed and ready for use. For information on installing WebCenter Content software with a Content Server instance and setting initial installation configuration options, see Preparing to Install and Configure Oracle WebCenter Content in *Installing and Configuring Oracle WebCenter Content*.

This chapter includes the following topics:

- [Understanding System Administrator Roles and Responsibilities](#)
- [Understanding System Administrator Interfaces](#)
- [Understanding WebCenter Content System Administration Tools](#)
- [Accessing Oracle WebCenter Content](#)
- [Configuring WebCenter Content User Interface](#)
- [Associating the WebCenter Content User Interface with Content Server](#)

2.1 Understanding System Administrator Roles and Responsibilities

The Oracle WebCenter Content system administrator must be assigned two administrator roles to be able to perform administrative tasks: the first role in the Oracle WebLogic Server domain through whatever authentication/authorization software is used for a site, and the second role in Oracle WebCenter Content through the Oracle WebLogic Server. Both roles are required for a user to have full administrative privileges for Enterprise Management Fusion Middleware Control, the Oracle WebLogic Server domain where WebCenter Content is deployed, and the WebCenter Content system and Content Server instance.

An administrator is typically specified during WebCenter Content software installation. More than one system administrator can be assigned for WebCenter Content, such as an administrator with limited permissions to manage certain applications, or an administrator for each WebCenter Content instance. See *Configuring the Administrator Account* in *Installing and Configuring Oracle WebCenter Content*.

WebCenter Content administrators can use the Oracle Enterprise Manager Fusion Middleware Control interface, the Oracle WebLogic Server Administration Console, and Content Server applications and utilities to perform administrative tasks including:

- Starting and stopping Content Server instances
- Configuring WebCenter Content system settings
- Configuring WebCenter Content security configuration, both internal and integrated with Fusion Middleware components

- Creating and assigning WebCenter Content user accounts, roles, permissions, user groups, and group accounts (this may be shared with the administrator of whichever authentication/authorization and database software is used for a site)
- Configuring and implementing WebCenter Content search tools
- Managing WebCenter Content system and custom components
- Managing WebCenter Content system migration and archiving
- Monitoring and troubleshooting WebCenter Content instances

Additional administration tasks include configuring and managing Content Server features such as the repository, workflow, content conversion, imaging, and records. See Introduction to Oracle WebCenter Content Features in *Managing Oracle WebCenter Content*.

2.2 Understanding System Administrator Interfaces

Oracle WebCenter Content system administrators have several browser interfaces in which to perform certain tasks.

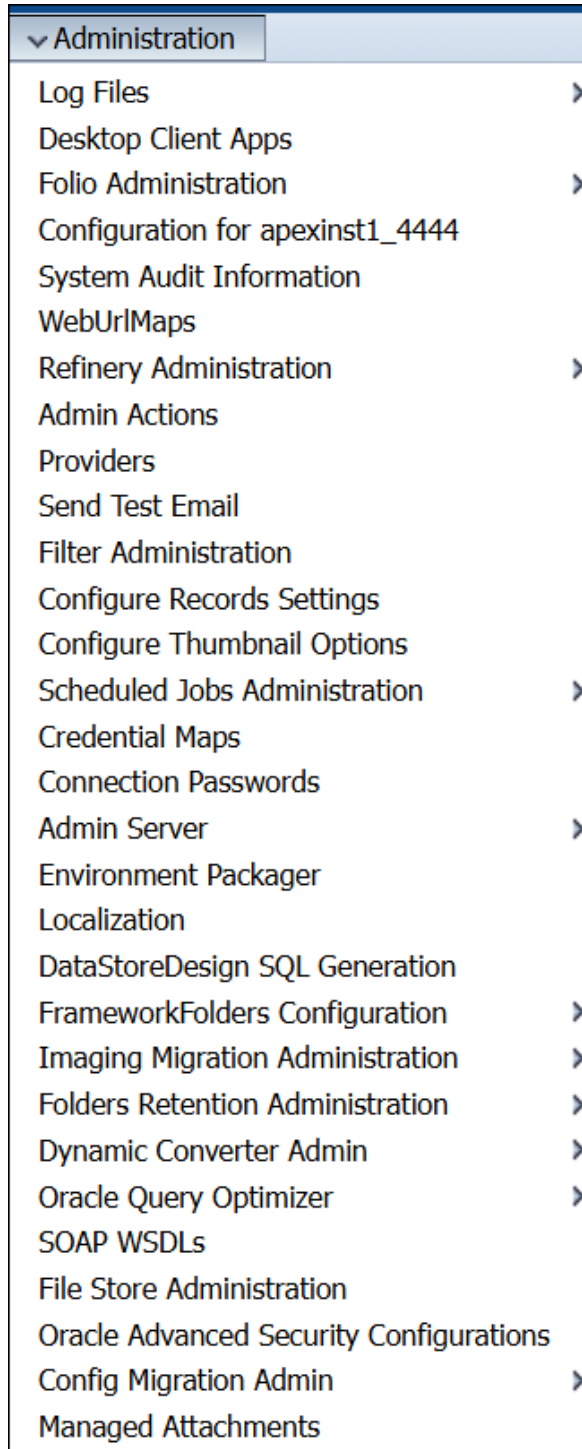
- [About the WebCenter Content Server Administration Interface](#)
- [About Oracle Enterprise Manager Fusion Middleware Control](#)
- [About the Oracle WebLogic Server Administration Console](#)

2.2.1 About the WebCenter Content Server Administration Interface

The Administration tray is the default layout for the WebCenter Content Server browser interface to provide access to Content Server administration log files and to pages for configuring and managing Content Server applications and tools.

To access the Administration tray, log in as a Content Server administrator, then choose **Administration** to view available administration options. If your Content Server instance is configured to use Menus, choose **Administration** to view the same options in a menu layout. [Figure 2-1](#) shows a sample Oracle WebCenter Content tray layout with the Administration selection expanded to show options.

Figure 2-1 Sample Oracle WebCenter Content Administration Tray



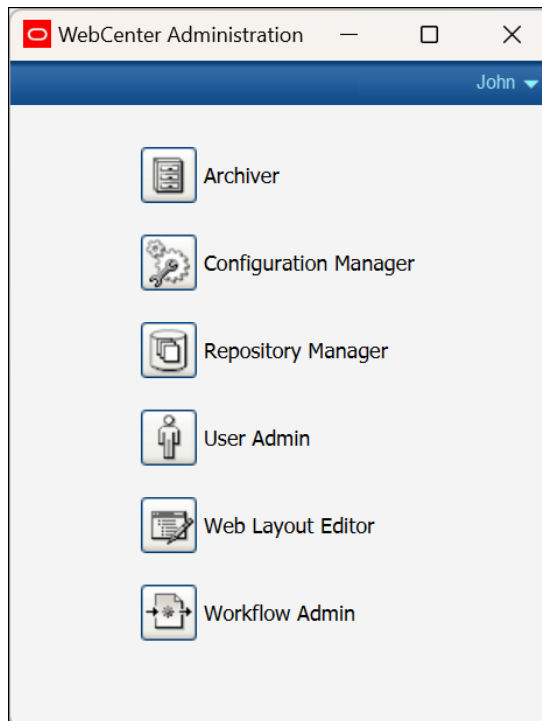
 **Note:**

WebCenter Content administrators use the *native interface* to perform administrative tasks using management pages and applications. The Oracle WebCenter Content application is configured by default to use the native interface for both administrators and users. If WebCenter Content is configured to use the *WebCenter Content user interface* (new as of 11.1.1.8), administrators must still use the native interface. For more information, see *Installing and Configuring Oracle WebCenter Content*, and *Getting Started with the WebCenter Content User Interface in Using Oracle WebCenter Content*.

The Administration Apps page provides access to Content Server administration apps and configuration tools. To access this page, log in as a WebCenter Content administrator and choose **Administration**, then **Desktop Client Apps**.

Administration apps accessed using a web browser are displayed and can be used only in the native interface.

Figure 2-2 Administration Apps page



 **Note:**

The Apple Safari browser is incompatible with Content Server administration apps and tools accessed using the Administration Apps page.

 **Note:**

You may experience problems if you start any Java applets (such as a Content Server administration applet or the multiple-file upload applet) from a browser that is using the Sun JDK 1.3/1.4 Java plug-in. These issues are related to authentication when launching an applet for the first time and applets closing when the parent window is changed.

2.2.2 About Oracle Enterprise Manager Fusion Middleware Control

Fusion Middleware Control is a Web-based interface that you use to monitor and administer a farm, domains, and WebCenter Content instances.

A **farm** is a collection of components managed by Fusion Middleware Control. It can contain an Oracle WebLogic Server domain, one Administration Server, one or more Managed Servers, clusters, one or more Oracle instances, and the Oracle Fusion Middleware components that are installed, configured, and running in the domain or Oracle instances, including Oracle WebCenter Content.

Fusion Middleware Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for the farm, domain, servers, components, and applications. These home pages make it easy to locate the most important monitoring data and the most commonly used administrative functions for a component from your web browser.

Fusion Middleware Control can be used to:

- Start and stop Oracle WebLogic Server
- Start and stop components
- Start and stop applications
- Access log files and manage log configuration
- Modify Oracle BPEL Process Manager MBean properties
- Debug applications such as Oracle BPEL Process Manager applications
- Deploy ADF applications
- Deploy Java EE applications
- Configure and manage auditing
- Configure SSL
- Manage Oracle HTTP Server
- Manage Oracle Web Cache

For more information about accessing Fusion Middleware Control to administer WebCenter Content, see [Accessing WebCenter Content Using Fusion Middleware Control](#). For more information about accessing and using Fusion Middleware Control, see Getting Started with Oracle Enterprise Manager Fusion Middleware Control in *Administering Oracle Fusion Middleware*.

For detailed information while using the Fusion Middleware Control Console, you can click **Help** at the top of the page. In most cases, the Help window displays a help topic about the current page. Click **Contents** in the Help window to browse the list of help topics, or click **Search** to search for a particular word or phrase.

2.2.3 About the Oracle WebLogic Server Administration Console

Oracle WebLogic Server Administration Console is a Web-based interface that you use to manage a WebLogic Server domain. It is accessible from any supported Web browser with network access to the Administration Server. A WebLogic Server domain includes one or more WebLogic Servers. You manage your applications as part of a domain.

One instance of WebLogic Server in each domain is configured as an Administration Server. The Administration Server provides a central point for managing a WebLogic Server domain. All other WebLogic Server instances in a domain are called Managed Servers. In a domain with only a single WebLogic Server instance, that server functions both as Administration Server and Managed Server. The Administration Server hosts the Administration Console, which is a Web application accessible from any supported Web browser with network access to the Administration Server. Managed Servers host applications.

The Administration Console can be used to:

- Configure, start, and stop WebLogic Server domains
- Configure WebLogic Server clusters
- Configure WebLogic Server services, such as database connectivity (JDBC) and messaging (JMS)
- Configure security parameters, including creating and managing users, groups, and roles
- Configure and deploy applications
- Monitor server and application performance
- View server and domain log files
- View application deployment descriptors

For detailed information on using the Oracle WebLogic Server Administration Console, click **Help** from any Administration Console page, or see *Getting Started Using Oracle WebLogic Server Administration Console* in *Administering Oracle Fusion Middleware*.

2.3 Understanding WebCenter Content System Administration Tools

Oracle provides software tools for managing a WebCenter Content system with a Content Server instance. The WebCenter Content administrator should use these tools instead of directly editing configuration files to perform Content Server administrative tasks unless a specific procedure requires that a file be edited. Editing a file may cause the settings to be inconsistent and generate problems.

The WebCenter Content system includes specific administration utilities and applications for managing processes, providers, archives, user, and so forth.

- [About Content Server Tools](#)
- [About Oracle WebLogic Scripting Tool \(WLST\)](#)

See the browser considerations section in your installation and deployment guide for information about Java browser plug-ins and applet display issues.

2.3.1 About Content Server Tools

Content Server provides the following administration software tools to configure and maintain system operation:

- [Management Pages](#)
- [Applications](#)
- [Utilities](#)
- [IdcShell Command-Line Tool](#)

2.3.1.1 Management Pages

Management pages can be accessed by using a web browser and choosing **Administration**, then choosing the management option in the Content Server interface. Some of the typical management pages are listed here.

 **Note:**

WebCenter Content administrators use the *native interface* to perform administrative tasks using management pages and applications. The Oracle WebCenter Content application is configured by default to use the native interface for both administrators and users. If WebCenter Content is configured to use the *WebCenter Content user interface* (new as of 11.1.1.8), administrators must still use the native interface. For more information on the WebCenter Content user interface, see *Installing and Configuring Oracle WebCenter Content*, and Getting Started with the WebCenter Content User Interface in *Using Oracle WebCenter Content*.

- **Admin Server:** Configure certain Content Server settings. A Content Server instance has its own Admin Server instance, which manages the Content Server instance on the WebCenter Content domain. Functions provided by the Admin Server for a Content Server instance also can be performed using Fusion Middleware Control.
 - **Component Manager:** View, enable or disable, install or uninstall, and download components which provide additional functionality to Content Server.
 - **General Configuration:** Specify a variety of settings used to configure WebCenter Content Server, including enabling accounts and adding configuration variables specific to your unique Content Server deployment.
 - **Content Security:** Set or modify select Content Server content security options.
 - **Internet Configuration:** View or modify Content Server Internet options.
- **Localization:** View and modify enabled and disabled locales for your Content Server instance.
- **Providers:** Add providers, configure provider information, and test providers.

2.3.1.2 Applications

The following Content Server applications can be started as standalone applications from the Administration Apps page through a web browser or by choosing the **Apps** menu in each of the tool interfaces.

 **Note:**

A WebCenter Content administrators use the *native interface* to perform administrative tasks using management pages and applications. The Oracle WebCenter Content application is configured by default to use the native interface for both administrators and users. If WebCenter Content is configured to use the *WebCenter Content user interface* (new as of 11.1.1.8), administrators must still use the native interface. For more information on the WebCenter Content user interface, see Getting Started with the WebCenter Content User Interface in *Using Oracle WebCenter Content*.

For more information on Configuration Manager, Repository Manager, Weblayout Editor, and Workflow Admin applications, see Understanding Management Tools in *Managing Oracle WebCenter Content*.

- **Archiver:** Export, import, transfer, and replicate content server files and information. For details, see the chapter on managing system archiving and migration.
- **Configuration Manager:** Manage content types, file formats, and custom metadata fields.
- **Repository Manager:** Perform file diagnostics, file management functions, search data re-indexing, and subscription management functions.
- **User Admin:** Manage the local user base, set up security (by assigning roles and permissions to users), define aliases, and manage security groups.
- **Weblayout Editor:** Build a website, work with reports, write queries.
- **Workflow Admin:** Set up workflows to route content to specific people for action.

2.3.1.3 Utilities

The following utilities can be started only as standalone applications from the computer where the Content Server instance is installed. For instructions on how to run standalone applications, see [Running Administration Applications in Standalone Mode](#).

- **Batch Loader:** Update or check in a large number of content items simultaneously.
- **Component Tool:** Install and enable or disable Content Server components using the command line.
- **Component Wizard:** Create and install custom components to modify Content Server behavior.
- **Content Analyzer:** Confirm the integrity of Content Server repository components, including the file system, database, and search index.
- **System Properties:** Configure the system options and functionality of a Content Server instance.

2.3.1.4 IdcShell Command-Line Tool

The IdcShell tool enables administrators to run Idoc Script from a command line. Idoc Script is a proprietary server-side scripting language for WebCenter Content. For more information, see [Using the IdcShell Command-Line Tool to Run Idoc Script](#) and Introduction to the Idoc Script Custom Scripting Language in *Developing with Oracle WebCenter Content*.

2.3.2 About Oracle WebLogic Scripting Tool (WLST)

The Oracle WebLogic Scripting Tool (WLST) can be used to manage Fusion Middleware components, such as Oracle WebCenter Content with a Content Server instance, from the command line.

The WebLogic Scripting Tool is a command-line scripting environment for creating, managing, and monitoring Oracle WebLogic Server domains. It is based on the Java scripting interpreter, Jython. In addition to supporting standard Jython features such as local variables, conditional variables, and flow control statements, the WebLogic Scripting Tool provides a set of scripting functions (commands) that are specific to Oracle WebLogic Server instances. Administrators can extend the WebLogic scripting language to suit site-specific needs by following the Jython language syntax.

Oracle WebCenter Content is supported by custom WLST commands for managing Content Server application connections (to the repository, portlet producers, external applications, and other back-end services) and for configuring the WebCenter Content user interface (based on the Oracle Development Application Framework). All the WLST commands specific to Oracle WebCenter Content Server are described in Oracle WebCenter Content Custom WLST Commands in *WebCenter WLST Command Reference*.

2.4 Accessing Oracle WebCenter Content

Oracle WebCenter Content administrators can use several interfaces for managing WebCenter Content instances and related software for databases and security. The two primary interfaces for administering day-to-day tasks for WebCenter Content instances are Fusion Middleware Control and the Oracle WebCenter Content user interface with administration functionality. These interfaces are described with instructions how to use them in:

- [Accessing WebCenter Content Using Fusion Middleware Control](#)
- [Accessing WebCenter Content Instances Using a Web Browser](#)

2.4.1 Accessing WebCenter Content Using Fusion Middleware Control

The Oracle Enterprise Manager Fusion Middleware Control interface can be used to access WebCenter Content and Content Server related screens for performing basic administration tasks. This section explains the following tasks.

- [Logging In to Fusion Middleware Control](#)
- [Navigating to the Content Server Home Page](#)

2.4.1.1 Logging In to Fusion Middleware Control

Oracle Fusion Middleware administrators can use Fusion Middleware Control to access and manage a Content Server instance. Fusion Middleware Control is configured for a domain and it is automatically started when you start the Oracle WebLogic Server Administration Server.

1. Enter the Fusion Middleware Control URL in your web browser. The URL must include the name of the host and the port number assigned during the installation.

```
http://adminServerHost:adminServerPort/em
```

For *adminServerHost*, specify the name of the computer that hosts the WebLogic Server Administration Server for your domain. For *adminServerPort*, specify the listen port number for the Administration Server. The default number is 7001. For example:

```
http://myHost.example.com:7001/em
```

You can find the exact URL, including the administration port number, in the `config.xml` file:

- Windows: `DOMAIN_HOME\config\config.xml`
- UNIX: `ORACLE_INSTANCE/config/config.xml`

2. Enter a valid Fusion Middleware administrator user name and password, and click **Login**.

A default user name for the administrator user is provided with the software. This is the account you can use to log in to Fusion Middleware Control for the first time. The password is the one supplied during the installation of Fusion Middleware.

The first page Fusion Middleware Control displays is the Farm domain home page. You can also view this page at any time by selecting the name of the farm in the navigation pane.

From the navigation pane, you can expand the tree and select a target to view and manage components in your farm.

2.4.1.2 Navigating to the Content Server Home Page

The Content Server home page in the Fusion Middleware Control interface is your starting place for managing a Content Server instance.

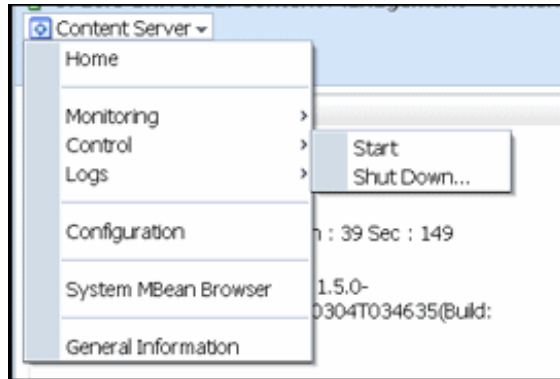
From the Content Server home page you can:

- Check the current status of an instance
- View overall response time for services
- View resource information on concepts and tasks

The Content Server home page displays the **Content Server** menu. From the **Content Server** menu you can:

- Start and shut down an instance
- Configure instance parameters and email settings
- Monitor instance performance metrics
- Analyze diagnostic information and log files
- Modify attributes using the system MBean browser
- View general information about the system configuration

Figure 2-3 Content Server Menu in Fusion Middleware Control



To navigate to the Content Server home page:

1. Log in to Fusion Middleware Control. See [Logging In to Fusion Middleware Control](#).
2. In the navigation pane, expand the tree to select the appropriate target domain name (for example, `Farm_base_domain`).
3. Expand **WebCenter**, then **Content**, then **Content Server**.
4. Select the Content Server instance to navigate to the home page.

Figure 2-4 shows an example of navigation on a WebLogic Server to the instance: Oracle WebCenter Content - Content Server (UCM_server1).

Figure 2-4 Navigation on WebLogic Server to Content Server



2.4.2 Accessing WebCenter Content Instances Using a Web Browser

To access a running WebCenter Content instance as an administrator, start a web browser and enter the URL for the specific WebCenter Content configuration.

- [Accessing a Content Server Instance](#)
- [Accessing a WebCenter Content: Inbound Refinery Instance](#)
- [Accessing a WebCenter: Records Instance](#)

2.4.2.1 Accessing a Content Server Instance

To access a Content Server instance:

1. Enter the URL:

```
http://managedServerHost:managedServerPort/cs
```

2. Log in with the administrator user name and password for the WebLogic Server.
 - For *managedServerHost*, specify the name of the computer that hosts the WebLogic Server Managed Server for the WebCenter Content domain where the Content Server instance is installed.
 - For *managedServerPort*, specify the listen port number for the WebLogic Server Managed Server for the WebCenter Content domain where the Content Server instance is installed.

The default port number for a Content Server instance is 16200. For example:

```
http://myHost.example.com:16200/cs
```

Note:

As a non-administrator user, if you access a Content Server instance, which is configured to use the WebCenter Content user interface instead of the native interface, be aware that the WebCenter Content user interface resides in a separate domain from Content Server and runs on a different port, 16225 by default.

2.4.2.2 Accessing a WebCenter Content: Inbound Refinery Instance

To access a WebCenter Content: Inbound Refinery instance:

1. Enter the URL:

```
http://managedServerHost:managedServerPort/ibr
```

2. Log in with the administrator user name and password for WebLogic Server.
 - For *managedServerHost*, specify the name of the computer that hosts the WebLogic Server Managed Server for the WebCenter Content domain where the Inbound Refinery instance is installed.
 - For *managedServerPort*, specify the listen port number for the WebLogic Server Managed Server for the WebCenter Content domain where the Inbound Refinery instance is installed.

The default port number for Inbound Refinery is 16250. For example:

```
http://myHost.example.com:16250/ibr
```

2.4.2.3 Accessing a WebCenter Content: Imaging Instance

To access a WebCenter Content: Imaging instance:

1. Enter the URL:

```
http://managedServerHost:managedServerPort/imaging
```

2. Log in with the administrator user name and password for WebLogic Server.
 - For *managedServerHost*, specify the name of the computer that hosts the WebLogic Server Managed Server for the WebCenter Content domain where the Imaging instance is installed.
 - For *managedServerPort*, specify the listen port number for the WebLogic Server Managed Server for the WebCenter Content domain where the Imaging instance is installed.

The default port number for Imaging is 16000. For example:

```
http://myHost.example.com:16000/imaging
```

2.4.2.4 Accessing a WebCenter: Records Instance

To access a WebCenter Content: Records instance:

1. Enter the URL:

```
http://managedServerHost:managedServerPort/cs
```

2. Log in with the administrator user name and password for WebLogic Server.
 - For *managedServerHost*, specify the name of the computer that hosts the WebLogic Server Managed Server for the WebCenter Content domain where the Records instance is installed.
 - For *managedServerPort*, specify the listen port number for the WebLogic Server Managed Server for the WebCenter Content domain where the Records instance is installed.

The default port number for Records is 16300.

```
http://myHost.example.com:16300/cs
```

2.5 Configuring WebCenter Content User Interface

You can configure Content Server with the WebCenter Content user interface in addition to the native user interface, which Content Server uses by default.

Before you start using the WebCenter Content user interface, set up the Remote Intradoc Client (RIDC), optionally set up additional configuration variables and the search engine for Content Server, set up full-text search, set up document conversions through Digital Asset Management (DAM) and Inbound Refinery, and also enable additional features to enhance the WebCenter Content user interface experience.

This section contains the following topics:

- [Setting up the Remote Intradoc Client \(RIDC\)](#)
- [Setting Additional Content Server Parameters](#)
- [Configuring Application Parameters](#)
- [Enabling Full-Text Searching](#)
- [Generating Thumbnails and Web-Viewable Renditions](#)
- [Configuring Digital Asset Management in Content Server](#)
- [Configuring Extended Features in Content Server](#)
- [Completing the Workflow Configuration](#)

2.5.1 Setting up the Remote Intradoc Client (RIDC)

The WebCenter Content user interface uses the IDC socket protocol to communicate with Content Server. To enable this communication, you must set the `IntradocServerPort` and `SocketHostAddressSecurityFilter` values in the `WCC_domain/ucm/cs/config/config.cfg` configuration file for Content Server, in the Oracle WebCenter Content domain. Server-specific `IntradocServerPort` (TCP listen port for `SystemServerSocket`) can now also be set through both Java system property and `config.cfg` parameter, enabling multiple Content servers to run `SystemServerSocket` providers on the same machine and avoid port conflict.

The following syntax shows how to set these values:

Example 1:

```
IntradocServerPort=port_number
SocketHostAddressSecurityFilter=IP addresses of permitted UI hosts separated
by a bar symbol (|)
```

For example:

```
IntradocServerPort=4444
SocketHostAddressSecurityFilter=123.456.789.0
```

If you want to open this up to all hosts in the network, use this setting:
`SocketHostAddressSecurityFilter=*. *.*.*`

Example 2:

In this example, the `config.cfg` values show that the server with `IDC_Id` value of `UCM_serverHA` has explicitly set a listen port number of 7036, rather than using the default listen port number:

```
IntradocServerPort=7034
IntradocServerPort.UCM_serverHA=7036
```

For more information about the `config.cfg` file, see *The config Directory* in *Developing with Oracle WebCenter Content*.

2.5.2 Setting Additional Content Server Parameters

For the WebCenter Content user interface, you can also set Content Server parameters for folders and searching.

To set additional Content Server parameters:

1. From the Content Server **Administration** menu or tray, choose **Admin Server** and then **General Configuration**.
2. Select the **Enable Accounts** checkbox.
3. In the Additional Configuration Variables area, add the following parameters, if not set already, to go in the `config.cfg` file:
 - `FoldersIndexParentFolderValues=true`
This parameter enables you to search for content within folders, including subfolders.
 - `FldEnforceFolderFileNameUniqueness=true`

This parameter prevents folders from having a child folder with the same name as a child document.

- `FldEnforceCaseInsensitiveNameUniqueness=true`

This parameter makes name-uniqueness checks for folder and file names case-insensitive. It also makes path resolution case-insensitive.

- `SearchIndexerEngineName=OracleTextSearch` or
`SearchIndexerEngineName=DATABASE.METADATA`

This parameter enables OracleTextSearch full-text searching or database metadata searching, instead of the default database full-text searching.

4. Restart the WebCenter Content Managed Server.

2.5.3 Configuring Application Parameters

When using the WebCenter Content user interface instead of the native interface, set the following properties using either MBean or WebLogic Scripting Tool.

- `temporaryDirectory`

Set this application configuration property to a safe location that does not automatically get cleaned up by the operating system or other scheduled jobs.

For example, on the Linux operating system, the default `temporaryDirectory` is `/tmp`. Many Linux distributions include cron jobs that automatically clean up the `/tmp` directory. If this happens, the application cannot recover from this unexpected error and it needs to be restarted.

- `maximumWindowsPerSession`

This configuration parameter limits the number of active Doc Properties windows. The default is 7.

If the WebCenter Content instance has a higher than desired memory consumption, set the parameter to 4 to reduce the required heap size.

For more information, see `updateWccAdfConfig` in *WebCenter Content Command Reference*.

2.5.4 Enabling Full-Text Searching

For full-text searching, you need to rebuild the Content Server index using OracleTextSearch (`SearchIndexerEngineName=ORACLETEXTSEARCH` parameter).

To enable full-text searching in the WebCenter Content user interface:

1. Access Content Server with the native user interface:

```
http://WCCHOST1:16200/cs
```

2. From the **Administration** menu or tray, choose **Desktop Client Apps** and then **Repository Manager**.
3. Click the **Indexer** tab.
4. Under **Collection Rebuild Cycle**, click the **Start** button.
5. Deselect **Use Fast Rebuild**.
6. Click the **OK** button.

2.5.5 Generating Thumbnails and Web-Viewable Renditions

If you want to obtain thumbnail images and web-viewable renditions of files from the WebCenter Content user interface, you can configure Inbound Refinery to provide them. You can set up an Inbound Refinery provider for thumbnails and file conversions, such as PDF Export, through the native user interface.

To configure thumbnails in Content Server:

1. Access Content Server with the native user interface:

```
http://WCCHOST1:16200/cs
```

2. From the **Administration** menu or tray, choose **Configure Thumbnail Options**.
3. Select **Enable this server to create the thumbnail images** box.
4. Click the **Update** button.

For more information about generating thumbnails and web-viewable renditions, see *Configuring Inbound Refinery* in *Managing Oracle WebCenter Content*.

2.5.6 Configuring Digital Asset Management in Content Server

Digital Asset Management (DAM) is available through the WebCenter Content user interface. To enable the DAM user interface in Content Server, you need to enable the DigitalAssetManager, DAMConverterSupport, ContentBasket, and ZipRenditionManagement components and set up document conversion for DAM documents in Inbound Refinery.

To configure DAM in Content Server:

1. Log in to Content Server (<http://WCCHOST1:16200/cs>) as a WebCenter Content administrator.
2. Enable these components, or verify that they are enabled:
 - DigitalAssetManager
 - DAMConverterSupport
 - ContentBasket
 - ZipRenditionManagement (enabled by default)
3. Restart Content Server.
4. Log in to the Inbound Refinery Managed Server (<http://WCCHOST1:16250/ibr>) by default, as an administrator, and enable the DAMConverter component for DAM.
5. Restart the Inbound Refinery Managed Server.
6. Log in to Content Server again as an administrator to choose file formats for conversion:
 - a. From the **Administration** menu or tray, choose **Desktop Client Apps** and then **Configuration Manager**.
 - b. From the **Options** menu, choose **File Formats**.
 - c. For image asset formats that you want to convert to digital assets (such as **image/gif** and **image/png**, change the conversion to **Digital Media Graphics**.

For more information about configuring DAM in Content Server and the Inbound Refinery Managed Server, see *Configuring Digital Asset Manager* in *Managing Oracle WebCenter Content*.

2.5.7 Configuring Extended Features in Content Server

Some Content Server features are supported but not necessarily required by the WebCenter Content user interface. For example, Access Control Lists (ACLs) and Accounts are not configured out of the box. If these features are enabled on Content Server, however, the WebCenter Content user interface provides access to the additional functionality.

For information about enabling ACLs in Content Server, see [Managing Access Control List Security](#).

For information about enabling Accounts in Content Server, see [Managing Accounts](#).

You can set up one of the three indexing configurations for Content Server: Oracle Text Search, Database metadata, or Database full text. For more information about how to do this, see [Configuring the Search Index](#).

These standard Content Server settings are not specific to the WebCenter Content user interface.

2.5.8 Completing the Workflow Configuration

To complete the workflow configuration for the WebCenter Content user interface, you need to restart the Managed Servers and verify the configuration. The `UseDatabaseWfInQueue` configuration variable enables the WebCenter Content user interface to filter workflows assigned to a user. The `EmailNotificationType` configuration variable specifies where the links in notification emails point for workflows and subscriptions in different Content Server user interfaces, and its default value is `NativeWebUI`.

To complete the workflow configuration:

1. Set `UseDatabaseWfInQueue=1` in `config.cfg`.
2. Make sure that the `WCC_DOMAIN/ucm/cs/config/config.cfg` file contains the `EmailNotificationType` variable with either of the following settings:
 - To generate emails with links that point only to the WebCenter Content user interface, set `EmailNotificationType=ContentUI` in `config.cfg`.
 - To generate emails with links that point to both the WebCenter Content user interface and the native user interface, set `EmailNotificationType=ContentUI,NativeWebUI` in `config.cfg`.
3. Restart the Content Server Managed Server.
4. Click the alert that appears on the Content Server home page after restart: Click to complete workflow setup.

Ensure that Content Server returns a success message: `Workflow setup is now complete.`
5. Restart the WebCenter Content user interface Managed Server.

For more information about workflows, see [Managing Workflows in Managing Oracle WebCenter Content](#).

2.6 Associating the WebCenter Content User Interface with Content Server

You can configure a JAX-WS, IDCS, IDC, HTTP, or HTTPS connection between the WebCenter Content user interface Managed Server and Content Server, to associate the WebCenter Content user interface with Content Server.

The following topics describe how to configure these connections:

- [Configuring a JAX-WS Connection from the WebCenter Content User Interface Server to Content Server](#)
- [Configuring a Secured Connection from the WebCenter Content User Interface Server to Content Server](#)
- [Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server](#)
- [Configuring an IDC Connection from the WebCenter Content User Interface Server to Content Server](#)
- [Configuring an HTTP Connection from the WebCenter Content User Interface Server to Content Server](#)
- [Configuring an HTTPS Connection to Content Server Without a Certificate](#)

2.6.1 Configuring a JAX-WS Connection from the WebCenter Content User Interface Server to Content Server

Complete the steps described in this section to configure a JAX-WS connection from the WebCenter Content user interface to Content Server.

To configure a JAX-WS connection to Content Server:

1. Ensure that Metadata Services (MDS) schemas have been created in Oracle Database by the Repository Creation Utility (RCU).

Create an MDS schema for the common Oracle WebCenter Content and WebCenter Content user interface domains.

2. Apply the WSM Policy Manager Template to the common Oracle WebCenter Content domain and the WebCenter Content user interface domain, if the domain does not already have this template. The template is in this file:

```
MW_HOME/oracle_common/common/templates/applications/  
oracle.wsmmpm_template_11.1.1.jar
```

If the file is not in the `MW_HOME/oracle_common/common/templates/applications` directory, you can extend the domain with the template.

To extend a domain with the WSM Policy Manager Template:

- a. If a Managed Server in the domain that you are planning to extend is running, stop it through the Administration Console.
- b. Launch an Oracle WebLogic Scripting Tool (WLST) shell in offline mode.

- c. Run the following commands in sequence:

```
wls:/offline> readDomain(r'${DOMAIN_HOME}')

addTemplate(r'${MW_HOME}/oracle_common/common/templates/applications /
oracle.wsmpt_template_11.1.1.jar')

updateDomain()


closeDomain()

exit()
```

The `addTemplate.cmd` command creates a dummy schema.

3. Restart the Administration Servers in the common domain.
4. For the common domain, update the `mds-owsm` JDBC connection pool to point to the MDS schema for the domain. The targets should be the Administration Server and all Oracle ADF servers. The update can be done from **Services > Data sources > mds-owsm** in the Administration Console.

After updating a domain, restart the corresponding Administration Server. Confirm that **Monitoring > Testing > Check data source** is giving zero errors. A success message is expected, like "Test of mds-owsm on server AdminServer was successful."

 **Note:**

Use separate schemas for ADF UI connection architecture and ADF UI OWSM.

5. Restart both the Managed Servers for UCM and Web user interface.
6. Create a policy set for the WebCenter Content user interface domain:
 - a. In Oracle Enterprise Manager Fusion Middleware Control, expand **WebLogic Domain** in the navigation tree on the left, and then click the name of the domain.
 - b. From the **WebLogic Domain** drop-down menu at the top of the domain page, choose **Web Services**, then **Policy Sets**.
 - c. From the **Type of Resources** menu under **Policy Set Summary**, choose **Web Service Client**, enter a name for the policy set in the **Name** field, and click **Create**.
 - d. Make sure the policy set is enabled.
 - e. Under the scope, enable the policy set, enter the name of the domain in the **Domain Name** field, and then attach a policy, such as `oracle/wss10_saml_token_client_policy`.
7. Create a policy set for the Oracle WebCenter Content domain:
 - a. In Fusion Middleware Control, expand **WebLogic Domain** in the navigation tree on the left, and then click the name of the domain.
 - b. From the **WebLogic Domain** drop-down menu at the top of the domain page, choose **Web Services**, then **Policy Sets**.
 - c. From the **Type of Resources** menu under **Policy Set Summary**, choose **Web Service Endpoint**, enter a name for the policy set in the **Name** field, and click **Create**.

- d. Make sure the policy set is enabled.
 - e. Under the scope, enter the name of the domain in the **Domain Name** field, and then attach a policy, such as `oracle/wss_saml_or_username_token_service_policy`.
8. To expedite applying the policy changes, restart the servers.
 9. Confirm that the WebCenter Content web service has the GPA policy applied by inspecting the WSDL, at the following URL:

```
http://WCC_HOST:WCC_PORT/idcnativews/IdcWebLoginPort?WSDL
```

For example:

```
http://slc05amp.example.com:16200/idcnativews/IdcWebLoginPort?WSDL
```

In the WSDL, check for this code:

```
wsp:PolicyReference xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/  
policy"  
URI="#wss_saml_or_username_token_service_policy" wsdl:required="false"/>
```

10. To do an identity switch over the top of a standard SAML identity propagation policy, you need to be able to override subject precedence from its default value of `true`, to be `false` instead.

This instructs the server not to automatically send the connected subject, but rather allow it to explicitly set the identity that should be sent across.

The connection architecture has a Boolean property that you can set to activate an RIDC filter that results in `requestContext.put(ClientConstants.WSM_SUBJECT_PRECEDENCE, "false")` being set.

 **Note:**

If a Credential map exists, ensure that the `password` property (`oracle.wcc.ridc.credential.password`) is cleared from the Credential map before executing the following command. To check this property in Fusion Middleware Control, go to the WebCenter Content user interface page, and from the **WebLogic Server** drop-down menu, choose **Security**, then **Credentials**, then **WccAdf.oracle.wcc.adf**, and then **anonymous#WccAdfServerConnection**. To clear the property, click **Edit**, remove `oracle.wcc.ridc.credential.password`, and save the change.

To activate the RIDC filter, run the following command:

```
updateRIDCConnection('Oracle WebCenter Content - Web UI',  
'WccAdfServerConnection',  
connUrl="http://slc05elc.example.com:16200/idcnativews",  
jaxwsRegisteridentityswitchfilter="true",credImpersonationAllowed='false')
```

Run the following Connection Architecture command:

```
displayRIDCConnection('Oracle WebCenter Content - Web UI',
    'WccAdfServerConnection')
```

Now the Connection Architecture attributes should look as follows:

```
PropConnectionUrl = http://WCCUI_HOST:16200/idcnativews
PropConnectionSocketTimeout = null
PropConnectionPoolMethod = null
PropConnectionPoolSize = null
PropConnectionWaitTime = null
PropCredentialUsername = weblogic
PropCredentialAppIdKey = null
PropCredentialImpersonationAllowed = null
PropProtocolJaxWSStack = null
PropProtocolJaxWSPolicy = null
PropProtocolJaxWSJpsConfigFile = null
PropProtocolJaxWSSkipStackOptimize = null
PropProtocolJaxWSServerInsName = null
PropProtocolJaxWSRegisterIdentitySwitchFilter = true
PropProtocolHttpLibrary = null
PropProtocolIdcsAlgorithm = null
PropProtocolIdcsKeystoreFile = null
PropProtocolIdcsKeystoreAlias = null
PropProtocolIdcsTrustManagerFile = null
```

 **Note:**

Make sure `PropCredentialImpersonationAllowed` is set to null or false, not to true.

11. For an application to switch identity, grant it a special policy-code grant in the `system-jazn-data.xml` file, under `WCCUI_MW_HOME/user_projects/domains/WCCUI_domain/config/fmwconfig`. Change the name, as in the following code:

```
<grant>
  <grantee>
    <codesource>
      <url>file:${common.components.home}/modules/oracle.wsm.agent.
        common_11.1.1/wsm-agent-core.jar</url>
    </codesource>
  </grantee>
  <permissions>
    <permission>
      <class>oracle.wsm.security.WSIdentityPermission</class>
      <name>resource=Oracle WebCenter Content - Web UI</name>
      <actions>assert</actions>
    </permission>
  </permissions>
</grant>
```


12. Restart the WebCenter Content user interface Managed Server.

2.6.2 Configuring a Secured Connection from the WebCenter Content User Interface Server to Content Server

An SSL Incoming Provider is leveraged and instantiated to create an SSL server socket to which Intradoc clients can connect, and whereby traffic is encrypted. The provider can be configured with or without requiring client authentication (the WebCenter Content user interface Managed Server is a client of Content Server). When client authentication is not required, the JAVA RIDC client making the connection to the SSL server socket (Intradoc secure-socket port) does not need to present a valid certificate. This mode is not very different from a normal, non-SSL Intradoc connection. The main difference, however, is that traffic is encrypted and cannot be viewed by packet capture, and so on, in the clear. Client authentication means that the client must supply a valid SSL certificate signed by an authority that is in the server's trust store. In this context, client authentication is not tied to any particular end user, but rather to the Java client program. When the Require Client Authentication option is selected for the provider, and a secure Intradoc connection is made by the Java RIDC client to Content Server, a client that does not present a valid certificate will receive an exception, such as this one:

```

javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate
oracle.stellent.ridc.protocol.ProtocolException:
javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate at
oracle.stellent.ridc.protocol.intradoc.HdaProtocol.readResponse(HdaProtocol.java:257) at oracle.stellent.ridc.IdcClient.sendRequest(IdcClient.java:184) at Ping.ping(Ping.java:42) at Ping.main(Ping.java:20) Caused by:
javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate at
com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Alerts.java:174) at
com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Alerts.java:136) at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.recvAlert(SSLSocketImpl.java:1720)
at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:954)
at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1138) at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.readDataRecord(SSLSocketImpl.java:753) at
com.sun.net.ssl.internal.ssl.AppInputStream.read(AppInputStream.java:75) at
java.io.BufferedReader.fill(BufferedReader.java:218) at
java.io.BufferedReader.read(BufferedReader.java:237) at
oracle.stellent.ridc.common.util.StreamUtil.readRawLine(StreamUtil.java:227)
at oracle.stellent.ridc.common.util.StreamUtil.readLine(StreamUtil.java:254)
at
oracle.stellent.ridc.protocol.intradoc.HdaProtocol.readHeaders(HdaProtocol.java:459) at
oracle.stellent.ridc.protocol.intradoc.HdaProtocol.readResponse(HdaProtocol.java:215)
    
```

If your client (the WebCenter Content user interface Managed Server) receives such an exception, first make sure that the `WCC_domain/ucm/cs/config/config.cfgfile` has

`SocketHostAddressSecurityFilter` correctly set. The `SocketHostAddressSecurityFilter` value includes the IP address of the client machine; for example:

```
#hostname -i :- 10.229.187.227
```

```
SocketHostAddressSecurityFilter=10.229.187.227|127.0.0.1|0:0:0:0:0:0:1
```

Failure to set `SocketHostAddressSecurityFilter` correctly will result in an exception such as `StatusMessage: Unable to establish connection to the server. Permission denied. Address '10.187.109.243' is not an allowable remote socket address.`

Setting `IntradocServerPort=XXXX` is not required. Setting this property allows for non-SSL/nonencrypted Intradoc connections to this particular port from machines in the preceding trusted IP address list.

 **Caution:**

If you want only SSL Intradoc connections with client-certificate authentication, but you inadvertently set `IntradocServerPort`, the client could go through this back door (assuming its IP address is in the trusted list).

2.6.3 Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server

You can configure an IDC secured (IDCS) connection with or without Require Client Authentication. The WebCenter Content user interface Managed Server is a client of Content Server.

This section contains the following topics:

- [Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server With Require Client Authentication](#)
- [Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server Without Require Client Authentication](#)

2.6.3.1 Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server With Require Client Authentication

You can configure an IDC secured (IDCS) connection with or without Require Client Authentication. The WebCenter Content user interface Managed Server is a client of Content Server.

To configure an IDC secured connection with **Require Client Authentication**:

1. In the Oracle WebCenter Content domain, make the following changes, in a `bash` environment:
 - a. Enter the following command to set the domain environment:

```
source WCCUI_DOMAIN_HOME/bin/setDomainEnv.sh
```

- b. Create a directory named `sslkeepaliveincomingprovider`:

```
mkdir -p $WCC_DOMAIN_HOME/ucm/cs/data/providers/
sslkeepaliveincomingprovider
cd $WCC_DOMAIN_HOME/ucm/cs/data/providers/sslkeepaliveincomingprovider
```

You can use a different name, as long as the directory name matches the provider name specified in Step 2d.

- c. Use the CertGen utility to create a server key-certificate pair signed by the demo CA cert CertGenCA, as follows:

```
java utils.CertGen -certfile ServerPublicCert -keyfile ServerPrivKey -
keyfilepass password -cn "`hostname -f`"
```

- d. Create a server keystore with the server key-certificate pair.

```
java utils.ImportPrivateKey -keystore keystore.jks -storepass password -
certfile ServerPublicCert.der -keyfile ServerPrivKey.der -keyfilepass
password -alias serverkey -keypass password
```

- e. Add the root CA to the server keystore, using the keytool utility:

```
keytool -importcert -file $WL_HOME/server/lib/CertGenCA.der -keystore
keystore.jks -storepass password -noprompt
```

The alias is not provided in the preceding command because it will be imported under the alias name `mykey`.

- f. Add the root CA to the trust keystore:

```
keytool -importcert -file $WL_HOME/server/lib/CertGenCA.der -keystore
truststore.jks -storepass welcome1 -noprompt
```

The alias is not provided in the preceding command because it will be imported under the alias name `mykey`.

2. In Oracle WebCenter Content Server, add a provider:

- a. Log in to the WebLogic Content user interface for Content Server, using the administrator user name and password.
- b. From the **Administration** tray or menu, choose **Providers**.
- c. On the Providers page, in **Provider Type** column of the **Create a New Provider** table, click **sslincoming** and then **Add** in the **Action** column of the same row.
- d. On the Add Incoming Provider page, enter or keep the following field values:
 - **Provider Name:** `sslkeepaliveincomingprovider` (or the name of the directory created in Step 1b.)
 - **Provider Description:** For testing RIDC over SSL
 - **Provider Class:** `idc.provider.ssl.SSLSocketIncomingProvider`
 - **Connection Class:** `intradoc.provider.SocketIncomingConnection`
 - **Server Thread Class:** `intradoc.server.IdcServerThread`

- **Server Port:** 9995
 - **Require Client Authentication:** Select.
 - **Keystore File Path:** Select Use Default (This value specifies \$WCC_DOMAIN_HOME/ucm/cs/data/providers/sslkeepaliveincomingprovider/keystore.jks)
 - **Keystore Password:** password
 - **Alias:** serverkey
 - **Alias Password:** password
 - **Truststore File Path:** Select Use Default (This value specifies \$WCC_DOMAIN_HOME/ucm/cs/data/providers /sslkeepaliveincomingprovider/truststore.jks)
 - **Truststore Password:** password
- e. Click the **Add** button at the bottom of the page.
- f. Restart the WebCenter Content Managed Server.
3. Verify the `WCC_DOMAIN_HOME/ucm/cs/data/providers/sslkeepaliveincomingprovider/provider.hda` file that gets generated. It should contain the following text:

```
- note passwords in clear!!
cat provider.hda
<?hda version="11gR1-11.1.1.7.0-idxprod1-120807T112220" jcharset="UTF8"
encoding="utf-8"?>
@Properties LocalData
=I
ncomingThread=intradoc.server.IdcServerThread
IntradocServerHostName=
KeystoreAlias=serverkey
KeystoreAliasPassword=password
KeystoreFile=/u01/app/oracle/product/Middleware/user_projects/domains/
base_dom
ain/ucm/cs/data/providers/sslkeepaliveincomingprovider/keystore.jks
KeystorePassword=password
NeedClientAuth=
PasswordScope=sslkeepaliveincomingprovider
ProviderClass=idx.provider.ssl.SSLSocketIncomingProvider
ProviderConfig=
ProviderConnection=intradoc.provider.SocketIncomingConnection
ProviderType=sslincoming
ServerPort=9995
TruststoreFile=/u01/app/oracle/product/Middleware/user_projects/domains/
base_do
main/ucm/cs/data/providers/sslkeepaliveincomingprovider/truststore.jks
TruststorePassword=password
UseDefaultKeystoreFile=1
UseDefaultTruststoreFile=1
WantClientAuth=
blDateFormat=M/d{/yy}{ h:mm[:ss]{ a}}!mAM,PM!tPST8PDT
@end
```

4. From the WebCenter Content user interface Managed Server machine, make the following changes (if you are requiring client authentication).

- a. Enter the following command to set the domain environment:

```
source WCCUI_DOMAIN_HOME/bin/setDomainEnv.sh
```

- b. Go to the user home directory:

```
cd /home/user
```

- c. Use the CertGen utility to create a client key-certificate pair signed by the demo CA cert CertGenCA, as follows:

```
java utils.CertGen -certfile ClientPublicCert -keyfile ClientPrivKey -keyfilepass password [-cn "`hostname -f`"]
```

 **Note:**

The optional `-cn` argument determines the common name to which the certificate is issued. If this argument is skipped, the certificate is issued to the host name of the machine from which the certificate is generated.

- d. Create a client keystore for the WebCenter Content user interface Managed Server, with the client key-certificate pair:

```
java utils.ImportPrivateKey -keystore keystore.jks -storepass password -certfile ClientPublicCert.der -keyfile ClientPrivKey.der -keyfilepass password -alias clientkey -keypass password
```

- e. Add the root CA to the client keystore, using the keytool utility:

```
keytool -importcert -file WCCUI_WL_HOME/server/lib/CertGenCA.der -keystore keystore.jks -storepass password -noprompt
```

5. Connect to the WebCenter Content user interface Managed Server.

6. Run the following `updateRIDCCConnection()` command, on one line:

```
updateRIDCCConnection('Oracle WebCenter Content - WebUI',
  'WccAdfServerConnection', connUrl='idcs://adc2120610.example.com:9995',
  credUsername='weblogic', idcsKeystoreFile='/home/user/keystore.jks',
  idcsKeystorePassword='password', idcsKeystoreAlias='clientkey', idcsKeystoreAliasPassword='password')
```

After the preceding command is run, the `cwallet.sso` file is updated under `/users/username/AppData/Roaming/JDeveloper/system11.1.2.2.39.61.83.1/DefaultDomain/config/fmwconfig`. The `cwallet.sso` file contains the password, as follows (decrypted content):

```
### Map: WccAdf.oracle.wcc.adf
1. + Key: anonymous#WccAdfServerConnection
class = oracle.security.jps.internal.credstore.GenericCredentialImpl
desc = null
type = java.util.Hashtable
```

```
cred = (oracle.wcc.ridc.protocol.idcs.keystore.alias.password, password)
cred = (oracle.wcc.ridc.protocol.idcs.keystore.password, password)
expires = null
```

7. Restart the WebCenter Content user interface Managed Server.

2.6.3.2 Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server Without Require Client Authentication

You can configure an IDC secured (IDCS) connection with or without Require Client Authentication. The WebCenter Content user interface Managed Server is a client of Content Server.

To configure an IDC secured connection without **Require Client Authentication** (only Content Server changes required):

1. Make the preceding changes to Content Server.
2. Connect to the WebCenter Content user interface Managed Server.
3. Run the following `updateRIDCConnection()` command, on one line

```
updateRIDCConnection('Oracle WebCenter Content - Web UI',
  'WccAdfServerConnection', connUrl='idcs://adc2120610.example.com:9995',
  credUsername='weblogic')
```

4. Ensure all other parameters are unset by running the `displayRIDCConnection('Oracle WebCenter Content - Web UI', 'WccAdfServerConnection')` cmd.
5. Restart the WebCenter Content user interface Managed Server.
6. If you encounter the following error message, you need to import a certificate from the Content domain into the Oracle WebCenter Content user interface domain:

```
Caused By: javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
```

This error means the certificate present in the WebLogic Server trusted store for the WebCenter Content Managed Server does not match or contain the `<cacerts>` entry present in WebLogic Server trusted store for Content Server). To import this certificate and add it to the trusted keystore in the WebCenter Content user interface domain:

- a. Export the Content Server certificate as `root.cer`:

```
keytool -export -file root.cer -keystore keystore_path
```

In the preceding command, `keystore_path` is the keystore that was configured on the `sslaliveincominprovider` page in Content Server. For example:

```
/user/11.1.1.9.0/mw9977/user_projects/domains/wccucm_domain/ucm/cs/data/
providers/sslkeepaliveincomingprovider/keystore.jks
```

- b. Enter the corresponding keystore password: `password`

- c. Import `root.cer` into the client:

```
Keytool -import -keystore <cacerts> -file root.cer
```

In the preceding command, `<cacerts>` is the Java Standard Trust Keystore that was specified for the WebCenter Content user interface Managed Server in the Administration Console. For example:

```
keytool -import -keystore jdk_location/jre/lib/security/cacerts -file  
root.cer
```

- d. If you are prompted for a password after running the preceding `keytool` command, you can enter the common password for a keystore.
- e. Restart the Web Center Content user interface Managed Server.

2.6.4 Configuring an IDC Connection from the WebCenter Content User Interface Server to Content Server

For an IDC connection to Content Server, the WebCenter Content user interface application is authenticated based on an IP address. Therefore, you need to make sure the `WCC_DOMAIN_HOME/ucm/cs/config/config.cfg` file has `SocketHostAddressSecurityFilter` set correctly. `SocketHostAddressSecurityFilter` includes the IP address of the client machine (the WebCenter Content user interface machine); for example: `#hostname - i :-
10.229.187.227 SocketHostAddressSecurityFilter=10.229.187.227|127.0.0.1|
0:0:0:0:0:0:0:1.`

To configure an IDC connection to Content Server:

1. Connect to the WebCenter Content user interface.
2. Run the following `updateRIDCCConnection()` command, on one line:

```
updateRIDCCConnection('Oracle WebCenter Content - Web UI',  
'WccAdfServerConnection',connUrl='idc://adc2120610.example.com:4444',  
credUsername='weblogic')
```

The port number `4444` is the `IntradocServerPort` value for Content Server.

3. Restart the WebCenter Content user interface Managed Server.

2.6.5 Configuring an HTTP Connection from the WebCenter Content User Interface Server to Content Server

The steps in this section describe how to configure an HTTP connection from the WebCenter Content UI to Content Server.

To configure an HTTP connection to Content Server:

1. Connect to the WebCenter Content user interface.
2. Run the following `updateRIDCCConnection()` command, on one line:

```
updateRIDCCConnection('Oracle WebCenter Content - Web UI',  
'WccAdfServerConnection',connUrl='http://adc2120610.example.com:7777/cs /
```

```
idcplg',credUsername='weblogic',credPassword='password',
httpLibrary='oracle',credImpersonationAllowed='true')
```

3. Restart the WebCenter Content user interface Managed Server.

2.6.5.1 Importing the Certificate from the Oracle WebCenter Content Domain to the WebCenter Content User Interface Domain

Over any secured connection, you need to follow the Certificate Authorities required to access secure sites using the SSL protocol. These Certificate Authorities may comprise the Identity and Trusted store.

If you see the following error on the WebCenter Content user interface Managed Server as soon as you try accessing it, you need to import the certificate for Content Server from the Oracle WebCenter Content domain to the WebCenter Content user interface domain:

```
Caused By: javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid
certification path to requested target
```

This error happens because the certificate present in the WebLogic Server trusted store for the WebCenter Content user interface domain does not match or contain the cacerts present in the Oracle WebCenter Content domain (which includes Content Server). Therefore, you need to import this certificate and install it in the trusted keystore for the WebCenter Content user interface domain.

To import the certificate from the Oracle WebCenter Content domain to the WebCenter Content user interface domain:

1. Export the Content Server certificate from a browser by opening the Content Server HTTPS URL and saving the certificate as, for example, `contentservercertificate.cer`.
2. Run the `keytool` utility from the same JDK location that is used by the WebLogic Server trusted keystore. You can find this location in the Administration Console, on the **Keystores** tab for the WebCenter Content user interface Managed Server. For example:

```
JAVA_HOME/bin/java/keytool -import -keystore
JAVA_HOME/jre/lib/security/cacerts -file contentservercertificate.cer
```

The output from this command is details about the certificate and a request for confirmation.

3. Confirm the certificate:

```
Trust this certificate? [no]: y
```

```
Certificate was added to keystore
```

If you are prompted for a password after running the preceding command, you can specify the common password for a keystore.

2.6.6 Configuring an HTTPS Connection to Content Server Without a Certificate

The steps in this section describe how to configure an HTTPS connection to Content Server without a certificate.

To configure an HTTPS connection to Content Server without a certificate:

1. Enable the SSL listen port in the WebLogic Server Administration Console. For example:

```
SSL listen port: 16201
```

2. Update the following two entries in the Content Server configuration file, `config.cfg`, under `WCC_MW_HOME/user_projects/domains/cs_domain/ucm/cs/config`:

```
HttpServerAddress=adc2120610.example.com:16201  
UseSSL=Yes
```

3. Restart the Oracle WebCenter Content Managed Server.
4. Connect to the WebCenter Content user interface.
5. Run the following `updateRIDCConnection()` command, on one line, with the appropriate SSL port:

```
updateRIDCConnection('Oracle WebCenter Content - Web UI',  
'WccAdfServerConnection',  
connUrl='https://adc2120610.example.com:16201/cs/idcplg',  
credUsername='weblogic',credPassword='password',httpLibrary='oracle',  
credImpersonationAllowed='true')
```

 **Note:**

In case the `httpLibrary` attribute is not set to `oracle` in the preceding command, Apache 3/4 is used for HTTP or HTTPS communication, so it is necessary to explicitly add the `httpclient/httpcodec` JAR in the WebCenter Content user interface (Model) classpath.

6. Restart the WebCenter Content Managed Server.

3

Managing System Processes

This chapter describes how to start and stop an Oracle Content Server or Inbound Refinery instance, how to start Content Server administration applications, and how to use a command-line tool to configure system variables.

This chapter includes the following topics:

- [Starting and Stopping Content Server and Inbound Refinery](#)
- [Starting and Stopping Content Server and Inbound Refinery Using Fusion Middleware Control](#)
- [Starting and Stopping Content Server Using WebLogic Server](#)
- [Starting and Stopping Content Server Using Scripts](#)
- [Running Content Server Administration Applications](#)
- [Using the IdcShell Command-Line Tool to Run Idoc Script](#)

3.1 Starting and Stopping Content Server and Inbound Refinery

There are several methods for starting, stopping, and restarting the Content Server instance. Which method you choose depends on your requirements, your authorization, and the task you want to complete. For example, when certain configuration changes are made to the Content Server instance, such as when components are enabled or disabled, the instance must be restarted.

For the Inbound Refinery (IBR) instance, the only method available is to use Oracle Enterprise Manager Fusion Middleware Control.

Available methods for managing the Content Server instance include:

- Oracle Enterprise Manager Fusion Middleware Control (see [Starting and Stopping Content Server and Inbound Refinery Using Fusion Middleware Control](#))
- Oracle WebLogic Server Administration Console (see [Starting and Stopping Content Server Using WebLogic Server](#))
- Oracle WebLogic Server scripts (see [Starting and Stopping Content Server Using Scripts](#))

Note:

In earlier releases, the Content Server's Admin Server could be used to start, stop, and restart the Content Server instance. This functionality has been replaced as of 11g Release 1 (11.1.1).

3.2 Starting and Stopping Content Server and Inbound Refinery Using Fusion Middleware Control

Oracle Enterprise Manager Fusion Middleware Control is used by administrators to manage an Oracle WebLogic Server running a WebCenter Content domain with the Content Server or Inbound Refinery instance.

The Content Server and Inbound Refinery instances are initially started during the process of installing and deploying the instance on a managed server on an Oracle WebLogic Server domain. The Content Server and Inbound Refinery instances can be stopped and restarted for several reasons, including changing the configuration, such as enabling or disabling a component.

- [Starting Content Server or Inbound Refinery Using Fusion Middleware Control](#)
- [Stopping Content Server or Inbound Refinery Using Fusion Middleware Control](#)
- [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#)

See Starting and Stopping Oracle WebLogic Server Instances in *Administering Oracle Fusion Middleware*.

3.2.1 Starting Content Server or Inbound Refinery Using Fusion Middleware Control

To start the Content Server or Inbound Refinery (IBR) instance:

1. Log in to Fusion Middleware Control.
2. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`), then **WebCenter**, then **Content**.
 - For the Content Server instance, expand **Content Server**, then select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
 - For the Inbound Refinery instance, expand **Oracle Inbound Refinery**, then select the Inbound Refinery instance name (for example, `IBR (IBR_server1)`).
3. On the instance home page, from the **Content Server** or **IBR** menu choose **Control**, then **Start**.

3.2.2 Stopping Content Server or Inbound Refinery Using Fusion Middleware Control

To stop the Content Server or Inbound Refinery (IBR) instance:

1. Log in to Fusion Middleware Control.
2. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`), then **WebCenter**, then **Content**.
 - For the Content Server instance, expand **Content Server**, then select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).

- For the Inbound Refinery instance, expand **Oracle Inbound Refinery**, then select the Inbound Refinery instance name (for example, `IBR (IBR_server1)`).
3. On the instance home page, from the **Content Server** or **IBR** menu choose **Control**, then **Shut Down...**

3.2.3 Restarting Content Server or Inbound Refinery Using Fusion Middleware Control

To restart the Content Server or Inbound Refinery (IBR) instance:

1. Log in to Fusion Middleware Control.
2. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`), then **WebCenter**, then **Content**.
 - For the Content Server instance, expand **Content Server**, then select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
 - For the Inbound Refinery instance, expand **Oracle Inbound Refinery**, then select the Inbound Refinery instance name (for example, `IBR (IBR_server1)`).
3. On the instance home page, from the **Content Server** or **IBR** menu choose **Control**, then **Shut Down...**
4. Confirm that the instance is shut down.
5. From the **Content Server** or **IBR** menu choose **Control**, then **Start**.

3.3 Starting and Stopping Content Server Using WebLogic Server

The Oracle WebLogic Server Administration Console is available to Content Server administrators because they must have administrative privileges to manage WebCenter Content with the Content Server instance. The Node Manager must be configured and running in order to start or stop the WebCenter Content managed server with the Content Server instance.

The Content Server instance is initially started during the process of installing and deploying the instance on a WebCenter Content server in an Oracle WebLogic Server domain. You might want to start the Content Server instance at other times, for example, to start the instance after it has been stopped when changing a Content Server configuration setting.

The Content Server instance can be stopped and restarted for several reasons, including changing the configuration, such as enabling or disabling a server component.

- [Starting Content Server Using WebLogic Server Administration Console](#)
- [Stopping Content Server Using WebLogic Server Administration Console](#)
- [Restarting Content Server Using WebLogic Server Administration Console](#)

See Starting and Stopping Oracle WebLogic Server Instances in *Administering Oracle Fusion Middleware*.

3.3.1 Starting Content Server Using WebLogic Server Administration Console

To start the Content Server instance:

1. On the Administration Console home page, in the Domain Configurations area, choose **Environment**, then **Servers**.
2. On the **Configuration** tab for the Summary of Servers page, select the name of the WebCenter Content server for the Content Server instance.
3. In the Settings for *server_name* section, click the **Control** tab.
4. On the **Start/Stop** tab, in the Server Status area, select the server name (for example, *UCM_server1*), then click **Start**.

3.3.2 Stopping Content Server Using WebLogic Server Administration Console

To stop the Content Server instance:

1. On the Administration Console home page, in the Domain Configurations area, choose **Environment**, then **Servers**.
2. On the **Configuration** tab for the Summary of Servers page, select the name of the WebCenter Content server for the Content Server instance.
3. In the Settings for *server_name* section, click the **Control** tab.
4. On the **Start/Stop** tab, in the Server Status area, select the server name (for example, *UCM_server1*), then click **Shutdown**.

3.3.3 Restarting Content Server Using WebLogic Server Administration Console

To restart the Content Server instance:

1. On the Administration Console home page, in the Domain Configurations area, choose **Environment**, then **Servers**.
2. On the **Configuration** tab for the Summary of Servers section, select the name of the WebCenter Content server for the Content Server instance.
3. In the Settings for *server_name* section, click the **Control** tab.
4. On the **Start/Stop** tab, in the Server Status area, select the server name (for example, *UCM_server1*), then click **Shutdown**.
5. Confirm that the Content Server instance has stopped, then click **Start** (or **Resume**).

3.4 Starting and Stopping Content Server Using Scripts

Scripts provide a quick method to execute actions on Oracle WebLogic servers. Before you can start a Managed Server for an application, you must start the Administration Server for the Oracle WebLogic Server domain.

The following script examples assume that the Content Server instance has been previously started as part of the software installation process. See *Installing and Configuring Oracle WebCenter Content*.

 **Caution:**

These script commands control the Oracle WebLogic Server, which includes the WebCenter Content and WebLogic Administration Servers. The Administration Server includes the Administration Console. If you do not want to start or stop the Oracle WebLogic Administration Server, then use another method to start the Content Server instance.

- [Starting Content Server Using Scripts](#)
- [Stopping Content Server Using Scripts](#)
- [Restarting Content Server Using Scripts](#)

3.4.1 Starting Content Server Using Scripts

To start the Content Server instance:

1. Run the appropriate type of script to start the Oracle WebLogic Server Administration Console.
2. Run the appropriate type of script to start the Oracle WebLogic Server Managed Server with the WebCenter Content server with the Content Server instance. In the following script examples, the instance is named `UCM_server1`.

Windows script:

```
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\startWebLogic.sh  
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\startManagedWebLogic.sh UCM_server1
```

UNIX script:

```
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/startWebLogic.sh  
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/startManagedWebLogic.sh UCM_server1
```

3.4.2 Stopping Content Server Using Scripts

To stop the Content Server instance:

1. Run the appropriate script to stop the WebCenter Content server with the Content Server instance on the Oracle WebLogic Server Managed Server. In the following script examples the instance is named `UCM_server1`.
2. Next, only if necessary, run the script to stop the Oracle WebLogic Server Administration Console.

Windows script:

```
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\stopManagedWebLogic.sh UCM_server1  
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\stopWebLogic.sh
```

UNIX script:

```
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/stopManagedWeblogic.sh UCM_server1  
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/stopWebLogic.sh
```

3.4.3 Restarting Content Server Using Scripts

To restart the Content Server instance:

1. Run the appropriate script to stop the Oracle WebLogic Server Managed Server with WebCenter Content and the Content Server instance. In the following script examples the instance is named `UCM_server1`.
2. Next, only if necessary, run the script to stop the Oracle WebLogic Server Administration Server.
3. When the server or servers have stopped, if appropriate run the script to start the Oracle WebLogic Server Administration Server.
4. Run the script to start the Oracle WebLogic Server Managed Server with WebCenter Content and the Content Server instance.

Windows script:

```
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\stopManagedWeblogic.sh UCM_server1  
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\stopWeblogic.sh  
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\startWeblogic.sh  
MW_HOME\user_projects\domains\DOMAIN_HOME\bin\startManagedWeblogic.sh UCM_server1
```

UNIX script:

```
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/stopManagedWeblogic.sh UCM_server1  
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/stopWeblogic.sh  
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/startWeblogic.sh  
MW_HOME/user_projects/domains/DOMAIN_HOME/bin/startManagedWeblogic.sh UCM_server1
```

3.5 Running Content Server Administration Applications

You can run Content Server administration applications either as applets or in standalone mode. Running applications in standalone mode requires additional configuration for database connections and that the Content Server administrator be a local user.

- [Running Administration Applications as Applets](#)
- [Running Administration Applications via the Oracle WebCenter Content Administration App](#)
- [Running Administration Applications in Standalone Mode](#)

3.5.1 Running Administration Applications as Applets

You can run several of the Content Server administration applications as applets from any web browser with access to the Content Server instance. Applets are convenient for remote administration.

 **Note:**

The Batch Loader, Component Wizard, System Properties, and Content Server Analyzer utilities cannot be run as applets; for security reasons, they must be run in standalone mode from the computer where the Content Server instance is deployed. See [Running Administration Applications in Standalone Mode](#).

Some functions that are available in the standalone version of an application are not available from the applet version. See the documentation for each application for more information.

To run an administration application as a Java applet within a Java-enabled browser:

1. Open a browser window.
2. Log in to the Content Server instance as an administrator.
3. Choose **Administration**, then **Desktop Client Apps**.
4. Choose an administration application from the list of applets.

3.5.2 Running Administration Applications via the Oracle WebCenter Content Administration App

You can run these Content Server administration applications using the desktop admin app: Archiver, Configuration Manager, Content Categorizer Administration, Data Engine Control Center, PDF Watermark Administration, Repository Manager, User Admin, Web Layout Editor, and Workflow Admin. You can also run the admin app in a browser via the native user interface.

The Batch Loader, Component Wizard, System Properties, and Content Server Analyzer utilities cannot be accessed via the desktop app for security reasons. They must be run in the standalone mode from the computer where the Content Server instance is installed. See [Running Administration Applications in Standalone Mode](#).

Some functions that are available in the standalone version of an application are not available in the desktop app. See the documentation for each application for more information.

Before You Begin

- The desktop admin app is supported only for 12.2.1.4.0 and higher releases.
- The desktop admin app supports the corporate single sign on (SSO).
- In the scenarios where the Content Server is front-ended by a load balancer or Oracle HTTP Server, the desktop admin app uses the URL of either of these to access the Content Server.
- The desktop admin app is designed to run on Windows, Mac, and Linux. See the certification matrix for information on the supported versions of these operating systems.
- If you have not already installed the admin app, you can do so now. Installers for Windows, Mac, and Linux are available for download via **Content Server Home > Administration > Desktop Client Apps**.

 **Note:**

After the installation is successfully completed, a desktop icon is created for you. The desktop admin app is installed at the following locations:

- **Windows:** C:\Program Files\Oracle WebCenter Content Administration. If the c:\ drive is not available, the installer automatically detects the program files folder, and the app is installed in that folder. To set proxy, if you use a server URL and port instead of a pac script, ensure that the URL is configured in the Internet Explorer options.
- **Mac:** /Applications/Oracle WebCenter Content Administration. On Mac, the proxy should be configured in **Safari > Preferences**.
- **Linux:** Where .tar is extracted. On Unix, you can set the proxy server in the terminal before launching the script: `export http_proxy=http://my.proxyserver.net:8080/`

- Once you've downloaded the .tar file for Linux, untar it. Instructions to install the admin app on Linux are available in the README file located in the wccadmin folder.
- When a new version of the admin app is available, the following message is displayed on your screen when you try to launch an older version of the app:

This version of the Administration client is too old to connect to the Content Server. Please install the Administration client associated with the Content Server.

On Windows and Mac, you can launch the app from the browser via the CS Administration Apps page by clicking **Launch Client**. To use the desktop admin app in a browser, you must first specify the Http server address in the `config.cfg` of the Content Server, if it's not already specified.

To run an administration application using the desktop app:

1. Double-click the desktop icon that is created after you install the app.
2. In the **Oracle WebCenter Content - Administration** dialog, log in to the Content Server instance as an administrator or subadministrator:
 - a. In the **User Name** field, enter the user name that has access rights.
 - b. In the **Password** field, enter the password.
 - c. In the **Server** field, enter the server address of your Content Server instance in this format: `https://host.example.com:16200/cs/`
If the Content Server version is compatible with the desktop admin app, then the app connects to the server and the last connected server URL is saved in this field. You can select the this URL from this drop-down list for subsequent logins. In case you try to connect to incompatible versions, an error message is displayed.
 - d. Click **OK**.
The WebCenter Administration app is displayed. This app lets you configure and manage the following applications: Archiver, Configuration Manager, Content Categorizer Administration, Data Engine Control Center, PDF Watermark Administration, Repository Manager, User Admin, Web Layout Editor, and Workflow Admin.

 **Note:**

The application are listed based on the users privileges and the components that are enabled in the Content Server.

3. In the WebCenter Administration app, click the application you want to configure or whose configurations you want to edit to display its configuration page.

3.5.3 Running Administration Applications in Standalone Mode

You can run Content Server administration Java applications in standalone mode from the computer where a Content Server instance is deployed. Some of the applications are the same as the apps accessed using a web browser, such as Configuration Manager and Repository Manager. Some utilities can be run only in standalone mode, such as System Properties and Batch Loader. The method required to start these programs differs slightly between Windows and UNIX installations.

Running the standalone version of an application offers greater security than browser apps, and enables you to send passwords without having them captured or copied from the web or a network.

Standalone administration applications require that the Content Server system administrator running the applications be a *local* admin user, instead of a user defined through Oracle WebLogic Server. (Local users are otherwise unused in Oracle WebLogic Server.) To use standalone administration applications that require a log-in, run the User Admin app and define a new local user with Admin permissions in Content Server. For information on local users, see [Local Users](#). For details on using the User Admin app to create a local user, see [Editing a User Login](#).

 **Note:**

Before you can run Content Server administration applications in standalone mode, additional configuration is required to authenticate the applications on Oracle WebLogic Server and to establish a JDBC connection to the system database and access to the Oracle WebLogic Server database connection. See [Configuring a System Database Provider for Standalone Mode](#) and [Configuring an External Database Provider for Standalone Mode](#).

If a standalone application is required to connect to a SSL-enabled database where digital certificates are used for authentication, then the database root CA certificate must be imported into the standard Java key store that the application uses to check trusted sources. See [Configuring the WebCenter Content Domain in Installing and Configuring Oracle WebCenter Content](#).

- [Running a Standalone Application on a UNIX System](#)
- [Running a Standalone Application on a Windows System](#)
- [Configuring a System Database Provider for Standalone Mode](#)
- [Configuring a JDBC Database Driver for Standalone Mode](#)
- [Configuring an External Database Provider for Standalone Mode](#)

3.5.3.1 Running a Standalone Application on a UNIX System

To run a Content Server administration application in standalone mode on a UNIX operating system:

1. Navigate to the `DomainHome/ucm/cs/bin/` directory. Executable applications are listed.
2. Enter `./application_name`, where `application_name` is the name of an executable file. If an application is not listed, it can be entered as a parameter to the `IntradocApp` application, as in this example:

```
% ./intradocApp workflow
```

3. Click **Enter**. For all applications except for the Component Wizard and the System Properties utility, a login window opens. For the Component Wizard and the System Properties utility, the main window of the application opens.
4. Enter the administrator login name and password.
5. Click **OK**.

3.5.3.2 Running a Standalone Application on a Windows System

To run a Content Server administration application in standalone mode on a Windows operating system.

1. Select the application or utility from the Windows **Start** menu:
 - To run an administration application, from the **Start** menu choose **Programs**, then **Content Server**, then *instance*, then *application*.
 - To run an administration utility, from the **Start** menu choose **Programs**, then **Content Server**, then **Utilities**, then *utility*.

For all applications except for the Component Wizard and the System Properties utility, a login window opens. For the Component Wizard and System Properties utility, the main window of the application opens.

 **Tip:**

It may take several seconds for the login window or the application window to appear, or the window may be hidden by other windows.

2. Enter the administrator login name and password.
3. Click **OK**.

The main window of the application opens.

3.5.3.3 Configuring a System Database Provider for Standalone Mode

Content Server administration applications and utilities that can only run in standalone mode require specific configuration to run in an Oracle WebLogic Server domain with Oracle WebCenter Content and the Content Server instance. The configuration changes for a standard (non-customized) Oracle WebLogic Server connection are necessary to have the applications authenticate Oracle WebLogic Server users and to set up a JDBC connection to the Oracle WebLogic Server system database.

Follow these steps to configure connections for standalone mode:

1. As system administrator, use VNC (or a similar tool such as putty or Xming) to navigate to the `DOMAIN_HOME/ucm/cs/bin/` directory. For example:

```
MW_HOME/user_projects/domains/ucm_domain/ucm/cs/bin
```

2. Run `./SystemProperties`.
3. In the **Paths** tab of the System Properties window, the **Specify Database Driver Classpath** check box is selected by default, so you must enter a path to a JDBC driver for your system database in the **Database Driver Classpath** field.

The Oracle driver `ojdbc6dms.jar` is provided with the Enterprise Content Management install in the following directory.

```
MW_HOME/oracle_common/modules/oracle.jdbc_11.1.1/ojdbc6dms.jar
```

4. In the **Database** tab, enter all the necessary JDBC connection information in the fields for your system database (database type, database user name, database user password, and so on).
5. Click **OK**. You should now be able to run a standalone application. For example, as the Administrator user you created on the Content Server instance, run `./BatchLoader`.

3.5.3.4 Configuring a JDBC Database Driver for Standalone Mode

For Content Server to work with administration applications that only run in standalone mode (for example, Batch Loader, System Properties, and Content Server Analyzer utilities) you must configure a JDBC driver for the system database or an external database provider. Oracle Fusion Middleware DataDirect JDBC drivers for Microsoft SQL Server and IBM DB2 databases are available to support Content Server standalone applications. You can use the System Properties utility to enter the configuration information.

To configure a JDBC Driver for standalone applications:

1. As a WebCenter Content system administrator, run `SystemProperties` from the `bin/` directory for the Content Server instance to start the System Properties utility:
 - **UNIX path:** `DomainHome/ucm/cs/bin/SystemProperties`
 - **Windows path:** `DomainHone\ucm\cs\bin\SystemProperties`
2. On the System Properties screen, click the **Database** tab, then select the appropriate driver and enter the connection string, user name, and password.

You do not need to enter a classpath or driver name, or copy any JAR files.

You can find JDBC connection string and user name information in the Oracle WebLogic Server Administration Console. Log in to the Administration Console, then select **Services**, then **Data Sources**, then **CSDS**, then **Connection Pool**. In the **Connection Pool** tab, the connection string is in the **URL** field, and the user name is in the **Properties** field. For security, the password is not displayed.

3. In the **Database** tab, select the appropriate driver under **Use Java Database Connectivity**, and enter the connection string.
 - For Microsoft SQL Server, select **DataDirect SQL Server JDBC Driver**, and enter a connection string of this form:

```
jdbc:weblogic:sqlserver://  
database_hostname:database_port_number;databaseName=database_name
```

- For IBM DB2, select **DataDirect DB2 JDBC Driver**, and enter a connection string of this form:

```
jdbc:weblogic:db2://
database_hostname:database_port_number;databaseName=database_name
```

4. Enter the user name and password for the database in the **JDBC User Name** and **JDBC User Password** fields.
5. Click **OK**.
6. Restart the Content Server instance.

3.5.3.5 Configuring an External Database Provider for Standalone Mode

You can create an external database provider in the Content Server instance for standalone applications to directly connect to a database with JDBC without using the System Database provider for the Oracle WebLogic Server data source.

For standalone applications to use the OracleTextSearch feature as an external search engine, you must configure the external database provider to include the JDBC connection information.

By default, the configuration of an incoming provider does not include values for **JDBC Driver** and **JDBC Connection String**. You must add these values, but be careful not to change the provider name because you cannot rename an existing provider. To change the name of a provider, you would need to delete it and then add it again.

3.6 Using the IdcShell Command-Line Tool to Run Idoc Script

The IdcShell tool enables administrators to run Idoc Script from a command line. Idoc Script is a proprietary server-side custom scripting language for the WebCenter Content system. This scripting language enables administrators to reference variables, conditionally include content in HTML pages, and loop over results returned from queries.

Idoc Script is used primarily for configuration settings and the presentation of HTML templates. Idoc variables (sometimes called *configuration variables* or *environment variables*) can be used in Idoc Script and in configuration files. See Configuration Variables in *Configuration Reference for Oracle WebCenter Content*. See Introduction to the Idoc Script Custom Scripting Language in *Developing with Oracle WebCenter Content*.

The IdcShell tool also includes some additional Idoc Script functions, listed in [Table 3-1](#), and some dynamichtml definitions, listed in [Table 3-2](#), which are useful for managing Content Server or Inbound Refinery instances.

The IdcShell tool has built-in help, which you can access by running the command:

```
bin/IdcShell "include shell_help"
```

[Table 3-1](#) lists and describes Idoc Script functions typically used with the IdcShell command-line tool.

Table 3-1 Command-Line Idoc Script Functions

Function	Description
doService(serviceName)	Executes a serviceName in the current context.
formatBinder()	Formats a DataBinder for easy reading.
getWithTrace()	Traces the get() function and reports on the source of the data.
promptUser(text, flags)	Displays text on the console and reads a user response. If flags is NO_ECHO, then it does not echo input.

Table 3-2 lists and describes dynamichtml definitions typically used with the IdcShell command-line tool.

Table 3-2 Dynamichtml Definitions

Dynamichtml definition	Description
get_username	Prompts for a user name on the console and assigns to userName.
get_password	Prompts for a password on the console and assigned to dPassword.
set_user_password	Sets a user's password.
create_user	Creates a new user, by default with Admin role.

4

Batch Loading Content

This section provides information on how to use the Batch Loader utility to check in (insert), delete, and update a large number of files simultaneously on an Oracle WebCenter Content Server instance.

This chapter covers these topics:

- [About Batch Loading](#)
- [Preparing a Batch Load File](#)
- [Running the Batch Loader](#)
- [Optimizing Batch Loader Performance](#)
- [Best Practice Case Study](#)

4.1 About Batch Loading

Batch loading a number of files can be automated to save time and effort by using the Batch Loader utility. The following are examples of when to use Batch Loader:

- You just purchased the WebCenter Content software, and you want check in all of your existing files with metadata that exists in a database.
- You have documents checked in to the Content Server repository, and you just created a new custom metadata field. You can use Batch Loader to add the values you specify for the new metadata field to each existing content item.
- You want to remove a large number of specific files from the system.

Batch Loader performs actions that are specified in a batch load file, which is a text file that tells Batch Loader which actions to perform and what metadata to assign to each content item in the batch.



Note:

For the Batch Loader utility to function correctly with an Oracle WebLogic Server instance, you must have JDBC connection settings configured. For instructions, see [Running Administration Applications in Standalone Mode](#).

This section covers these topics:

- [About Batch Load File Records](#)
- [About Batch Load Actions](#)
- [About Batch Load Insert Action](#)
- [About Batch Load Delete Action](#)
- [About Batch Load Update Action](#)
- [About Optional Batch Load File Parameters](#)

- [About Custom Metadata Fields](#)

4.1.1 About Batch Load File Records

A batch load file is made up of *file records*, which are sets of name/value pairs that specify the action to perform, or the metadata for individual content items, or both.

Note:

Field names and parameters are case sensitive. They must appear in the batch load file exactly as they appear in the following sections. For example, `dDocName` is not the same as `ddocname`, `dDocname`, or `DDOCNAME`.

- Each file record ends with an `<<EOD>>` (end of data) marker.
- A pound sign (`#`) followed by a space at the beginning of a line indicates a comment. The comment character must be followed by a space. For example: `# primaryFile=test.txt` works properly, but `#primaryFile=test.txt` will cause errors.
- The following is an example of a file record:

```
# This is a comment
Action=insert
dDocName=Sample1
dDocType=Document
dDocTitle=Batch Load record insert example
dDocAuthor=sysadmin
dSecurityGroup=Public
primaryFile=links.doc
dInDate=8/15/2001
<<EOD>>
```

4.1.2 About Batch Load Actions

Valid actions for batch loading are *Insert*, *Delete*, and *Update*.

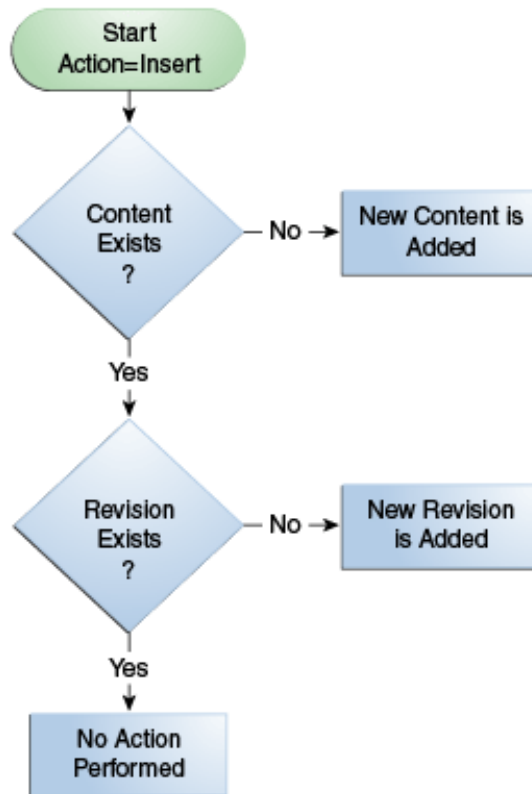
- If no action is specified for a file, the system tries to perform an update.
- Each file record can have only one action, but file records with different actions can be present in the same batch load file.
- The logic process for each action is different.

4.1.3 About Batch Load Insert Action

The *Insert* action checks a new file in to the Content Server repository. [Figure 4-1](#) illustrates the insert action.

- If the Content ID (`dDocName`) does not exist in the Content Server database, then a new file is created.
- If the Content ID (`dDocName`) exists in the Content Server database, and no revision (`dRevLabel`) is specified, then a new revision is created.
- If the Content ID (`dDocName`) and the specified revision (`dRevLabel`) exist in the Content Server database, then no action is performed.

Figure 4-1 The Insert Action Sequence for Checking In a New File



4.1.3.1 Insert Requirements

The following table defines the fields required for successful performance of an insert action.

 **Note:**

Batch loaded revisions will not enter a workflow even if they meet the criteria for an active workflow.

- Field Length: Maximum number of characters permitted in the field.
- Carried Over: If the next record does not contain this field, the value of this field will be taken from the previous record.

 **Important:**

If you have defined any custom metadata fields as required fields, those fields also need to be defined for an insert action.

Required Items	Field Length	Carried Over	Definition
Action=insert	N/A	Yes	The command to insert a file. The term Action is case sensitive and must be initial capitalized.
dDocName	30	No	The metadata field named Content ID.
dDocType	30	Yes	The metadata field named Type.
dDocTitle	80	No	The metadata field named Title.
dDocAuthor	30	Yes	The metadata field named Author.
dSecurityGroup	30	Yes	The metadata field named Security Group.
primaryFile	N/A	N/A	The metadata field named Primary File. The Primary File name can be a complete path or just the file name. If a file name only is specified, the location of the file is determined as follows: <ul style="list-style-type: none"> – If the <code>SetFileDir</code> optional parameter has been set in this file record or any previous file record, the directory specified in <code>SetFileDir</code> will be used. – If the <code>SetFileDir</code> parameter has not been set, the batch load file path is used. (The path is specified in the Batch Load File field on the Batch Loader window.) By default, the length of the Primary File name cannot exceed 80 characters (of which the extension can only be 8 characters maximum).
dInDate	N/A	No	The metadata field named Release Date. <ul style="list-style-type: none"> – The <code>dInDate</code> must use the date format of the locale of the user executing the Batch Loader. For example, the US English date format is <code>mm/dd/yy hh:mm:ss am/pm</code>. – Time information is optional. If you specify the time, only the <code>hh:mm</code> part is required. The <code>ss</code> and <code>am/pm</code> parts are optional.
<<EOD>>	N/A	N/A	Indicates the end of data for the file record.

4.1.3.2 Insert Example

The following code fragments show the batch load file syntax for inserting files. This example shows two file records.

The first file record includes all required fields and the action statement, `Action=insert`. The second file record does not list the required fields: `dDocType`, `dDocAuthor`, or `dSecurityGroup`. However, the information for these items is taken from the previous record. Also, the second record does not specify an action, so the insert action is carried over. Therefore, if the Content ID `HR003` does not exist, the file will be inserted. However, if the Content ID does exist, it will not be inserted because the action is insert and not update.

- First record:

```
Action=insert
dDocName=HR001
dDocType=Form
dDocTitle=New Employee Information Form
dDocAuthor=Olson
dSecurityGroup=Public
```

```
primaryFile=hr001.doc  
dIndate=3/15/97  
<<EOD>>
```

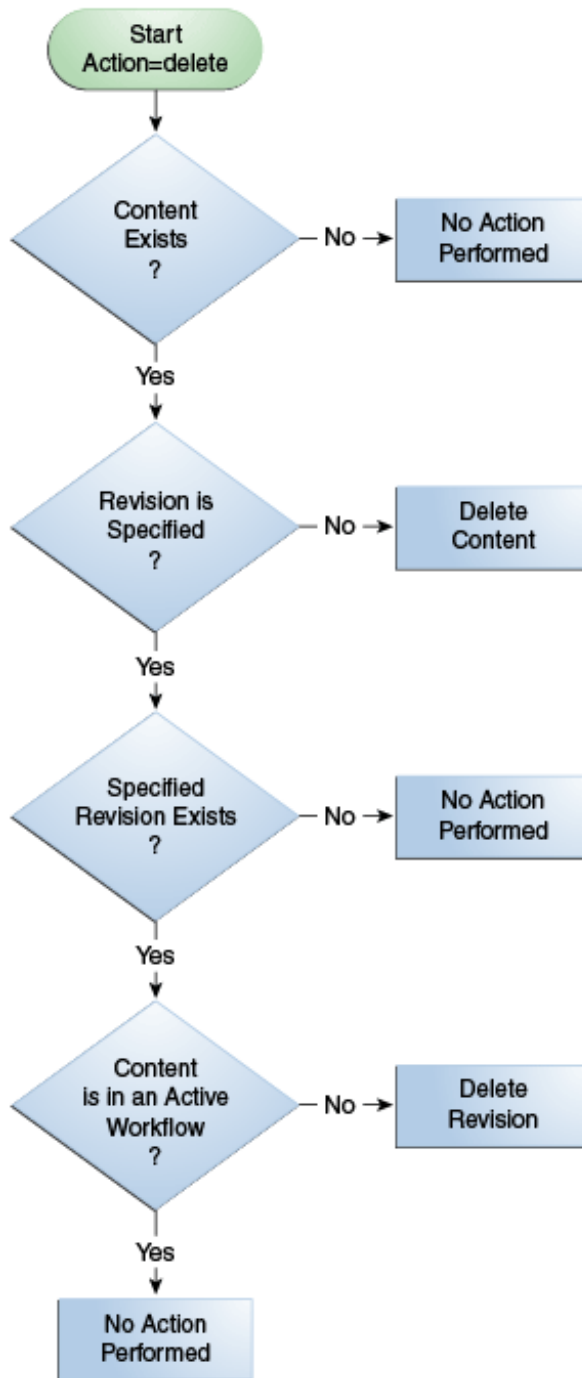
- **Second record:**

```
dDocName=HR003  
dDocTitle=Performance Review  
primaryFile=hr003.doc  
dIndate=3/15/97  
<<EOD>>
```

4.1.4 About Batch Load Delete Action

The *delete* action deletes one or all revisions of an existing file from the Content Server repository. If the specified Content ID (dDocName) does not exist in the Content Server database, no action is performed. [Figure 4-2](#) illustrates the delete action.

Figure 4-2 The Delete Action Sequence



4.1.4.1 Delete Requirements

The following table defines the fields required for successful performance of a delete action.

Required Items	Definition
Action=delete	The command to delete a file. The term Action is case sensitive and must be initial capitalized.

Required Items	Definition
dDocName	The metadata field named Content ID.
<<EOD>>	Indicates the end of data for the file record.

4.1.4.2 Delete Example

The following example shows the batch load file syntax for deleting files. This example shows two file records. The first file record will delete all revisions of the Content ID HR001. The second file record will delete revision 2 of the content item HR002.

```
Action=delete
dDocName=HR001
<<EOD>>
Action=delete
dDocName=HR002
dRevLabel=2
<<EOD>>
```

4.1.5 About Batch Load Update Action

The *update* action updates existing content items. One of the following actions occurs, depending on what items are present in the file record and what content exists in the system:

- A new revision of an existing content item is created.
- An existing file's metadata is updated.
- A new content item is inserted (*Action=insert* is performed).

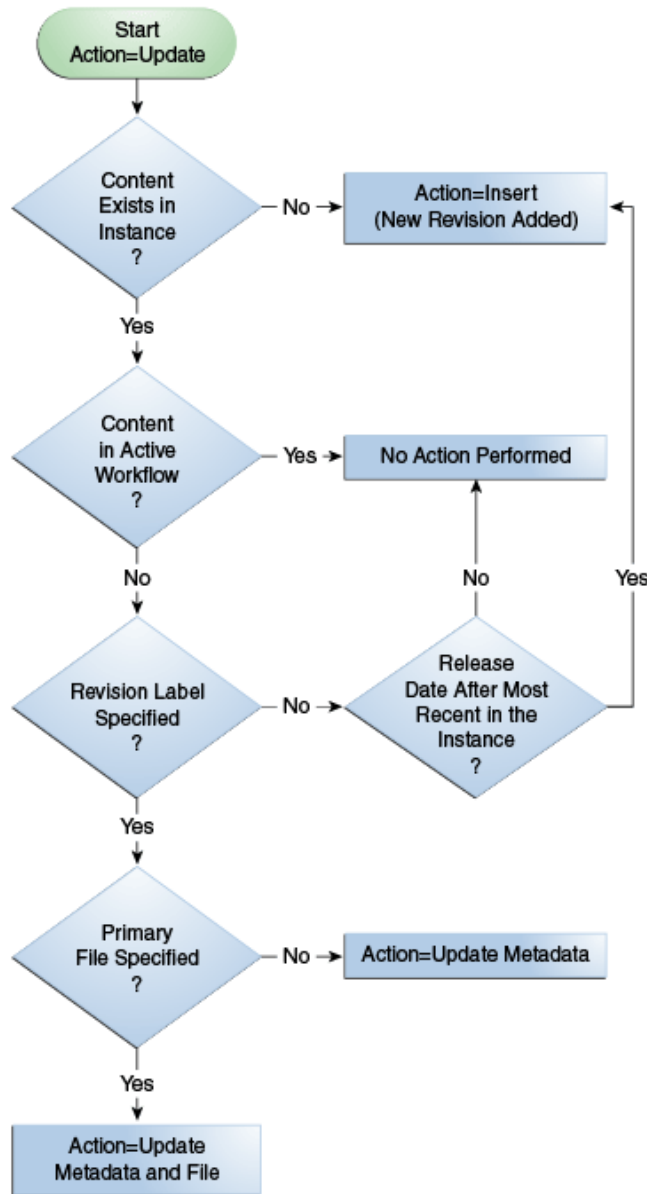
Note:

Batch loaded revisions will not enter a workflow even if they meet the criteria for an active workflow.

A new revision is created when one of the following scenarios occur:

Scenario	Content ID (dDocName)	Revision (dRevLabel)	Release Date in Batch Load file (dInDate)
Scenario 1	Exists in Content Server instance	Not specified in the batch load file.	After the release date of the latest revision of the file in the system.
Scenario 2	Exists in Content Server instance	Specified in the batch load file, but does not exist in Content Server instance.	After the release date of the latest revision of the file in the system.

Figure 4-3 The Update Action Sequence



4.1.5.1 Update Requirements

The following table defines the fields required for successful performance of an update action.

Required Items	Field Length	Carried Over	Definition
Action=update	N/A	Yes	The command to update a file. The term <i>Action</i> is case sensitive and must be initial capitalized.
dDocName	30	No	The metadata field named Content ID.
dDocType	30	Yes	The metadata field named Type.

Required Items	Field Length	Carried Over	Definition
dDocTitle	80	No	The metadata field named Title.
dDocAuthor	30	Yes	The metadata field named Author.
dSecurityGroup	30	Yes	The metadata field named Security Group.
primaryFile	N/A	N/A	<p>The metadata field named Primary File.</p> <p>If only the metadata is being updated, the primaryFile field is not required but dRevLabel is required.</p> <p>If the optional dRevLabel field is specified and matches a revision label that exists in the Content Server instance, the primaryFile field is not required; the primary file specified for that revision is used.</p> <p>It is important to note that although dRevLabel is not a required field, if the primaryFile is not present, then dRevLabel becomes a required field.</p> <p>The Primary File name can be a complete path or just the file name. If a file name only is specified, the location of the file is determined as follows:</p> <ul style="list-style-type: none"> • If the <code>SetFileDir</code> optional parameter has been set in this file record or any previous file record, the directory specified in <code>SetFileDir</code> will be used. • If the <code>SetFileDir</code> parameter has not been set, the batch load file path is used. (The path is specified in the Batch Load File field on the Batch Loader window.)
dInDate	N/A	No	<p>The metadata field named Release Date.</p> <ul style="list-style-type: none"> • The <code>dInDate</code> must use the date format of the locale of the user executing the Batch Loader. For example, the US English date format is <code>mm/dd/yy hh:mm:ss am/pm</code>. • Time information is optional. If you specify the time, only the <code>hh:mm</code> part is required. The <code>ss</code> and <code>am/pm</code> parts are optional.
<<EOD>>	N/A	N/A	Indicates the end of data for the file record.

4.1.5.2 Update Example 1

This example assumes that two files are already checked in to the system with the following metadata:

- HR001 has a Release Date of 9/26/98 and Revision of 1
- HR002 has a Release Date of 3/15/99 and Revision of 2

The first file record, Content ID HR001, exists in the system, but it does not have a Revision (dRevLabel) specified in the batch load file. Therefore, the Batch Loader will compare the Release Date of the latest revision in the system with the Release Date specified in the batch load file. Since 2/20/99 is after 9/26/98, a new revision 2 for HR001 is added.

The second file record, Content ID HR002, exists in the system and has a Revision (dRevLabel) specified, but Revision 3 does not exist in the system. Therefore, a new revision 3 for HR002 is added.

```
Action=update
dDocName=HR001
dDocType=Form
dDocTitle=New Employee Form
```

```
dDocAuthor=Olson
dSecurityGroup=Public
primaryFile=hr001.doc
DInDate=2/20/99
<<EOD>>
dDocName=HR002
dDocTitle=Payroll Change Form
primaryFile=hr002.doc
DInDate=2/20/99
dRevLabel=3
<<EOD>>
```

4.1.5.3 Update Example 2

This example assumes that one file is already checked in to the system with the following metadata:

- Content ID = HR003
- Release Date = 3/15/97
- Revision = 1
- Title = Performance Review
- Author = Smith

Because Revision 1 of the Content ID HR003 exists in the system (and is not in an active workflow), the revision will be updated with the new Title, Author, and Release Date metadata.

```
Action=update
dDocName=HR003
dDocType=Form
dDocTitle=Performance Review Template
dDocAuthor=Smith
primaryFile=hr003.doc
dInDate=2/20/99
dRevLabel=1
<<EOD>>
```

4.1.6 About Optional Batch Load File Parameters

The following table lists the optional parameters you can use in any file record in a batch load file.

In a batch load file, there are two methods you can use to override the primary and alternate formats assigned to a content item check-in:

- Specifying a value for the `primaryFile:format` parameter, or specifying a value for the `alternateFile:format` parameter, both. However, it is possible to override these values by using the `primaryOverrideFormat` or `alternateOverrideFormat` parameters. It is also possible that certain components will force specific formats on certain types of check-ins or certain application functionality may exist in some components that forces a different format.
- Specifying a value for the `primaryOverrideFormat` parameter, or specifying a value for the `alternateOverrideFormat` parameter, or both. However, these will only work as parameters in the batch load file if you enable the `IsOverrideFormat` configuration variable. Note that using this method will override any values that you set for the `primaryFile:format` and `alternateFile:format` parameters.

Optional Parameters	Definition
dRevLabel	The metadata field named Revision. Maximum field length is 10 characters. Values must be an integer or comply with the Major/Minor Revision Label Sequence established by the System Properties settings.
dDocAccount	The metadata field named Accounts. Maximum field length is 30 characters. This field is not carried over to the next file record. Do not specify this field if accounts are not enabled. If accounts are enabled and this field is not specified, dDocAccount will be set to an empty value.
xComments	The metadata field named Comments. Maximum field length is 255 characters.
dOutDate	The metadata field named Expiration Date. The dOutDate must use the date format of the locale of the user executing the Batch Loader. For example, the English-US date format is mm/dd/yy hh:mm:ss am/pm. Time information is optional. If you specify the time, only the hh:mm part is required. The ss and am/pm parts are optional.
primaryFile:path	Specifies the location of the file. If a primaryFile:path value is specified, the value overrides the value specified for the primaryFile parameter. However, the primaryFile:path value is not used to determine the file conversion format. If a value for primaryFile:path is not specified, the location is determined from the primaryFile value. This parameter uses the following syntax: <code>primaryFile:path=complete_path/primary_file_name</code>
primaryFile:format	Specifies the file format to use for the Primary File. This file format overrides the one specified by the file extension of the file and the value specified for the primaryFile parameter. If a primaryFile:format value is not specified, the file format is determined from the file extension for the primaryFile value. This parameter uses the following syntax: <code>primaryFile:format=application/conversion_type</code>
alternateFile	The metadata field named Alternate File. The Alternate File name can be a complete path or just the file name. If a file name only is specified, the location of the file is determined as follows: If the SetFileDir optional parameter has been set in this file record or any previous file record, the directory specified in SetFileDir will be used. If the SetFileDir parameter has not been set, the batch load file path is used. (The path is specified in the Batch Load File field on the Batch Loader window.)

Optional Parameters	Definition
alternateFile:path	<p>Specifies the location of the alternate file. If an <code>alternateFile:path</code> value is specified, the value overrides the value specified for the <code>alternateFile</code> parameter. However, the <code>alternateFile:path</code> value is not used to determine the file conversion format. If an <code>alternateFile:path</code> value is not specified, the location is determined from the <code>alternateFile</code> parameter, if a value is specified. Otherwise, by default, the <code>primaryFile</code> value is used for the computation.</p> <p>This parameter uses the following syntax: <code>alternateFile:path=complete_path</code></p>
alternateFile:format	<p>Specifies the file format to use for the Alternate File. This file format overrides the one specified by the file extension of the file and the value specified for the <code>alternateFile</code> parameter. If an <code>alternateFile:format</code> value is not specified, the file format is determined from the file extension for the <code>alternateFile</code> parameter, if a value is specified. Otherwise, by default, the <code>primaryFile</code> value is used for the computation.</p> <p>This parameter uses the following syntax: <code>alternateFile:format=application/conversion_type</code></p>
webViewableFile	<p>The <code>webViewableFile</code> name can be a complete path or just the file name. If a <code>webViewableFile</code> value is specified, then the conversion process is not performed. If a file name only is specified, the location of the file is determined as follows:</p> <p>If the <code>SetFileDir</code> optional parameter has been set in this file record or any previous file record, the directory specified in <code>SetFileDir</code> will be used.</p> <p>If the <code>SetFileDir</code> parameter has not been set, the batch load file path is used. (The path is specified in the Batch Load File field on the Batch Loader window.)</p>
webViewableFile:path	<p>Specifies the location of the web viewable file. If a <code>webViewableFile.path</code> value is specified, the value overrides the value specified for the <code>webViewableFile</code> parameter. However, the <code>webViewableFile:path</code> value is not used to determine the file conversion format. If a value for <code>webViewableFile:path</code> is not specified, the location is determined from the <code>webViewableFile</code> value.</p> <p>This parameter uses the following syntax: <code>webViewableFile:path=complete_path</code></p>
webViewableFile:format	<p>Specifies the file format to use for the web viewable file. This file format overrides the one specified by the file extension of the file and the value specified for the <code>webViewableFile</code> parameter. The <code>webViewableFile:format</code> value should be explicitly specified, it is not determined from the <code>webViewableFile</code> value.</p> <p>This parameter uses the following syntax: <code>alternateFile:format=application/conversion_type</code></p>
primaryOverrideFormat	<p>Specifies which file format to use for the Primary File. This file format overrides the one specified by the file extension of the file. This option will only work as a parameter if you enable the <code>IsOverrideFormat</code> configuration variable. You can set this variable by selecting Allow Override Format in the System Properties utility. However, a better (and recommended) alternative would be to use the <code>primaryFile:format</code> parameter.</p>

Optional Parameters	Definition
<code>alternateOverrideFormat</code>	Specifies which file format to use for the Alternate File. This file format overrides the one specified by the file extension of the file. This option will only work as a parameter if you enable the <code>IsOverrideFormat</code> configuration variable. You can set this variable by selecting Allow Override Format in the System Properties utility. However, a better (and recommended) alternative would be to use the <code>alternateFile:format</code> parameter.
<code>SetFileDir</code>	Specifies the directory where the Primary Files and Alternate Files are located. This field is carried over to the next file record.

4.1.7 About Custom Metadata Fields

Any custom metadata field that has been defined in the Configuration Manager can be included in a file record.

- If you have defined any custom metadata fields as required fields, those fields must be defined for an insert action or an update action.
- If a custom metadata field is not a required field, but it has a default value (even if blank), then the default value will be used if the value is not specified in the batch load file.
- When specifying a custom metadata field value, the field name preceded with an **x**. For example, if you have a custom metadata field called `Location`, then the batch load file entry will be `xLocation=value`.
- Keep in mind that some add-on products use custom metadata fields. For example, if you have PDF Watermark, you will have created a field called `Watermark`. To include this field in a batch load file, precede it with an **x** just like any other custom metadata field (for example, `xWatermark`).

4.2 Preparing a Batch Load File

This section covers these topics:

- [About Preparing a Batch Load File](#)
- [Mapping Files](#)
- [Creating a Batch Load File from the BatchBuilder Window](#)
- [Creating a Mapping File](#)
- [Creating a Batch Load File from the Command Line](#)

4.2.1 About Preparing a Batch Load File

You can use any method you prefer to create a batch load file, if the resulting text file conforms to the batch load file syntax requirements. However, the Batch Loader provides a tool called the BatchBuilder to assist you in creating batch load files.

- The BatchBuilder creates a batch load file based on the files in a specified directory. The BatchBuilder reads recursively through all the sub-directories to create the batch load file.
- A mapping file tells the BatchBuilder how to determine the metadata for each file record. You can use the BatchBuilder to create and save custom [Mapping Files](#).
- You can run the BatchBuilder from the standalone utility interface or from the command line.

- The BatchBuilder can also be used to create *external collections* of content, which are indexed and stored in a separate search collection rather than in the Content Server database. You can set up read-only external collections, where users can search for content but cannot update metadata or delete content. This option is recommended when external content is also included in another Content Server instance.

If you plan to use the Batch Loader utility to update and insert a large number of files on your Content Server instance simultaneously, you must create a batch load file. Two of the optional parameters that you can include in your batch load file are `primaryOverrideFormat` and `alternateOverrideFormat`. However, these options only work as parameters in the batch load file if you enable the `IsOverrideFormat` configuration variable. You can set this variable using the System Properties utility.

4.2.2 Mapping Files

Mapping files are text files that have an `.hda` extension, which identifies them as a type of data file used by the Content Server instance.

For more information on HDA files, LocalData properties, and ResultSets, see Elements in HDA Files in *Developing with Oracle WebCenter Content*.

4.2.2.1 Mapping File Formats

The metadata mapping can be defined in one of two formats:

- As name/value pairs in a LocalData definition, a mapping file would look like the following:

```
@Properties LocalData
dDocName=<${filename$}>.<${extension$}>
dInDate=<${filetimestamp$}>
@end
```

- As a BatchBuilderMapping ResultSet, a mapping file would look like the following:

```
@ResultSet SpiderMapping
2
mapField
mapValue
dDocName
<${filename$}>.<${extension$}>
dInDate
<${filetimestamp$}>
@end
```

4.2.2.2 Mapping File Values

The following values can be used in a mapping file:

Value	Description	Example
Normal string	All files will have the specified metadata value.	<code>dDocType=Document</code> All files will be the Document content type.
Idoc script	Any supported Idoc script. See Introduction to the Idoc Script Custom Scripting Language in <i>Developing with Oracle WebCenter Content</i>	<code>xLanguage=<\${if strEquals(dir2, "EN")} \$>English<\${elseif strEquals(dir2, "SP")} \$>Spanish<\${else\$}>French<\${endif\$}></code>

Value	Description	Example
<\$dir1\$>, <\$dir2\$>	The directory name at the specified level in the file's path. <\$dir1\$> refers to the root directory specified in the "Directory" field, <\$dir2\$> refers to the next level directory, and so on.	<p>dDocType=<\$dir1\$> dSecurityGroup=<\$dir2\$> dDocAccount=<\$dir3\$></p> <p>If the file path is f:/docs/public/sales/march.doc and you have specified the Directory value as f:/docs, the values would be:</p> <p><\$dir1\$> = "docs" <\$dir2\$> = "public" <\$dir3\$> = "sales"</p>
<\$dUser\$>	The user currently logged in.	<p>dDocAuthor=<\$dUser\$></p> <p>If administrator is logged in, then <\$dUser\$> would equal administrator.</p>
<\$extension\$>	The file extension of the file.	<p>dDocTitle=<\$filename\$>.<\$extension\$></p> <p>If the file path is d:/salesdocs/sample.doc, then <\$extension\$> would equal doc.</p>
<\$filename\$>	The name of the file.	<p>dDocName=<\$filename\$></p> <p>If the file path is d:/salesdocs/sample.doc, then <\$filename\$> would equal sample.</p>
<\$filepath\$>	The entire directory path of the file, including the file name.	<p>xPath=<\$filepath\$></p> <p>If the file path is c:/docs/public/acct/sample.doc, then <\$filepath\$> is c:/docs/public/acct/sample.doc.</p>
<\$filesize\$>	The size of the file (in bytes).	<p>xFileSize=<\$filesize\$></p> <p>For a 42KB file, <\$filesize\$> would be 43008.</p>
<\$filetimestamp\$>	The date and time the file was last modified.	<p>dInDate=<\$filetimestamp\$></p> <p>If the last modified date is September 13, 2001 at 4:03 pm, then <\$filetimestamp\$> would equal 9/13/01 4:03 PM for an English-US locale.</p>
<\$URL\$>	The URL of the file, based on the values of the physical file root and relative web root.	

4.2.3 Creating a Batch Load File from the BatchBuilder Window

To create a batch load file from the BatchBuilder window:

1. Start the Batch Loader utility:
 - Windows: Choose **Start**, then **Programs**, then **Content Server**, then *instance_name*, then **Utilities**, then **BatchLoader**.
 - UNIX: Go to the *DomainHome/ucm/cs/bin/* directory, type `./BatchLoader` in a shell window, and press the RETURN key on your keyboard.
2. In the login window, enter the Content Server administrator user name and password, then click **OK**.
3. In the Batch Loader window, choose **Options**, then **Build Batch File**.
4. In the **Directory** field on the BatchBuilder window, enter the location of the files to be included in the batch load file.
5. In the **Batch Load File** field, enter the path and file name for the batch load file. You can click the Browse button to navigate to and select the directory and file.
6. From the Mapping list, select a mapping file. To create a new mapping file or edit an existing one, see [Creating a Mapping File](#).
7. Optional: In the **File Filter** field, enter filter settings to include or exclude particular files from the batch load file.
8. Optional: To batch load a read-only external collection, choose **External**, and select the external collection options.
9. Click **Build**.
10. When the build process is complete, click **OK**.
11. Open the batch load file in a text editor and double-check the file records.
12. To save the current batch load file settings as the default, choose **Options**, then **Save Configuration**.

4.2.4 Creating a Mapping File

To create a mapping file.

1. Open the BatchBuilder window.
2. Click **Edit** next to the **Mapping** field.
3. In the BatchBuilder Mapping List window, click **Add**.
4. In the Add BatchBuilder Mapping window, enter a name and description for the mapping file, and click **OK**.
5. In the Edit BatchBuilder Mapping window, click **Add**.
6. In the Add/Edit BatchBuilder Mapping Field window, enter a metadata field name to be defined. For example, enter `dDocName` for the **Content ID** field, or `xComments` for the **Comments** field.
7. Enter the value for the metadata field.
 - Type any constant text and Idoc script directly in the **Value** field. For example, to set Document as the Type for all documents in the batch load file, enter **dDocType** in the

Field field, and enter **Document** in the **Value** field. See Introduction to the Idoc Script Custom Scripting Language in *Developing with Oracle WebCenter Content*.

- To add a predefined variable to the **Value** field, select the variable in the right column and click the << button. For example, to set each document's second-level directory as the Security Group, enter `dSecurityGroup` in the **Field** field, and insert the `<${dir1$}` variable in the **Value** field.

 **Note:**

Be careful when choosing predefined variables. Many metadata fields have length limitations and cannot contain certain characters (such as spaces or punctuation marks). See Managing Content in *Managing Oracle WebCenter Content*.

8. Click **OK**.
9. Repeat steps 4 through 8 for as many metadata fields as you want to define.
10. Click **OK** to save changes and close the Edit BatchBuilder Mapping window.

The mapping file is saved as `MapFileName.hda` in the `IntradocDir/search/external/mapping/` directory.

11. Click **Close** to close the BatchBuilder Mapping List window.

4.2.5 Creating a Batch Load File from the Command Line

You can create a batch load file by entering the BatchBuilder parameters from a command line rather than entering them in the BatchBuilder window. To create a batch load file from the command line:

1. Open the `DomainHome/ucm/cs/bin/intradoc.cfg` file in a text editor, and add the following line, where `sysadmin` is the user name of the Content Server system administrator:

```
BatchLoaderUserName=sysadmin
```

This is required so that the system logs in as the system administrator, because only users who have admin rights have permission to run the Batch Loader and BatchBuilder utilities.

2. Save and close the file.
3. Open a command line window and change to the `DomainHome/ucm/cs/bin/` directory.

 **Caution:**

Run the BatchBuilder using the same operating system account that runs the Content Server instance. Otherwise, the software might not process your data due to permissions problems.

4. Enter the following command:

- Windows:

```
BatchLoader.exe -spider -q -ddirectory -mmappingfile -nbatchloadfile
```

- UNIX:

```
BatchLoader -spider -q -ddirectory -mmappingfile -nbatchloadfile
```

The following flags can be used with the BatchLoader command to run the BatchBuilder from the command line:

Flag	Required?	Description
-spider or /spider	Yes	Runs the BatchBuilder utility.
-q or /q	No	Runs the BatchBuilder in quiet mode in the background. (If the BatchBuilder is run from the command line without this flag, the BatchBuilder window will appear.)
-d or /d	Yes	Directory field value.
-m or /m	Yes	Mapping field value.
-n or /n	Yes	Batch Load File field value.
-e or /e	No	Exclude specified files (Exclude check box selected).
-i or /i	No	Include specified files (Exclude check box deselected).

4.2.5.1 Windows Example

The following example shows the correct syntax to run the BatchBuilder from a Windows command line, where:

- Directory = c:/myfiles
- Mapping File = MyMappingFile
- Batch Load File = c:/batching/batchinsert.txt
- Excluded files = *.exe and *.zip

```
BatchLoader.exe -spider -q -dc:/myfiles -mMyMappingFile -nc:/batching/batchinsert.txt -eexe,zip
```

4.2.5.2 UNIX Example

The following example shows the correct syntax to run the BatchBuilder from a UNIX command line, where:

- Directory = /myfiles
- Mapping File = MyMappingFile
- Batch Load File = /batching/batchinsert.txt
- Excluded files = index.htm and index.html

```
BatchLoader -spider -q -d/myfiles -mMyMappingFile -n/batching/batchinsert.txt -eindex.htm,index.html
```

4.3 Running the Batch Loader

This section covers these topics:

- [About Running the Batch Loader](#)
- [Batch Loading from the Batch Loader Window](#)
- [Batch Loading from the Command Line](#)

- [Using the IdcCommand Utility and Remote Access](#)
- [Batch Loading Content as Metadata Only](#)
- [Batch Loader -console Command Line Switch](#)
- [Adding a Redirect](#)
- [Correcting Batch Load Errors](#)

4.3.1 About Running the Batch Loader

The Batch Loader uses the information from a batch load file to check in (insert), delete, or update a large number of files on your Content Server instance simultaneously.

- You can run the Batch Loader from the standalone utility interface or from the command line.
- After you run the Batch Loader, the Content Server instance processes files through the Inbound Refinery instance and the Indexer as it would for any other content item.

4.3.2 Batch Loading from the Batch Loader Window

To batch load content using the Batch Loader window:

1. Open the Batch Loader window.
2. Click **Browse**, navigate to and select the batch load file.
3. To change the number of errors that can occur before the Batch Loader stops processing, enter the number in the **Maximum errors allowed** field.
4. To delete files from the hard drive after they are successfully checked in or updated, select **Clean up files after successful check in**.
5. To create a text file containing the file records that failed during batch loading, select **Enable error file for failed revision classes**.
6. Click **Load Batch File** to start the Batch Loader process.

When the batch load process is complete, a Batch Loader message window opens, indicating the number of errors that occurred, if any.

7. If you enabled the error file, write down the file name shown in the message box.
8. Click **OK**.
9. Correct any problems with the batch load.
10. To save the current Batch Loader settings as the default, choose **Options**, then **Save Configuration**.

4.3.3 Batch Loading from the Command Line

You can batch load content by entering the Batch Loader parameters from a command line rather than entering them in the Batch Loader window. To run the Batch Loader from the command line:

1. Open the `DomainHome/ucm/cs/bin/intradoc.cfg` file in a text editor, and add the following line, where `sysadmin` is the user name of the Content Server system administrator:

```
BatchLoaderUserName=sysadmin
```

This is required so that the system logs in as the system administrator, because only users who have admin rights have permission to run the Batch Loader utility.

2. Save and close the file.
3. Open a command line window and go to the `DomainHome/ucm/cs/bin/` directory.

 **Note:**

Run the Batch Loader using the same operating system account that runs the Content Server instance. Otherwise, the software might not process your files due to permissions problems.

4. Enter the following command:

- Windows:

```
BatchLoader.exe -q -nbatchloadfile
```

- UNIX:

```
BatchLoader -q -nbatchloadfile
```

The Batch Loader processes the batch load file, but message boxes will not be shown.

5. Correct any problems with the batch load.

The following flags can be used with the BatchLoader command from the command line:

Flag	Required?	Description
-q or /q	No	Runs the Batch Loader in quiet mode in the background. (If the Batch Loader is run from the command line without this flag, the Batch Loader window will appear.)
-n or /n	Yes	Batch Load File field value.
-console	No	Echoes all output to the HTML Content Server log and to the console window that is running the Batch Loader. For details, see Batch Loader - console Command Line Switch .

4.3.3.1 Windows Example

The following example shows the correct syntax to run the Batch Loader from a Windows command line, where the batch load file is `c:/batching/batchinsert.txt`:

```
BatchLoader.exe -q -nc:/batching/batchinsert.txt
```

4.3.3.2 UNIX Example

The following example shows the correct syntax to run the Batch Loader from a UNIX command line, where the batch load file is `/batching/batchinsert.txt`:

```
BatchLoader -q -n/batching/batchinsert.txt
```

4.3.4 Using the IdcCommand Utility and Remote Access

Occasionally, you may need to use remote access when managing your Content Server instance. This does not necessarily mean that remote terminal access is required. However, you must have the ability to submit commands to the server from a remote location.

Combining remote access with the IdcCommand utility provides a powerful toolset and an easy way to check in a large number of files to your instance. To take advantage of this functionality, you will need to properly set up the workstation to submit commands and be able to use the IdcCommand utility with a batch load command file.

This section covers the following topics:

- [Batch Load Command Files](#)
- [Preparing for Remote Batch Loading](#)

4.3.4.1 Batch Load Command Files

A batch load command file contains a set of commands for each file that is loaded. If you are loading a large number of files, the command file may contain hundreds of lines. Using an editing tool can simplify the task of creating the numerous required lines. For example, the procedure for [Preparing for Remote Batch Loading](#) shows how you can prepare a batch load command file using the editing and mail merge features of Microsoft Office.

The following is an example Batch Load command file:

```
@Properties LocalData
IdcService=CHECKIN_UNIVERSAL
doFileCopy=1
dDocTitle=thisfile
dDocType=Native
dSecurityGroup=Internal
dDocAuthor=sysadmin
primaryFile=filename
primaryFile:Path=pathtothefile/primaryfilename
xComments=Initial Check In
@end
<<EOD>>@Properties LocalData
IdcService=CHECKIN_UNIVERSAL
doFileCopy=1
dDocTitle=99.tif
dDocType=Native
dSecurityGroup=Internal
dDocAuthor=sysadmin

primaryFile=350.afp
primaryFile:path=/lofs/invoices/350.afp
xComments=Initial Check In
@end
<<EOD>>
```

4.3.4.2 Preparing for Remote Batch Loading

You can perform batch loading from remote locations. The following procedure is written for a Microsoft Windows operating system and contains these main stages:

- Configure the local computer
- Test the configuration for the remote workstation
- Create a batch load command file
- Execute the upload

4.3.4.2.1 Configuring the Local Computer

To configure the local computer:

1. Open Windows Explorer.
2. Create a working directory (for example, `C:\working_dir`).
3. In the working directory, create one or more directories for the Content Server instances you will be accessing (for example, `C:\working_dir\development` and `C:\working_dir\contribution`). These directories can be referred to as *DomainHomeName*.
4. In each *DomainHomeName* directory, create a `cmdfiles` subdirectory.
5. From the remote Content Server instance, copy the following directories from `MW_HOME\user_projects\domains\Domain_Name\ucm\cs` in to their respective *DomainHomeName* (in this case `C:\working_dir\development` and `C:\working_dir\contribution`).
 - `working_dir\DomainHomeName\ucm\cs\bin`
 - `working_dir\DomainHomeName\ucm\cs\config`
6. From the remote Content Server instance, copy the following directories (and their files) to your working directory:
 - `working_dir\idc\bin`
 - `working_dir\idc\components`
(copying the `CSDms` and `NativeOsUtils` component files should be sufficient)
 - `working_dir\idc\config`
 - `working_dir\idc\jlib`
 - `working_dir\idc\resources\core\lang`
 - `working_dir\idc\resources\core\table`
 - `working_dir\idc\resources\core\config`
7. Using a text editor, open the `DomainHomeName\ucm\cs\bin\intradoc.cfg` file on your local system and update the `IntradocDir` configuration variable to match your directory structure. For example:

```
IntradocDir=working_dir\DomainHomeName\ucm\cs,  
IdcHomeDir=working_dir\idc  
WeblayoutDir=working_dir\DomainHomeName\ucm\cs\weblayout
```
8. Using a text editor, open the `working_dir\DomainHomeName\ucm\cs\config\config.cfg` file on your local system and verify the following settings are correct.

```
IntradocServerPort=4444  
IntradocServerHostName=HostMachineName
```
9. In the remote Content Server instance, add the IP address of the local computer to the Security Filter, using the Systems Properties utility.
10. Restart the remote Content Server instance.

4.3.4.2.2 Testing the Configuration for the Remote Workstation

To test the configuration for the remote workstation:

1. In the `cmdfiles` directory, create a file named `pingservertest.hda` and add the following lines:

```
@Properties LocalData  
IdcService=PING_SERVER  
@end
```

2. Open a command prompt and change to your working `bin` directory (for example, `cd C:\working_dir\development\bin`)

3. Issue the following command:

```
IdcCommand -f ..\cmdfiles\pingservertest.hda -u sysadmin -l ..\pingservertest.log -c server
```

4. Confirm the output. If you are successful, you will get the following message from the server.

```
3/24/04: Success executing service PING_SERVER.  
You have completed your setup for remote commands.
```

4.3.4.2.3 Creating a Batch Load Command File

This procedure uses the editing and mailmerge features of Microsoft Office to create a batch load command file. To create a batch load command file:

1. Create a file listing of your directory contents:
 - a. Open a command prompt and change to the root directory representing the files you intend to load.
 - b. Create a file listing, using the following command to redirect the output in to a file:

```
dir /s /b > filelisting.txt
```

- c. Check your `filelisting.txt` file; it will look something like this:

```
V:\policies\ADMIN\working_dir_Admin\AbbreviationList.doc  
V:\policies\ADMIN\working_dir_Admin\Abbreviations.doc  
V:\policies\ADMIN\working_dir_Admin\AbsencePres.doc  
V:\policies\ADMIN\working_dir_Admin\AdmPatientCare.doc  
V:\policies\ADMIN\working_dir_Admin\AdmRounds.doc  
V:\policies\ADMIN\working_dir_Admin\AdverseEvents.doc  
V:\policies\ADMIN\working_dir_Admin\ArchivesPermanent.doc  
V:\policies\ADMIN\working_dir_Admin\ArchivesRetrieval.doc  
V:\policies\ADMIN\working_dir_Admin\ArchivesStandardReq.doc
```

Note:

When working with batch loads, it is important to note that the file must exist on the server indicated by the `primaryFile` statement in the batch load command file. Optimally, you should use the same letter to map the directory of files to the server and to your local system. Alternatively, you can copy the directory of files to the server temporarily.

2. Edit the file listing to create your file name and title data:
 - a. Open your `filelisting.txt` file in Excel.
 - b. Using **Replace**, remove all the directory information leaving only the file name. Also look for and remove the line for `filelisting.txt`.
 - c. Copy column A (containing the file names) to column B. In this example the file name is also used for the title and Column B will become the title.
 - d. Using **Replace**, remove the file extension from the names in column B.
 - e. Insert a new first line and enter *filename* in the first column and *title* in the second.
 - f. Save the file.

3. Create an .hda file from the file listing using Mail Merge features:
 - a. Open the Word application and create a new document with your set of batch load commands. The following example shows basic batch load commands. You must match your configuration settings when you create your batch load commands.

```
@Properties LocalData
IdcService=CHECKIN_UNIVERSAL
doFileCopy=1
dDocTitle=
dDocType=Native
dSecurityGroup=Internal
dDocAccount=Policy/Admin
dDocAuthor=sysadmin
primaryFile=d:/temp/working_dir_Admin/
xComments=Initial Check In
@end
<<EOD>>
```

- b. Select **Tools / Letters and Mailing / Mail Merge Wizard** and advance through the wizard. Choose the selections below to use your `filelisting.txt` file as input to the mail merge.
 - Letter Document (step 1)
 - Current document (step 2)
 - Existing List (step 3) and select your Excel spreadsheet as the data source
 - More Items (step 4), place the title and filename fields in to the word document so that it looks like the following:

```
@Properties LocalData
IdcService=CHECKIN_UNIVERSAL
doFileCopy=1
dDocTitle="title"
dDocType=Native
dSecurityGroup=Internal
dDocAccount=Policy/Admin
dDocAuthor=sysadmin
primaryFile=d:/temp/working_dir_Admin/"filename"
xHistory=Initial Check In
@end
<<EOD>>
```

- c. Complete the mail merge (Steps 5 and 6) and you will have a new Word document with one merge record per page.
- d. Edit the letters, selecting all, and use the Replace feature to remove all of the section breaks.
- e. Save the file as a plain text file to the `/cmdfiles` directory with the file extension of `hda` (for example, `filelisting.hda`)

4.3.4.2.4 Executing the Batch Load Upload

To execute the upload:

1. Open a command prompt.
2. Navigate to the working `bin` directory.
3. Issue the command:

```
IdcCommand -f ../cmdfiles/filelisting.hda -u sysadmin -l ../filelisting.log -c server
```

Your files will be checked in to the Content Server repository and a message appears in the command window as each file is checked in.

4.3.5 Batch Loading Content as Metadata Only

Depending on the action you plan to perform using the Batch Loader, certain fields are required in the batch load file. If you are updating only the metadata in existing content items, the **primaryFile** field is not required in the batch load file; for more information see [Update Requirements](#).

However, if you want to load (insert action) content in to the Content Server instance as metadata only, then the **primaryFile** field is required in the batch load file. Although the field is ignored by the import, the Batch Loader expects it to be defined. If the **primaryFile** field is missing, you will get an error as follows (or similar):

```
Please check record number <number>. BatchLoader: unable to check in '<record>' because the required field 'primaryFile' is missing.
```

To batch load content as metadata only:

1. Open the Content Server instance `config.cfg` file:

```
IntradocDir/config/config.cfg
```

2. Add the following configuration variables:

```
createPrimaryMetaFile=true  
AllowPrimaryMetaFile=true
```

3. Save and close the `config.cfg` file.
4. In the batch load file, add the following fields for each record:

```
primaryFile=  
createPrimaryMetaFile=true
```

Note that leaving the **primaryFile** field blank is acceptable. The field is ignored but must be included.

5. Continue to batch load your content using the Batch Loader procedure or the command line procedure. For more information, see [Batch Loading from the Batch Loader Window](#) or [Batch Loading from the Command Line](#).

4.3.6 Batch Loader -console Command Line Switch

Adding the `-console` switch to the Batch Loader command line causes all output to be echoed to the HTML Content Server log and to the console window that is running the Batch Loader. Alternatively, you can use operating system redirects to send the output to a separate log file.

Note:

The `-console` switch does not follow standard Windows command line syntax (although this may be corrected in later versions). You must use the `-console` syntax usually associated with UNIX instead of the `/console` syntax. With most other command line utilities, both syntaxes will work on both platforms.

Command Line Example

- Windows command line:

```
BatchLoader.exe -console -q -nc:/batching/batchinsert.txt
```

- UNIX command line:

```
BatchLoader -console -q -n/u2/apps/batching/batchinsert.txt
```

Sample Output

```
Processed 1 of 4 record.  
Processed 2 of 4 records.  
Processed 3 of 4 records.  
Processed 4 of 4 records.  
Done processing batch file 'c:/batching/batchinsert.txt'. Out of 4 records processed, 4  
succeeded and 0 errors occurred.
```

4.3.7 Adding a Redirect

You can use a redirect symbol on the command line to send the Batch Loader output to a separate log file. The symbol works on both UNIX and Windows. By default, the `-console` switch sends the Batch Loader's output to `stderr`. To redirect the output to a different file, use the special redirect symbol `2>`.

In the following examples, each command must be entered all on one line.

- Windows command line with redirect:

```
BatchLoader.exe -console -q -nc:/batching/batchinsert.txt 2> batchlog.txt
```

- UNIX command line with redirect:

```
BatchLoader -console -q -n/u2/apps/batching/batchinsert.txt 2>  
/logs/CSbatchload.log
```

4.3.8 Correcting Batch Load Errors

To correct any errors that occur during batch loading.

1. Choose **Administration**, then **Log Files**, then **Content Server Logs**.
2. In the Content Server log file, look through the Type column for the word `Error`.
3. Read the description to determine the problem.
4. Fix the error in one of these files:
 - The batch load file.
 - The error file for the failed content. (This option is available only if you enabled it on the Batch Loader window.) The error file is located in the same directory as the batch load file, with several digits appended to the batch load file name.

Note:

If you rerun an entire batch load file, content items that have already been checked in will usually fail. This occurs because the release dates of the existing content items will be the same as the ones you are trying to insert.

Figure 4-4 Sample Content Server Log File

Content Server Log File Created: 11/1/01 11:14 AM		
Type	Time	Description
Info	11/1/01 11:14 AM	Done creating batch file 'C:/stellent/samples/Batchloader/batchinsert1.txt'. Created 13 records with 0 errors.
Error	11/1/01 11:16 AM	Content item 'CDS Request Form-Bug Tracking' was not successfully checked in. It contains spaces. The content ID 'CDS Request Form-Bug Tracking' is invalid.
Error	11/1/01 11:16 AM	Content item 'CDS Request Form' was not successfully checked in. It contains spaces. The content ID 'CDS Request Form' is invalid.
Error	11/1/01 11:16 AM	Content item 'Custom Documentation Services Fact Sheet' was not successfully checked in. It contains spaces. The content ID 'Custom Documentation Services Fact Sheet' is invalid.
Error	11/1/01 11:16 AM	Content item 'customizeddocs' was not successfully checked in. The release date (11/1/01 11:14 AM) of the new revision is not later than the release date (11/1/01 11:14 AM) of the latest revision in the system.
Error	11/1/01 11:16 AM	Content item 'Documentation Assessment Checklist' was not successfully checked in. It contains spaces. The content ID 'Documentation Assessment Checklist' is invalid.
Error	11/1/01 11:16 AM	Content item 'Graphics Tracking Form' was not successfully checked in. It contains spaces. The content ID 'Graphics Tracking Form' is invalid.
Error	11/1/01 11:16 AM	Content item 'Stellent Consulting Services Methodology Fact Sheet' was not successfully checked in. It contains spaces. The content ID 'Stellent Consulting Services Methodology Fact Sheet' is invalid.
Error	11/1/01 11:16 AM	Content item 'To Do List' was not successfully checked in. It contains spaces. The content ID 'To Do List' is invalid.
Info	11/1/01 11:16 AM	Done processing batch file 'c:/stellent/samples/Batchloader/batchinsert1.txt'. Out of 13 records processed, 5 succeeded and 8 errors occurred. Compare the system log and error file 'c:/stellent/samples/Batchloader/batchinsert1_011111116.txt', correct any deficiencies and run the error file to load remaining items.

4.4 Optimizing Batch Loader Performance

This section provides some basic guidelines that you can use to improve Batch Loader performance. These suggestions can minimize potentially slow batch load performance when you are checking in a large number of content items. In many cases, proper tuning for batch loading can significantly speed up a slow server.

To minimize batch loading slow downs, try implementing the following Batch Loader adjustments:

- Temporarily disable other activities such as shutting down Inbound Refinery (see Starting and Stopping Oracle WebCenter Content Server and Inbound Refinery Instances in *Managing Oracle WebCenter Content*) and suspending the automatic update cycle feature of the Repository Manager.
- Analyze your database usage during a batch load to help the database query optimizer. Databases have built-in optimizer utilities that can help make database queries more efficient. However, to maximize the efficiency of optimizers, it is necessary to update or re-create the statistics about the physical characteristics of a table and the associated indexes. These characteristics include number of records, number of pages, and the average record length. The optimizers use these statistics to access data.

Each database has a proprietary command that you can use to invoke the statistic update or recreation process. For example:

- For Oracle, use the `ANALYZE TABLE COMPUTE STATISTICS` command
- For SQL Server, use the `CREATE STATISTICS` statement
- For DB2, use the `RUNSTATS` command

4.5 Best Practice Case Study

This case study describes a very slow load batch performance and the steps taken to diagnose and correct the situation. This information can serve as a model for isolating underlying issues and resolving batch loading performance problems.

- [Background Information](#).
- [Preliminary Troubleshooting](#).
- [Solution](#).

4.5.1 Background Information

A user wanted to load 27,000 content items in to the Content Server instance that was running on an AIX server. The DB2 database was running on a separate AIX server. The content items included TIF files as the native files and corresponding PDF files as the web-viewable files. Inbound Refinery generated thumbnails from the native files.

Initially during the batch load, the performance was acceptable with sub-second insert times. However, after a few thousand content items were loaded, the performance began to degrade. Content items started to require a few seconds to load and, eventually, the load time was over 10 seconds per content item.

4.5.2 Preliminary Troubleshooting

While the batch load was running, nothing seemed to be wrong with the Content Server instance. It had sufficient memory, the CPU utilization was low (less than 5%), and there were no disk bottlenecks. The Inbound Refinery server was busy, but was processing thumbnails at an acceptable rate.

Two issues were found with the database server:

- Two processes were taking turns to update the database. While one process was executing, the second process waited for other process to release database locks. When the first process completed, the second process executed while the first process waited. The processes in this execute/wait cycle included:
 - The actual batch load process that was updating the database tables after inserting a content item.
 - The Content Server instance was updating the database tables; changing the status from GENWWW to DONE after receiving notification that a thumbnail had been completed.

The two processes should not have been contending with each other because they were not updating the same content items. It seemed that the two processes were locking each other out because DB2 had performed lock escalation and was now locking entire database pages instead of single rows.

- There were a large number of tablespace scans being performed by both processes.

4.5.3 Solution

A two-step solution was used:

1. Inbound Refinery was shut down to prevent the status update process from competing with the batch loading process. The performance did improve because there was a 2000+ backlog of content items from the completed thumbnails.
2. A `RUNSTATS` command was issued on all the Content Server database tables to update the table statistics. This dramatically improved the performance of the batch load. The insert time returned to sub-second and the batch load completed within a short amount of time. It took 21 hours to insert the first 22,000 content items. After updating the table statistics, the remaining 5,000 content items were inserted in 13 minutes.

Part III

Monitoring Oracle WebCenter Content Server

This part provides information on monitoring Content Server and Inbound Refinery using the Oracle Enterprise Manager Fusion Middleware Console and WebCenter Content applications.

This part contains the following chapters:

- [Monitoring Content Server Status](#)
- [Monitoring Content Server Log Files](#)
- [Monitoring Content Server and Inbound Refinery Using Fusion Middleware Control](#)

5

Monitoring Content Server Status

This chapter describes how to monitor the status of a Content Server instance using various Oracle WebCenter Content Server internal resources.

This chapter includes the following topics:

- [Viewing Content Server Status](#)
- [Viewing Content Server Console Output](#)
- [Viewing System Configuration Information](#)
- [Viewing System Audit Information](#)
- [Viewing Server Output](#)
- [Viewing Event Output](#)
- [Checking Schema Cache](#)
- [Viewing Localization Audit Information](#)
- [Monitoring Scheduled Jobs](#)

5.1 Viewing Content Server Status

You can view the current status (such as running or stopped) of the Content Server instance.

To view current Content Server status using Fusion Middleware Control:

1. In the navigation tree, expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
4. On the Content Server home page, you can view the current status of a Content Server instance.

5.2 Viewing Content Server Console Output

You can view console output from the Content Server instance. This shows the same information that is located in the `DomainHome/ucm/cs/data/trace/classname.log` file.

1. Choose **Administration**, then **System Audit Information**.
2. Click **View Server Output**.
3. To refresh the output messages, click **Refresh Page**. To clear the output messages, click **Clear**.

5.3 Viewing System Configuration Information

Oracle WebCenter Content provides a Configuration Information page that displays system configuration information for the Content Server instance, which can be useful while troubleshooting a problem or working with the Oracle support organization.

To access the Configuration Information page:

1. Choose **Administration**, then **Configuration for *instance***.
2. To view details, click the link for each type of configuration information.

Configuration information provided includes:

- Server name
- Version
- Class loader
- Instance directory
- Database type
- Database version
- HTTP server address
- Mail server
- Search engine name
- Index engine name
- Active index
- Number of installed features
- Number of enabled components
- Number of disabled components
- Auto number prefix
- Use accounts
- Ntlm security enabled
- Allow get copy for user with read privilege
- Allow only original contribute to check out
- Java version

 **Note:**

Some options are specified during the software installation, while other options are set using the System Properties utility.

5.4 Viewing System Audit Information

Oracle WebCenter Content provides a System Audit Information page for a Content Server instance, which can be useful when troubleshooting a problem or adjusting the Content Server's performance.

The System Audit Information page provides several types of information.

- [System Audit General Information](#)
- [System Audit Localization Information](#)
- [System Audit Tracing Sections Information](#)
- [System Audit Cache Information](#)
- [System Audit Configuration Entry Information](#)
- [System Audit Component Report Information](#)

5.4.1 System Audit General Information

You can view general system audit numbers and details in the General Information section of the System Audit Information page.

To access the System Audit Information page, choose **Administration**, then **System Audit Information**.

- Amount of time the Content Server instance has been up and running.
- Number of server requests processed, and whether the system is handling server requests successfully. If the system is receiving too many requests, an email is sent to the system administrator regarding load performance.
- Total JVM memory capacity and total JVM available memory. Also information about the memory usage for the system, which may be useful in troubleshooting any "out of memory" errors you might receive. This can be important when running the Content Server instance with many users and a large quantity of data.
- Total number of threads, and information about which Java threads are currently running. This may be useful in determining the cause of an error.
- Total number of active database connections, and information about database activity.
- Total number of audit messages.

To view more details, click the link on the page for the type of configuration information.

5.4.2 System Audit Localization Information

You can view numbers about localization for your Content Server instance in the Localization Information section of the System Audit Information page.

To access the System Audit Information page, choose **Administration**, then **System Audit Information**.

- String key count
- Whether the Localization system is using a string index
- Localization test run time

- Localization test lookups per second

5.4.3 System Audit Tracing Sections Information

You can view tracing details in the Tracing Sections Information section of the System Audit Information page. This section enables tracing in the Content Server instance and can be activated on a section-by-section basis. Tracing for active sections is displayed by clicking **View Server Output** on the System Audit Information page. Section tracing can be useful for determining which section of the Content Server is causing trouble, or when you want to view the details of specific sections.

To access the System Audit Information page, choose **Administration**, then **System Audit Information**.

- To view a list with brief descriptions of sections available for tracing, click the **Info** icon next to the Tracing Sections Information heading.
- To see in-depth tracing for any active section that supports it, select **Full Verbose Tracing**. For more information, see [Using Tracing](#).
- To save tracing information, select **Save**.
- To specify additional sections for tracing, enter a comma-separated list of section names, or select sections from the menu next to the **Active Sections** field. The wildcard character ***** is supported; for example, using `schema*` will trace all sections that begin with the prefix `schema`. After specifying sections, click **Update**.
- To specify additional services to trace, enter a comma-separated list of service names in the Active Services field, then click **Update**.
- To specify additional threads to trace, enter a comma-separated list of thread names in the Active Threads field, then click **Update**.
- To specify what text to trap in the trace, enter the text in the **Event Trap Text** field, then click **Update**. For more information about using Event Trap, see the "[Caught in the Act!](#)" blog.
- To add a thread dump to the trace, select **Add Thread Dump**, then click **Update**.
- To return to the previous setting for any field you modified, click **Reset**.

Important:

Any options set in Tracing Sections Information will be lost when the Content Server instance is restarted unless you enable **Save** and click **Update**.

5.4.4 System Audit Cache Information

The Content Server instance caches various items for quick access. You can view current details for three caches in the Cache Information section of the System Audit Information page.

To access the System Audit Information page, choose **Administration**, then **System Audit Information**.

- **Search cache:** The number of permanently loaded pages and resource files. The number at which cache is temporarily capped. Whether any temporary items are loaded. Total number of distinct search queries being executed. Total number of distinct search queries being executed. These details are useful when troubleshooting any search related issues.

- **Schema cache:** Total number of items stored in schema cache. Number of bytes used out of number permitted. Additional details of any schema objects currently in cache.
- **Buffer pool cache:** Information about objects in cache and how much memory each object is using, which is reflected in the memory information of the System Audit General Information section. This information may be useful in pinpointing which object may be responsible for any memory leaks or other memory issues. (For information on troubleshooting, see [Troubleshooting Oracle WebCenter Content](#).)

To view more information, click the link for the type of cache information on the page.

5.4.5 System Audit Configuration Entry Information

You can view numbers and details in the Configuration Entry Information section of the System Audit Information page.

To access the System Audit Information page, choose **Administration**, then **System Audit Information**.

- Number of environment keys
- Number of overwritten config values
- Number of ignored settings
- Number of removed settings

To view more information for an item, click the link for the type of configuration entry information on the page.

5.4.6 System Audit Component Report Information

You can view information about components in the Component Report section of the System Audit Information page. This page lists Content Server components in alphabetical order by name. To view details about a component, click the component name in the list. Component details.

To access the System Audit Information page, choose **Administration**, then **System Audit Information**.

- Location: Pathname for the component in the instance
- Version: Date, build, and revision number
- Status: Current status of the component (Loaded or Skipped)
- Reason: Explanation of the component status

5.5 Viewing Server Output

You can view server output, which is the console output of the Content Server instance. This is the same information that is located in the `DomainHome/ucm/cs/data/trace/classname.log` file.

1. Choose **Administration**, then **System Audit Information**.
2. Click **View Server Output**.

5.6 Viewing Event Output

You can view event output from the server.

1. Choose **Administration**, then **System Audit Information**.
2. Click **View Event Output**.
3. To view other than the current output, select an earlier timestamp from the menu.
4. To update the current view, click **Refresh Page**.

5.7 Checking Schema Cache

You can view the newest schema cache information from the server.

1. Choose **Administration**, then **System Audit Information**.
2. Click **Check Schema Cache**.

The System Audit Information page opens and shows the Cache Information section with additional columns for View Names and Bytes Used in schema cache.

3. To see details for a specific schema cache view, select the name in the View Name column.

5.8 Viewing Localization Audit Information

You can view information regarding the availability of localized variables for the Content Server user interface on the Localization Audit page. This information is useful in determining if any custom metadata field labels or other customized Content Server text requires localization. Localization auditing is not persistent and must be started and stopped when using it.

1. Choose **Administration**, then **System Audit Information**.
2. Click **Localization Auditing**.
3. To start localization auditing, click **Start auditing**.
4. To stop localization auditing, click **Stop auditing**.
5. To view the generated Java exceptions, click **Show** in the Stack Trace column.

5.9 Monitoring Scheduled Jobs

Scheduled jobs run as part of events scheduled by system components. The Scheduled Jobs Administration interface can be used to monitor information about scheduled jobs on the Content Server instance and in some cases edit scheduled jobs.

- [Viewing Active Scheduled Jobs](#)
- [Viewing Scheduled Jobs History](#)
- [Modifying a Scheduled Job](#)
- [Canceling or Deleting a Scheduled Job](#)

5.9.1 Viewing Active Scheduled Jobs

To view active scheduled jobs:

1. Choose **Administration**, then **Scheduled Jobs Administration**, then **Active Scheduled Jobs**.

The job name, job description, processed date and time, current status, and available actions are listed for each scheduled job on the Scheduled Jobs Listing page. The status icons represent Priority, Inactive/Processed, Once/Repeat, and Short/Long.

2. Click **Actions** to select any of the following actions for a scheduled job:

- **Info**: Display the Scheduled Jobs Information page.
- **Edit**: Edit the scheduled job.
- **Cancel**: Cancel the scheduled job.
- **Delete**: Delete the scheduled job.

3. Click **Info**.

The Scheduled Jobs Information page opens.

5.9.2 Viewing Scheduled Jobs History

To view a scheduled job history:

1. Choose **Administration**, then **Scheduled Jobs Administration**, then **Scheduled Jobs History**.

The Historical Scheduled Jobs Listing page opens and lists the job name, job description, last process date, last status, and actions for each scheduled job.

2. Click the **Info** icon in the Actions column to open the Scheduled Jobs Information page for a specific job.

5.9.3 Modifying a Scheduled Job

To modify a scheduled job:

1. Choose **Administration**, then **Scheduled Jobs Administration**, then **Active Scheduled Jobs**.

2. For a specific job in the list on the Scheduled Jobs Listing page, click the **Actions** icon, then **Edit**.

The job name, description, category, exception parent job, initial user, queue type, schedule type, current state, priority, interval, start token, progress status, create date, update date, process date, last processed date, and last processed status are displayed.

3. Edit the appropriate fields (not all fields can be modified).
4. Click **Update**. If you want to remove your changes, click **Reset**.

5.9.4 Canceling or Deleting a Scheduled Job

To cancel or delete a scheduled job:

1. Choose **Administration**, then **Scheduled Jobs Administration**, then **Active Scheduled Jobs**.

2. To cancel a specific job in the list on the Scheduled Jobs Listing page, click the **Actions** icon for the job, then select **Cancel**.
3. To delete a specific job in the list on the Scheduled Jobs Listing page, click the **Actions** icon for the job, then select **Delete**.

6

Monitoring Content Server Log Files

This chapter provides information on finding and using Content Server status information and errors in log files.

This chapter includes the following topics:

- [Introduction to Managing Content Server Log Files](#)
- [About Content Server Log File Characteristics](#)
- [Accessing Content Server Logs](#)
- [Accessing Archiver Logs](#)
- [Accessing Inbound Refinery Logs](#)

6.1 Introduction to Managing Content Server Log Files

Oracle WebCenter Content stores status information and errors in log files. Log files are used to register system events, with their date and time of occurrence. They can be valuable tools for troubleshooting, especially if verbose logging is turned on. Not only do logs indicate that specific events occurred, they also provide important clues about a chain of events that led to an error or problem.

Note:

When applied to trace log output, verbose logging can quickly increase the size of a log file and possibly cause the Content Server instance to slow down. It is recommended that for trace logs, verbose logging is only used when troubleshooting a specific issue. Content Server logs for system events do not have this issue with verbose logging.

For information on troubleshooting, see [Troubleshooting Oracle WebCenter Content](#). For information on viewing system audit information, see [Monitoring Content Server Status](#).

Information is also captured in logs controlled by Oracle Fusion Middleware Control and the Oracle WebLogic Server Administration Console using Oracle log APIs. The WebCenter Content interface provides access to these logs. For more information about using Fusion Middleware Control to monitor logs, see [Managing Log Information Using Fusion Middleware Control](#).

6.2 About Content Server Log File Characteristics

Log files associated with the Content Server instance have the following characteristics:

- They are created only once each day at the time the first status, error, or irrecoverable error occurs.
- No empty log files are generated.

Each log file contains the following columns:

- **Type:** Specifies the kind of incident that prompted the log entry: Information, Error, or Fatal.
- **Time:** Lists the date and time the log entry occurred.
- **Description:** Describes the incident that occurred.

The log files are standard HTML pages and are maintained for each Content Server instance. Logs are kept in revolving file name format for a maximum of 30 files. When the 31st file is created, the oldest one is deleted. Therefore, log file names in Content Server bear no relation to the date they were generated. To find a certain day in the log file, view the index file in a browser and select that day's link. The file name is displayed in the browser's status bar (if it is enabled).

 **Note:**

Bookmark your log file pages. This will help you to troubleshoot problems, even if the Content Server instance is unavailable. Also, know where your configuration files are so you can find them if the Content Server instance is unavailable.

6.3 Accessing Content Server Logs

The Content Server logs are listed by date and time. One file is generated for each day. Entries are added to the file throughout the day as events occur.

The following types of server log entries are generated:

- **Info:** Displays basic status information. For example, status information is logged if the server is ready and waiting.
- **Error:** Displays errors that occur but do not stop the software from functioning. For example, an error is logged if a user requests secure information that they are not allowed to access.
- **Fatal:** Displays errors that stop the software from functioning. For example, a fatal error is logged if the Content Server instance cannot access the database.

To access a Content Server log:

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Log Files**.
3. Select **Content Server Logs**.
4. On the Content Server Logs page, select the link that corresponds to the date and the time of the log that you want to view.

 **Note:**

You must be logged in to the Content Server instance as an administrator to be able to view the log files.

If, for whatever reason, you cannot view the log files from the Administration tray or menu, you can also access them on the file system of the Content Server instance. The log files can be found in these locations:

Log Files	Found in:
Content Server	<i>IntradocDir/weblayout/groups/secure/logs</i>
Console Output Logs	<i>IntradocDir/bin/classname.log</i>
Refinery	<i>IntradocDir/weblayout/groups/secure/logs/refinery</i>
Archiver	<i>IntradocDir/weblayout/groups/secure/logs/archiver</i>

6.4 Accessing Archiver Logs

Content Server Archiver logs show information about imports, exports, and replications. The Archiver logs are listed by date and time. They are generated once a day when the first Archiver information status, fatal error, or error occurs.

The following types of Archiver log entries are generated:

- **Info:** Displays basic status information. For example, status information is logged when an export and an import starts and finishes.
- **Error:** Displays user/administration errors that occur but do not stop the software from functioning. For example, an error is logged if there is no file information for a content item that you are trying to export.
- **Fatal:** Displays errors that stop the software from functioning. For example, a fatal error is logged if the Content Server instance cannot access the database. Check the connection string, user name, and password.

To access an Archiver log:

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Log Files**, then select **Archiver Logs**. Alternately, click the **Archiver Logs** link on the Administration page.
3. On the Archiver Logs page, select the link that corresponds to the date and the time of the log.

A table showing the type, date and time, and description of each action opens. The table also includes the name of the Content Server instance that created the archive.

6.5 Accessing Inbound Refinery Logs

All Oracle WebCenter Content: Inbound Refinery logs are accessed through the Inbound Refinery interface. For information on monitoring Refinery status through log files, see *Inbound Refinery in Managing Oracle WebCenter Content*.

7

Monitoring Content Server and Inbound Refinery Using Fusion Middleware Control

This chapter describes how to monitor Oracle WebCenter Content Server and Inbound Refinery logs, performance information, and MBean information by using Oracle Enterprise Manager Fusion Middleware Control.

This chapter includes the following topics:

- [Managing Log Information Using Fusion Middleware Control](#)
- [Viewing Performance Information Using Fusion Middleware Control](#)
- [Viewing MBean Information Using Fusion Middleware Control](#)

7.1 Managing Log Information Using Fusion Middleware Control

You can view log messages and manage the log configuration for the Content Server or InBound Refinery instance using the Fusion Middleware Control interface.

- [Viewing Log Information Using Fusion Middleware Control](#)
- [Modifying Log Information Using Fusion Middleware Control](#)

7.1.1 Viewing Log Information Using Fusion Middleware Control

1. Log in to Fusion Middleware Control.
2. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`), then **WebCenter**, then **Content**.
 - For the Content Server instance, expand **Content Server**, then select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
 - For the Inbound Refinery instance, expand **Oracle Inbound Refinery**, then select the Inbound Refinery instance name (for example, `IBR (IBR_server1)`).

3. On the home page for the instance, from the **Content Server** or **IBR** menu choose **Logs**, then **View Log Messages**.

The Log Messages page contains information about the contents of all available log files. You can use this page to:

- Search for log messages logged during the past "n" hours.
- Search for log messages that were logged between two time intervals.
- Filter log messages based on message type.

7.1.2 Modifying Log Information Using Fusion Middleware Control

1. Log in to Fusion Middleware Control.

2. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`), then **WebCenter**, then **Content**.
 - For the Content Server instance, expand **Content Server**, then select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
 - For the Inbound Refinery instance, expand **Oracle Inbound Refinery**, then select the Inbound Refinery instance name (for example, `IBR (IBR_server1)`).
3. On the home page for the instance, from the **Content Server** or **IBR** menu choose **Logs**, then **Log Configuration**.
4. Use the Log Configuration page to configure basic and advanced log configuration settings for log levels and log files. You can:
 - Change log levels of persistent loggers (loggers defined in the logging configuration file).
 - Change log levels of run-time loggers.
 - Specify loggers that are currently neither persistent nor run time.
 - Specify the log file configuration parameters such as the log file path and log rotation policies.
 - Create a new log file configuration.
 - Create a new log file configuration using an existing log file configuration.
 - View the log file configuration parameters.
 - Associate one or more loggers with a log file configuration.

7.2 Viewing Performance Information Using Fusion Middleware Control

You can monitor performance information for the Content Server or Inbound Refinery instance to quickly assess the performance of the system. Information includes a graph of key metrics and values, and a listing of recent service requests.

To view performance information:

1. Log in to Fusion Middleware Control.
2. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`), then **WebCenter**, then **Content**.
 - For the Content Server instance, expand **Content Server**, then select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
 - For the Inbound Refinery instance, expand **Oracle Inbound Refinery**, then select the Inbound Refinery instance name (for example, `IBR (IBR_server1)`).
3. On the home page for the instance, from the **Content Server** or **IBR** menu choose **Monitoring**, then **Performance Summary**. The Performance Summary page appears.

By default, the Performance Summary page shows the performance metrics for the past 15 minutes. You can use the **Slider** or the **Enter Time** icon to change the time period for metrics to appear.

The Performance Summary page displays information in a graph format. To view metrics in a table format, select **Table View**.

The key Inbound Refinery metric displayed by default is the rate of conversion, measured in documents per minute. Key Content Server metrics are described in [Table 7-1](#).

Table 7-1 Key Content Server Metrics

Element	Description
Active Threads	The number of active threads in the Content Server instance.
Active Database Connections	The number of active database connections made by the Content Server instance.
Audit Messages	The total number of audit messages.
Read Actions	The number of Read service requests processed, and whether the system is handling the requests successfully.
Write Actions	The number of Write service requests processed, and whether the system is handling the requests successfully.
Search Queries Cached	The number of search queries cached (rows).
Hit to Miss Ratio	The hit to miss ratio for the number of search queries performed.
Documents in GenWWW State	The number of documents in a GenWWW state waiting for Inbound Refinery.
Documents Waiting to be Indexed in Done State	The number of documents in a Done state waiting to be indexed.
Documents in Workflow	The number of documents currently in workflows.
Average Requests Per Sec	The average number of Services requested per second.

- Click **Show Metric Palette** to see all the metrics that can be viewed in the chart. The Metric Palette lists available options for metrics to display in graphs.

Click **Hide Metric Palette** to collapse the Metric Palette and provide more space to view the metric chart.

- With the Metric Palette expanded, select the check box for each metric you want to appear.

Metric Palette Content Server metrics are described in [Table 7-2](#).

Metric Palette IBR metrics are described in [Table 7-3](#).

Table 7-2 Content Server Metric Palette

Element	Description
Cache Information	<ul style="list-style-type: none"> Items Temporarily Loaded: Indicates whether any temporary items are loaded. Pages Permanently Loaded: The number of permanently loaded pages. Resource Files Permanently Loaded: The number of permanently loaded resource files. Temporary Cache capped at: The number at which cache is temporarily capped. Temporary Items Consuming: The total number of items in cache.

Table 7-2 (Cont.) Content Server Metric Palette

Element	Description
Connections	<ul style="list-style-type: none"> • Active Database Connections: The total number of active database connections made by the WebCenter Content Server instance. • Active Threads: The total number of active threads. • Audit Messages: The total number of audit messages. • Read Actions: The number of Read service requests processed, and whether the system is handling the requests successfully. • Write Actions: The number of Write service requests processed, and whether the system is handling the requests successfully.
Inbound Refinery Queue	<ul style="list-style-type: none"> • Documents in GenWWW State: The number of documents waiting for Inbound Refinery in a GenWWW state. • Documents Waiting to be Indexed in Done State: The number of documents waiting to be indexed in a Done state.
Localization Information	<ul style="list-style-type: none"> • Localization test lookups per second: The number of localization test lookups per second. • String Key Count: The number for the string key count.
Memory Details	<p>The number of Write service requests processed, and whether the system is handling the requests successfully.</p> <ul style="list-style-type: none"> • Available Processors: The number of processors available to the WebCenter Content Server instance. • Free Memory (bytes): The total free memory available in JVM on the WebCenter Content Server instance. • Maximum Memory (bytes): The maximum JVM memory capacity for the WebCenter Content Server instance. • Total Memory (bytes): The total JVM memory for the WebCenter Content Server instance.
Response	Status: Whether the WebCenter Content Server instance is up or down. It takes on values 1 or 0: 1 indicates up and 0 indicates down.
Schema Cache Details	Number of Items Stored: The total number of items in cache.
SearchCache	<ul style="list-style-type: none"> • Hit to Miss Ratio: The hit to miss ratio for the number of search queries performed. • Search Queries Cached: The number of search queries cached (rows).
Server State	State: The current state of the WebCenter Content Server.
Service Requests	Average Requests Per Sec: The average number of Services requested per second
Workflow	Documents in Workflow: The number of documents currently in workflows.

Table 7-3 Inbound Refinery Metric Palette

Element	Description
Jobs By Size	Number of jobs per file size.
Jobs By Type	Number of jobs per conversion type.

Table 7-3 (Cont.) Inbound Refinery Metric Palette

Element	Description
Job Summary	<ul style="list-style-type: none"> • Active Jobs: Number of jobs currently being converted. • Conversion Rate: The rate since startup at which documents are converted, measured in documents per minute. • Failed Jobs: The number of documents that were not converted successfully. • Succeeded Jobs: The number of documents that were converted successfully • Total Jobs: All documents processed by Inbound Refinery, including those that succeeded and those that failed.
PreconversionQueueMetrics	Number of jobs currently waiting to be converted.
PostconversionQueueMetrics	Number of jobs that have been converted and are waiting to be picked up by Content Server.
Response	Status: Whether the Inbound Refinery instance is up or down. It takes on values 1 or 0: 1 indicates up and 0 indicates down.

7.3 Viewing MBean Information Using Fusion Middleware Control

You can use the MBean browser to view MBean attribute information about the Content Server or Inbound Refinery instance.

To view MBean information:

1. Log in to Fusion Middleware Control.
2. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`), then **WebCenter**, then **Content**.
 - For the Content Server instance, expand **Content Server**, then select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
 - For the Inbound Refinery instance, expand **Oracle Inbound Refinery**, then select the Inbound Refinery instance name (for example, `IBR (IBR_server1)`).
3. On the home page for the instance, from the **Content Server** or **IBR** menu choose **System MBean Browser**.

The System MBean Browser page displays the navigation pane with the instance name highlighted and the configuration MBean application deployment information for the instance.

4. On the Attributes tab, you can view individual attribute names, descriptions, type of access, and values. If you change an attribute value, click **Apply**.
5. On the Operations tab, you can view and invoke individual MBean operations.
 - To view details, select an MBean.
 - To apply an MBean operation, select **Invoke**.
 - To reset an operation to its previous setting, click **Revert**.
 - To go back to the Operations tab, click **Return**.

See Understanding WebLogic Server MBeans in *Developing Custom Management Utilities Using JMX for Oracle WebLogic Server*.

Part IV

Administering System Configuration

This part provides information about administering the Oracle WebCenter Content system configuration, including system settings, components, search index, file store system, providers, and mapping URLs.

This part contains the following chapters:

- [Configuring System Properties](#)
- [Managing Components](#)
- [Managing Search Features](#)
- [Configuring the Search Index](#)
- [Managing a File Store System](#)
- [Configuring Providers](#)
- [Mapping URLs](#)

8

Configuring System Properties

This chapter describes how to configure Oracle WebCenter Content Server system properties using Oracle Enterprise Manager Fusion Middleware Control, the Content Server Administration interface, and the Content Server System Properties utility. This chapter includes the following topics:

- [About System Properties](#)
- [Configuring System Properties Using Fusion Middleware Control](#)
- [Configuring General Options](#)
- [Configuring Content Security](#)
- [Configuring Internet Information Using Content Server](#)
- [Configuring System Database Properties](#)
- [Configuring Oracle Content Management Integration Settings](#)
- [Configuring Server Properties](#)
- [Configuring Localization Properties](#)
- [Configuring Paths Properties](#)

8.1 About System Properties

System properties are system-wide settings that enable you to tailor the Content Server instance to your particular requirements. System properties are set during installation and are generally updated occasionally, or as needed, in contrast to use of other administration tools for more regular maintenance of users and content.



Note:

Regardless of which method is used to modify system properties, you must restart the Content Server instance for any configuration changes to take effect.

There are several tools for modifying system properties:

- The Enterprise Manager Fusion Middleware Control interface can be used to view and modify server, Internet, e-mail, security, and component configuration for the Content Server instance. For information on accessing Fusion Middleware Control, see [Starting and Stopping Content Server and Inbound Refinery](#).
- The Content Server's Administration interface can be used to view and modify server, Internet, e-mail, security, and component configuration for the Content Server instance. Information on accessing these configuration options is provided in this chapter.
- The System Properties utility is a Content Server administration application that can be used to configure system-wide settings from the system on which a Content Server instance is installed. This utility runs as a standalone application. For information on

running the System Properties utility, see [Running Administration Applications in Standalone Mode](#).

 **Note:**

For the System Properties utility to run as a standalone application for a Content Server instance on a WebCenter Content domain, additional configuration is required.

- Most system properties settings correspond to a configuration variable in one of the following configuration files:

- `IntradocDir/config/config.cfg`
- `DomainHome/ucm/cs/bin/intradoc.cfg`
- `IntradocDir/search/search.cfg`

It is recommended that you make changes to these files using the Administration interface or the System Properties utility to ensure that the settings are entered correctly. While it is possible to edit these files directly using a text editor, it might allow errors to be introduced. See Configuration Variables in *Configuration Reference for Oracle WebCenter Content*.

 **Tip:**

There are many techniques for optimizing the performance of a Content Server instance. One of the types of tuning involves changing default parameters and software settings that affect the core Content Server performance. System optimization and performance tuning is often accomplished by adjusting system settings and configuration variables or tuning resources such as databases and indexes.

For example, as the content in your Content Server instance increases, you might experience a shortage of available space. In this case, moving the vault, weblayout, and search index directories to another drive with more space can help alleviate storage problems. Moving these directories requires adding entries in to the `DomainHome/ucm/cs/bin/intradoc.cfg` file.

8.2 Configuring System Properties Using Fusion Middleware Control

This section describes how to use Oracle Enterprise Manager Fusion Middleware Control interface to configure certain Content Server system properties.

This section covers the following topics:

- [Modifying Content Security Configuration Using Fusion Middleware Control](#)
- [Modifying General Configuration Using Fusion Middleware Control](#)
- [Modifying Internet Configuration Using Fusion Middleware Control](#)
- [Modifying Email Configuration Using Fusion Middleware Control](#)



Note:

For information on using Fusion Middleware Control to manage Content Server components, see [Managing Components Using Fusion Middleware Control](#).

For information on records management configuration options, see Configuring Retention Definitions and Options in *Managing Oracle WebCenter Content*.

8.2.1 Modifying Content Security Configuration Using Fusion Middleware Control

WebCenter Content Server security configuration specifies settings used to control user access to WebCenter Content Server content items.

To modify content security configuration for WebCenter Content Server:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`). The home page for your WebCenter Content Server instance appears.
4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **General Configuration**.
5. You can modify the settings in the Content Security section of the General Configuration page. Settings are described in [Table 8-1](#).
6. Click **Apply**.

If you do not want to apply changes, click **Revert** to return to the previous configuration settings.

Table 8-1 General Configuration: Content Security

Element	Description
Allow get copy for user with Read privilege	Allows a user with Read privilege to a content item to get a copy of the content item. To enable, select the check box.
Allow author to delete revision	Allows the author of a content item to delete revisions of the item as long as the author/owner has Read privilege (otherwise requires Delete privilege to the content item's security group). To enable, select the check box. Note: If a site is using Contribution Folders, then this setting means an author/owner can delete the content item without having Delete privilege to the content item's security group.
Allow only original contributor to checkout	Allows only the original contributor of a content item to check out the item. To enable, select the check box.
Show only known accounts	Displays only known accounts to users. Known accounts are those to which a user has been authorized. To enable, select the check box.

8.2.2 Modifying General Configuration Using Fusion Middleware Control

General configuration specifies a variety of settings used to configure WebCenter Content Server, including enabling accounts and adding configuration variables specific to your unique deployment.

To modify general configuration for WebCenter Content Server:

1. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).

The home page for your WebCenter Content Server instance appears.

4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **General Configuration**.
5. You can modify the settings in the General Admin Server Configuration section of the General Configuration page. Settings are described in [Table 8-2](#).
6. Click **Apply**.

If you do not want to apply changes, click **Revert** to return to the previous configuration settings.

Table 8-2 General Configuration: General Admin Server Configuration

Element	Description
Allow override format on check-in	Allows the format to be overridden on a content item when it is checked in to the repository. To enable, select the check box.
Enable accounts	Enables the use of accounts in WebCenter Content Server. To enable, select the check box. For more information, see Managing Accounts .
Automatically assign a content ID on check-in	Automatically assigns a content ID to a content item when it is checked in to the repository. To enable, select the check box.
Major revision label sequence	Displays the Major Revision Label Sequence from the system configuration.
Minor revision label sequence	Displays the Minor Revision Label Sequence from the system configuration.
Auto number prefix	Displays the auto number prefix from the system configuration.
Additional Configuration Variables	Displays additional general configuration variables for the system configuration. You can add configuration variables in this field. See Configuration Variables in <i>Configuration Reference for Oracle WebCenter Content</i> .

8.2.3 Modifying Internet Configuration Using Fusion Middleware Control

WebCenter Content Server configuration settings specify information used to identify a Content Server deployment scenario.

To modify the Internet server configuration:

1. In the navigation tree, expand the appropriate domain name (for example, `Farm_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
The home page for your Content Server instance appears.
4. On the Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Internet Configuration**.
5. You can modify some of the settings in the Server Configuration section of the Internet Configuration page. Some of the settings are Read Only and cannot be changed. Settings are described in [Table 8-3](#).
6. Click **Apply**.
If you do not want to apply changes, click **Revert** to return to the previous configuration settings.

Table 8-3 Oracle WebCenter Content - Internet Configuration

Element	Description
HTTP Address	<p>Name of the HTTP web server for the Content Server instance. For security reasons, this field cannot be changed from the interface. You must change the field using the Oracle WebCenter Content standalone application.</p> <p>The server address is used to formulate full URLs in the Content Server user interface. This prevents users from being prompted to log in again because the domain name used to enter the server is not changed when links on pages are relative. Example: <code>pc.idc.example.com</code>.</p>
IP Address Filter	<p>The list of IP addresses that can be used to access the Content Server instance. This field is required.</p> <p>The list of IP addresses are allowed to communicate to the Content Server instance through the Intradoc Server Port. The field accepts both IP and IPv6 addresses, with a pipe as the separator between addresses. This list must be well defined because it is a trusted connection. Example: <code>10.131.123.*</code>.</p>
Intradoc Server Port	<p>The server port number for the Content Server instance.</p> <p>The Intradoc server port is the port number listened to by the Content Server instance. This is a trusted connection where only the user ID is required to authenticate. Example: <code>4056</code>.</p>
Use SSL	<p>Specifies whether a Secure Sockets Layer (SSL) enabled web server is being used. For security reasons, this field cannot be changed from the interface. You must change the field using the Oracle WebCenter Content standalone application.</p> <p>SSL is related to the HTTP server address and indicates that the full URL uses the secured HTTP nomenclature. For example, it generates an address with <code>https://HttpServerAddress/...</code> instead of <code>http://HttpServerAddress/...</code></p>

8.2.4 Modifying Email Configuration Using Fusion Middleware Control

WebCenter Content Server email configuration settings specify information used to identify the Content Server deployment scenario.

To modify the email configuration:

1. In the navigation tree, expand the appropriate domain name (for example, Farm_base_domain).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the Content Server instance name (for example, Oracle WebCenter Content - Content Server (UCM_server1)).
4. On the Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Internet Configuration**.
5. You can modify some of the settings in the Email Configuration section of the Internet Configuration page. One of the settings is Read Only and cannot be changed. Settings are described in [Table 8-4](#)
6. Click **Apply**.

If you do not want to apply changes, click **Revert** to return to the previous configuration settings.

Table 8-4 Oracle WebCenter Content - Email Configuration

Element	Description
Mail Server	Name of the mail server used to send email notifications from the Content Server instance. Example: mailserver.example.com.
SMTP Port	Port number used for SMTP communications. Example: 25. For security reasons, this field cannot be changed from the interface. You must change the field using the Oracle WebCenter Content standalone application.
Admin Mail Address	Email address for the administrator for the Content Server instance. This is the administrator email address that receives error messages. Such messages are generally logged, but this is an additional method of notification. Example: mymail@example.com.
HTTP Server Address	Web address on which the mail server runs where a partial URL is used instead of a full address. Example:HttpServerAddress=example.

8.3 Configuring General Options

After WebCenter Content and a Content Server instance are deployed and initial configuration specified, you can set or modify general function options for Content Server using the Options tab on the System Properties utility or using the General Configuration page accessed through the Administration interface.

- To access the System Properties: Options tab, see [Running Administration Applications in Standalone Mode](#).
- To access the General Configuration page, choose **Administration**, then **Admin Server**, then **General Configuration**.

Using general function options, you can:

- Enable users to select the format of a document during check-in
- Enable users to select multiple files to check out or download at the same time
- Enable users to check in multiple files as a single Zip file

- Enable the use of accounts
- Enable all full-text search terms to be highlighted in returned PDF, HTML, and text documents.
- Enable Enterprise Search fields to be displayed on search pages if Enterprise Search is configured for use
- Enable Content IDs to be generated automatically as six-digit, sequential numbers
- If automatic Content ID generation is enabled, the string specified in this field is added as a prefix to the six-digit, sequential number
- Specify how the optional second letter or number in a revision number is incremented

You must restart the Content Server instance for any configuration changes to take effect.

8.3.1 Revision Label Sequence

Among the General Configuration options that can be set is the revision label sequence. The metadata field named "Revision" has a default revision number sequence of 1, 2, 3, 4, 5, and so forth. This number increments automatically for each revision of a document.

You can override the Revision default by changing the definition of the revision label. The revision label consists of two parts: a major revision sequence and minor revision sequence. The *Major Revision Label Sequence* (MajorRevSeq) is the first number or letter and the *Minor Revision Label Sequence* (MinorRevSeq) follows. For example, in the revision sequence 1a, 1b, 1c, 2a, 2b, 2c, 3a, 3b, 3c, and so forth, the numbers 1, 2, 3 are the major revision sequence and a, b, c are the minor revision sequence.

8.3.1.1 Revision Label Ranges

Both the major and minor revision sequences are defined as a range of numbers or letters. The major sequence can have multiple ranges, while the minor sequence can only have one range.

The following are the restrictions on defining the range:

- Numbers or letters can be used, but not both. For example, 1 through 10 is a valid range but A through 10 is not a valid range.
- Letter ranges can have only one letter. For example, A through Z is a valid range but AA through ZZ is not a valid range.
- If a letter range is used in the major revision sequence, then the minor revision sequence must be either a numeric range or not used. If a numeric range is used in the major revision sequence, then the minor revision sequence must be either a letter range or not used.

8.3.1.2 Revision Examples

The following are examples of different revision sequences and how you would define the major and minor revision entries in the config.cfg file.

Example 1

```
MajorRevSeq=A-D,1-99
```

The revision sequence is A, B, C, D, 1, 2, 3, 4, and so forth.

Example 2

```
MajorRevSeq=1-99
```

```
MinorRevSeq=a-c
```

The revision sequence is 1a, 1b, 1c, 2a, 2b, 2c, 3a, 3b, 3c, and so forth.

8.3.1.3 Revision Configuration Settings

To change the default revision sequence manually in the *IntradocDir/config/config.cfg* file, enter the following name/value pairs:

- `MajorRevSeq=range1,range2,range3...`
- `MinorRevSeq=range`

where *range1,range2,range3...* and *range* are the defined range sequence.

8.3.2 Chunking Function

The Content Server *Chunking* function protects large data transfers from transfer failures by dividing data into chunks and transferring one chunk at a time. If a transfer fails, all chunks transferred to the Content Server instance before failure are saved, and the transfer can be resumed from the point of failure.

 **Note:**

If the client session using the Chunking function is terminated, either by timeout or by closing the client browser, the transfer will fail.

You can use the Chunking function with the upload applet.

To enable and configure the Chunking function:

1. Enable the upload applet or the HTTP provider. See [Configuring General Options](#).
 - For information on how to enable the upload applet, see [Configuring General Options](#).
 - For information on how to create a HTTP provider, see [Managing Additional Content Server Security Connections](#).
2. Set the following configuration settings in the **Additional Configuration Variables** field on the General Configuration page:

```
DisableHttpUploadChunking=false  
AppletChunkThreshold=size in bytes  
AppletChunkSize=size in bytes
```

The `AppletChunkSize` setting sets the size of the individual chunks. The `AppletChunkThreshold` setting sets the minimum file size that will use the Chunking function. Both of these values default to 1M.

3. To debug the Chunking function, set **ChunkedRequestTrace=true**. This setting enables you to view chunked requests on the Server Output page.
4. Save the changes.

5. Restart the Content Server instance.

8.3.3 Vertical Clustering and Scale-Up

You can set up instance specific configurations (in vertical scale-up):

1. Open a new browser window, and log in to the Content Server instance as system administrator.
2. Choose **Administration**, then **Admin Server**, then **General Configuration**.
3. Set **Server Port (Default)**, **Server Port (<server_name>)**, **Server IP Filter**, and **Server Hostname Filter** fields.

Example:

```
IntradocServerPort=4444
```

Server specific IntradocServerPort can be specified by appending a "." and a server name:

```
IntradocServerPort.UCM_server1=5500
```

```
SocketHostAddressSecurityFilter=127.0.0.1|10.196.18.56|0:0:0:0:0:0:1
```

4. Click **Save**.
5. Restart the Content Server instance.

8.3.3.1 Extending WebCenter Content: Inbound Refinery Components

WebCenter Content: Inbound Refinery components don't use WebLogic Server clustering for scale up and failover. You can deploy and configure multiple, independent Inbound Refinery Managed Servers for WebCenter Content to use.

8.3.3.2 WebCenter Content Scaleup and Ports

When you scale up WebCenter Content, the scaled-up server uses a port which is different from the port that you configured in the Configuration Wizard.

In the WebCenter Content configuration file, you must specify the IntradocServerPort value for each Managed Server instance. The port for each Managed Server instance that resides in one machine must be unique. For example, if `Content_server1` and `Content_server2` are in the same machine, the configuration file should look similar to the following:

```
IntradocServerPort=4444  
IntradocServerPort.UCM_serverd1=4444  
IntradocServerPort.UCM_serverd2=4445
```

8.4 Configuring Content Security

After WebCenter Content and a Content Server instance are deployed and initial configuration specified, you can set or modify some Content Server content security options using the Content Security tab on the System Properties utility Content Security tab or using the Content Security page accessed through the Administration interface.

- To access the System Properties: Content Security tab, see [Running Administration Applications in Standalone Mode](#).
- To access the Content Security page, choose **Administration**, then **Admin Server**, then **Content Security**.
- To configure security options using Fusion Middleware Control, see [Modifying Content Security Configuration Using Fusion Middleware Control](#).

Using content security options, you can:

- Allow users with only Read privilege to a content item's security group to get a copy of the native file.
- Allow only the author or a user with Admin privilege to a content item's security group to check out the content item.
- Allow the author of a content item to delete the content item as long as they have Read privilege, where otherwise they would need Delete privilege to the content item's security group.

 **Note:**

If a site is using Contribution Folders, then this setting means an author can delete the content item without having Delete privilege to the content item's security group.

- Allow only globally predefined accounts to appear in the Accounts list on checkin page.

You must restart the Content Server instance for any configuration changes to take effect.

8.5 Configuring Internet Information Using Content Server

After the WebCenter Content domain and Content Server are deployed and initial configuration specified, you can view or modify Content Server Internet options using the Internet tab on the System Properties utility, or using the Internet Configuration page accessed through the Administration interface. Typically Internet options are specified during Oracle WebCenter Content installation and initial configuration.

- To access the System Properties: Internet tab, see [Running Administration Applications in Standalone Mode](#). Certain fields can only be modified using the System Properties utility.
- To access the Internet Configuration page, choose **Administration**, then **Admin Server**, then **Internet**.

Using Internet configuration options, you can:

- View the HTTP server address for the Content Server instance. For security reasons, this field cannot be changed from the interface. You must change the field using the Oracle WebCenter Content standalone application.
- View and modify the IP Address Filter which lists IP addresses that can be used to access the Content Server instance.
- View and modify the Intradoc Server Port, which is the server port number for the Content Server instance.
- View whether a Secure Sockets Layer (SSL)-enabled web server is used. For security reasons, this field cannot be changed from the interface. You must change the field using the Oracle WebCenter Content standalone application.

- View and modify the email server used to send email notifications from the Content Server instance
- View the port used for SMTP communications. For security reasons, this field cannot be changed from the interface. You must change the field using the Oracle WebCenter Content standalone application.
- View and modify the administrator email address that the Content Server instance uses to send email notifications.

You must restart the Content Server instance for any configuration changes to take effect.

8.6 Configuring System Database Properties

After WebCenter Content and a WebCenter Content Server instance are deployed and initial configuration specified, you can set or modify Content Server system database properties. The system database can be an Oracle Database, Microsoft SQL Server, IBM DB2, or another database.

For information about supported databases, see the "System Requirements and Supported Platform" document for your product on the Oracle Fusion Middleware Supported System Configurations page on the Oracle Technology Network at:

<http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html>

See Configuring the WebCenter Content Domain in *Installing and Configuring Oracle WebCenter Content*.

Note:

For security reasons, the Content Server Administration interface cannot be used to configure these options. You must start the System Properties utility as a standalone application from the computer where the Content Server instance is installed. The method required to start this program differs slightly between Windows and UNIX installations. For details, see [Running Administration Applications in Standalone Mode](#).

Using system database options, you can:

- Modify whether JDBC is enabled and choose a driver option.
- Modify whether the database is case sensitive (such as Oracle or Informix).
- Modify whether a database driver classpath must be specified in the Database Driver Classpath field to support a database connection.
- Specify the classpath for the database driver.
- Specify the name of the JDBC driver.
- Specify the connection string for the JDBC driver.
- Specify the user name that owns the tables inside the database.
- Specify the password for the user name that owns the tables inside the database.

You must restart the Content Server instance for any configuration changes to take effect.

8.6.1 About the Content Server System Database

Content Server uses an Oracle WebLogic Server data source to communicate with the system relational database where metadata and other information is stored. The Oracle WebLogic Server Administration Console must be used to manage the database connection information for the system relational database, therefore JDBC user name and password information is no longer stored in the `IntradocDir/config/config.cfg` file and it is *not* managed through the System Properties utility.

▲ Caution:

If you set database connection information for an Oracle WebLogic Server domain using the System Properties utility, the JDBC user name and password are encrypted and stored in an unspecified location.

Content Server supports GridLink data sources for connections to an Oracle Database relational database for an Oracle Real Application Cluster (RAC). For details, see *Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server* and *Oracle Fusion Middleware Administrator's Guide*.

For information on configuring database connections for a Content Server instance running applications in standalone mode, see:

- [Configuring a System Database Provider for Standalone Mode](#)
- [Configuring a JDBC Database Driver for Standalone Mode](#)
- [Configuring an External Database Provider for Standalone Mode](#)

8.6.2 Configuring Content Server for IBM DB2 Database Searches

An IBM DB2 database does not support the keyword `CONTAINS` in search queries. The correct configuration of the Content Server instance for IBM DB2 searches requires the addition of the flag `SSUseContains=false` variable. To configure the Content Server instance:

1. Open a new browser window, and log in to the Content Server instance as system administrator.
2. Choose **Administration**, then **Admin Server**, then **General Configuration**.
3. Add the following line in the Additional Configuration Variables area of the General Configuration page:

```
SSUseContains=false
```

4. Check that the variable `DatabasePreserveCase` is set to `true` (or `1`) in the `config.cfg` file. If the variable is not set to `true`, add `DatabasePreserveCase=true` to the Additional Configuration Variables area of the General Configuration page.
5. Click **Save**.
6. Restart the Content Server instance.

8.7 Configuring Oracle Content Management Integration Settings

Oracle Content Management integration with Content Server provides Oracle WebCenter Content users with the ability to store and retrieve documents in the Oracle Content Management cloud. It also allows users to copy content stored in the Content Server to Oracle Content Management cloud.

To configure Content Server to integrate with Oracle Content Management:

1. Enable the OracleDocumentsFolders component using the Component Manager. See [Enabling or Disabling a Component Using the Component Manager](#).

 **Note:**

Ensure that the FrameworkFolders component is enabled before enabling the OracleDocumentsFolders component.

2. Configure the Oracle Content Management connection information on the Oracle Content Management Integration Settings page.
 - a. Open a new browser window, and log in to the Content Server instance as system administrator.
 - b. Choose **Administration**, then **Oracle Content and Experience**. The **Oracle Content and Experience Integration Settings** page opens.
 - c. Enter the following details:
 - Oracle Content Management URL
 - Oracle Content Management User Name
 - Oracle Content Management Password
 - d. Select one of the following options from the **Select when cloud folders can be shared** drop-down list:
 - **Never**: To prevent sharing the cloud folder from the WebCenter Content user interface.
 - **Creation**: To enable sharing of a cloud folder when it is being created with only the folder owner's ODCS account. After the folder is created, it cannot be shared.
 - **Always**: To enable sharing of a cloud folder during and after its creation. A cloud folder can be shared during its creation with the owner's ODCS account, and after its creation, users who have access to the cloud folder can share it with their respective ODCS accounts
 - e. Click **Save**.

 **Note:**

You can test the Oracle Content Management Server connection settings by clicking the **Test** button.

You must restart the Content Server instance for any configuration changes to take effect.

3. Configure wildcard hostname verifier in Content Server using the Oracle WebLogic Server Administration Console.
 - a. On the Administration Console home page, in the Domain Configurations area choose **Environment**, then **Servers**.
 - b. On the **Configuration** tab for the Summary of Servers page, select the name of the WebCenter Content server for the Content Server instance.
 - c. Click the **SSL** sub-tab, and expand **Advanced**.
 - d. Configure the following settings:
 - i. In the Hostname Verification field, select Custom Hostname Verifier.
 - ii. In the Custom Hostname Verifier field, enter `weblogic.security.utils.SSWLSWildcardHostnameVerifier`.
 - iii. Click **Save**.

8.8 Configuring Server Properties

After WebCenter Content and a Content Server instance are deployed and an initial configuration specified, you can set or modify Content Server options using the Server tab on System Properties utility.

Note:

For security reasons, the Content Server Administration interface cannot be used to configure these options. You must start the System Properties utility as a standalone application from the computer where the Content Server instance is installed. The method required to start this program differs slightly between Windows and UNIX installations. For details, see [Running Administration Applications in Standalone Mode](#).

Using server options you can:

- Specify how the Content Server instance handles several language-specific issues such as the language of the user interface, stemming rules, sort order, and date/time format.
- Select the time zone in which the Content Server instance is located.
- Specify the instance name that is displayed in the Windows **Start** menu.
- Restrict access to the Content Server instance to computers with the specified IP address.
- Specify the password for the proxy.
- Specify whether internal JSP support is enabled in the Content Server instance.
- Specify the security groups that are enabled for internal JSP support.

You must restart the Content Server instance for any configuration changes to take effect.

▲ Caution:

If you do not use a Hostname filter, IP Address filter, or some other network-based security, you will have a security hole in your Content Server instance. For example, with no login, any user with in-depth knowledge of the system could create or modify any other user to have system administrator access.

Hostname filter or IP Address filter values must be set to allow communication with the Content Server instance in the following situations:

- Running Inbound Refinery and PDF Converter (even on the same physical computer as the Content Server instance).
- Transferring Content Server archives between computers.
- Configurations where the web server and the Content Server instance are on different systems.
- EJB-enhanced operations.
- Using the IdcCommand or IdcCommandX utilities on a system separate from the Content Server instance. (You must change the default value and specify the IP address of the web server.)

8.9 Configuring Localization Properties

After WebCenter Content and Content Server instance are deployed and an initial configuration specified, you can use the Localization tab on the System Properties utility to change language-specific items such as date/time format, default time zone, sort zone, and enabled interface languages.

You can use the Localization page to enable or disable locales for users to select in their User Profile.

- To access the System Properties: Localization tab, see [Running Administration Applications in Standalone Mode](#).
- To access the Localization page, on the Content Server portal choose **Administration**, then **Localization**.

8.9.1 Configuring Date Format

The default English-US locale uses two digits to represent the year (yy), where the year is interpreted to be between 1969 and 2068. In other words, 65 is considered to be 2065, not 1965. If you want years before 1969 to be interpreted correctly in the English-US locale, you must change the default date format for that locale to use four digits to represent years (yyyy).

This issue does not apply to the English-UK locale, which already uses four digits for the year.

To modify the default English-US data format:

1. Start the System Properties applet:
 - Windows: Choose **Start**, then **All Programs**, then **Content Server**, then **instance_name**, then **Utilities**, then **System Properties**.
 - UNIX: Run the System Properties utility, which is located in the `/bin` subdirectory of the Content Server installation directory:

```
./SystemProperties
```

2. Select the **Localization** tab.
3. Choose the **English-US** entry in the list of locales, and click **Edit**.
4. In the Configure Locale dialog, modify the date format to use four digits for the year (yyyy) rather than two (yy).
5. After you are done editing, click **OK** to close the Configure Locale dialog.
6. Click **OK** to apply the change and exit System Properties.
7. Restart the Content Server instance for configuration changes to take effect.

8.9.2 Configuring Interface Language

To add, edit, remove, enable, or disable interface languages for the Content Server instance:

1. Select a locale in the Localization tab of the System Properties utility using the same basic procedure described in [Configuring Date Format](#).
2. Make the interface language change, and click **OK**. Enabling a locale on the Localization tab also enables it on the Administration Localization page.

8.9.2.1 Specifying a Locale

Administrators can enable multiple locales so that users can select one of the enabled locales from their User Profile for their individual user interface language.

To specify what locales are enabled for users to select:

1. On the Content Server main page, choose **Administration**, then **Localization**.
2. Select the check boxes from the list of Enabled Locales to specify the languages.
3. Click **Update**.

8.10 Configuring Paths Properties

After WebCenter Content and a Content Server instance are deployed and initial configuration specified, you can use the Paths tab on the System Properties utility to:

- Modify the location of the browser executable that is used to display the online help from the standalone administration utilities and applications.
- Modify the path to the Java class files.
- Modify the path to the shared directory.

You must restart the Content Server instance for configuration changes to take effect.

Note:

For security reasons, the Content Server Administration interface cannot be used to configure these options. You must start the System Properties utility as a standalone application from the computer where the Content Server instance is installed. The method required to start this program differs slightly between Windows and UNIX installations. For details, see [Running Administration Applications in Standalone Mode](#).

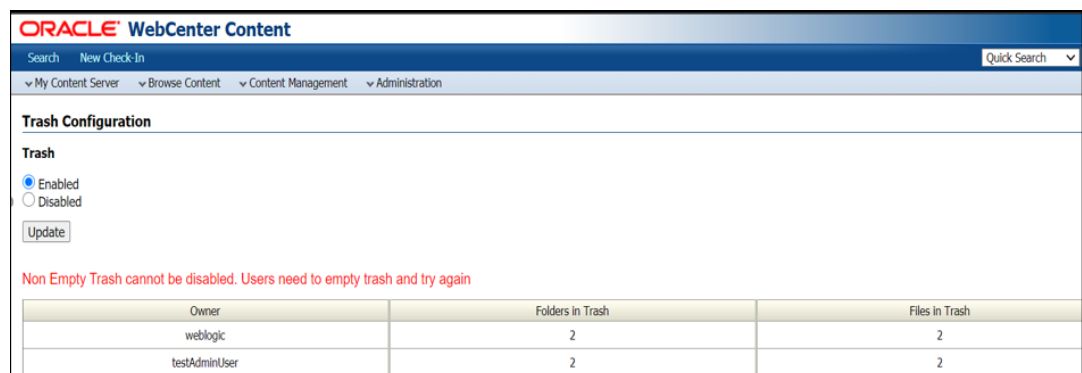
8.11 Configuring Trash

You can configure FrameworkFolders component in On-premise Oracle WebCenter Content to enable or disable trash. This feature is available to the users having Administrator access.

To toggle the trash feature:

1. Choose **Administration**, then **FrameworkFolders Configuration**, and then **Trash Configuration**.
2. The Trash Configuration page will appear. You can choose to **Disable** or **Enable** the trash feature. By default, the trash feature is enabled.
3. If you disable trash, the trash folder will no longer be available under the `/Users/<username>` hierarchy. Before you disable trash, the trash folder should be empty for all users in the system. If there is any content present in one of the user's trash, the system will not allow disabling trash. If you try to disable non-empty trash, the below screen will appear showing the content present in the trash folder.

Figure 8-1 Trash Configuration



ORACLE WebCenter Content

Search New Check-In Quick Search

My Content Server Browse Content Content Management Administration

Trash Configuration

Trash

Enabled
 Disabled

Update

Non Empty Trash cannot be disabled. Users need to empty trash and try again

Owner	Folders in Trash	Files in Trash
weblogic	2	2
testAdminUser	2	2

9

Managing Components

This chapter describes how to enable, disable, and upload system and custom Content Server components by using the Oracle WebCenter Content Component Manager, Fusion Middleware Control, and the Component Tool. It also describes how to create new Content Server components by using the Component Wizard.

This chapter includes the following topics:

- [About Components](#)
- [Using the Component Manager](#)
- [Managing Components Using Fusion Middleware Control](#)
- [Managing Components Using the Command Line](#)
- [Updating Component Configurations](#)
- [Creating Components Using the Component Wizard](#)

9.1 About Components

A component is a functional unit that can be plugged into the Content Server to provide additional features or to modify existing functionality. The primary use for components is to modify the user interface for existing pages and to alter behavior of existing services. Standard and system components are provided with the Content Server, and additional components can be acquired from the Oracle Technology Network. Administrators and developers can create their own custom components for their sites.

 **Note:**

For detailed information on the structure of and customizing components, see *Getting Started with Content Server Components* in *Developing with Oracle WebCenter Content*.

[Table 9-1](#) lists and briefly describes most standard and system Content Server components. Not all components are enabled by default. Detailed information about most components can be found in the WebCenter Content documentation set.

Table 9-1 Content Server Components

Component	Description
ActiveDirectoryLdapComponent	Enables the Content Server instance to authenticate users against an Active Directory server using LDAP. The provider also pulls in all group membership and specified user metadata from Active Directory.

Table 9-1 (Cont.) Content Server Components

Component	Description
AppAdapterCore	Provides Oracle business application attachments framework core functionality. It enables business application users to store and retrieve application business entity attached documents managed in the Content Server repository. Application-specific Content Server integration component(s) also need to be enabled for this component to function correctly. This component is a required part of the E-Business Suite Adapter for Oracle WebCenter Content (Managed Attachments Solution) and the PeopleSoft Adapter for Oracle WebCenter Content (Managed Attachments Solution).
AppAdapterEBS	Creates the E-Business Suite integration search results display page and the customization template required to enable the E-Business Suite Managed Attachments Solution. The AppAdapterCore component also needs to be enabled for this component to function correctly. This component is a required part of the E-Business Suite Adapter for Oracle WebCenter Content (Managed Attachments Solution).
AppAdapterPSFT	Creates the PeopleSoft integration search results display page and the customization template required to enable the PeopleSoft Managed Attachments Solution. The AppAdapterCore component also needs to be enabled for this component to function correctly. This component is a required part of the PeopleSoft Adapter for Oracle WebCenter Content (Managed Attachments Solution).
AppAdapterUniversal	This component is a required part of the Enterprise Application Adapter Framework solution for use with any business application. It contains the customizable UI layout, document profiles, and application field definitions. The AppAdapterCore component also needs to be enabled for this component to function correctly. NOTE: The Enterprise Application Adapter for Oracle WebCenter Content includes other required components that need to be installed on servers other than the Content Server.
ArchiveReplicationExceptions	Enables administrators to prevent failed imports from stopping replication by capturing failed imports and putting them into an exceptions archive, then sending email to the administrator that a failed import has occurred.
AutoSuggestConfig	Supports the WebCenter Content user interface. The AutoSuggestConfig component is valid only with the WebCenter Content user interface and not with the native interface. Disable this component if the system is not configured to support the WebCenter Content user interface. Note: The AutoSuggestConfig component is configurable. You can enable or disable this component based on your requirement.
BpelIntegration	Adds the ability to interact with Business Process Execution Language (BPEL) Process Manager from within Content Server workflows. Administrators can configure Content Server workflows to initiate a deployed process on the BPEL server.
BrowserUrlPath	Changes the computation of the Content Server variable <code>HttpBrowserFullCgiPath</code> and the function <code>proxiedBrowserFullCgiWebUrl()</code> so that they are no longer hardwired to a particular protocol. If the request comes in on port 443 (the SSL port), then the variable or function returns a result with HTTPS as the protocol. Otherwise, the variable or function returns a result with HTTP as the protocol.
CheckSCSHealth	Adds services used to check on the "health" of the search engine, providers, and the file system. These services are mainly useful when integrating Content Server with a third-party monitoring utility.
ClassifiedEnhancements	Allows DoD classified records requirements.
CommonUtils	Used by all records management feature levels.

Table 9-1 (Cont.) Content Server Components

Component	Description
ConfigMigrationUtility	Used to select elements of a Content Server instance to migrate to another Content Server instance.
ContentAccess-system	Performs standard "in place" conversion and filtering for the Content Server instance. It is used to create HTML renderings of native content, extract text for full text indexing, and extract links for link reference management. The specific component name depends on the type of <i>system</i> on which Content Server is installed.
ContentBasket	Enables users to select renditions of content items and place them in a personal storage space called the Content Basket. When this component is installed independently, renditions can be selected and placed in the Content Basket from either the Search Result or Content Information pages via the Actions menu on either page. Users can choose either native file or web-viewable renditions. When using Image Manager or Video Manager, additional rendition types can be selected for the Content Basket via Actions options on the Rendition Information page. Note: The Content Basket component is required when using either Image Manager or Video Manager.
ContentCategorizer	Suggests metadata values for documents being checked in to the Content Server instance, and it can be used to recategorize the metadata of documents that are already in. Metadata values are determined according to search rules provided by the administrator.
ContentFolios	Provides a quick and effective way to assemble, track, and access logical groupings of multiple content items from within the secure environment of the Content Server instance. For example, this component can be used to set up a new project that requires a virtual place to assemble all relevant content items in a particular hierarchy, whenever they are checked in, with restricted access to particular areas of the hierarchy.
ContentPortletSuiteBundle	Provides portlets used to manage the content creation and distribution process. Portlet support is provided for BEA WebLogic, Plumtree, and Sun ONE portal servers.
ContentTracker	Monitors activity on the Content Server instance and records selected details of those activities. It then generates reports that can help administrators understand the ways in which the system is being used.
CoreWebdav	Provides a way to remotely author and manage content in the Content Server repository using clients that support the WebDAV protocol.
DAMConverterSupport	Enables Inbound Refinery to create multiple packaged (zipped) renditions of a checked-in graphic file. The ZipRenditionManagement system component can be used to access the renditions created by the refinery.
DBSearchContainsOpSupport	Adds support of hasAsWord(Contains) operator to DATABASE and DATABASEFULLTEXT on SQL Server, Oracle, and DB2 databases.
DesktopIntegrationSuite	Provides a set of embedded applications that help administrators seamlessly integrate the desktop experience with the Content Server. It provides convenient access to the Content Server from Microsoft Windows Explorer, desktop applications like Microsoft Word and Excel, and email clients like Microsoft Outlook and Lotus Notes.
DesktopTag	Modifies documents supported by the CleanContent component by maintaining a set of custom properties in the documents. These properties are used by the Desktop Integration Suite Microsoft Office integrations to aid in using files with the Content Server.

Table 9-1 (Cont.) Content Server Components

Component	Description
DigitalAssetManager	Enables users to define and provide images and videos in specified formats and sizes for download. The component creates multiple formats of digital assets automatically when an image or video is checked in to the Content Server, and lists the formats under one content ID.
DodConfig	Provides functionality for configuring DoD requirements.
DynamicConverter	Converts a document into a web page for everyone to see without use of the application used to create that document.
ElectronicSignatures	Supports the creation and management of Electronic Signatures for managed content objects. The component is loosely integrated with Oracle WebCenter Content Workflow.
EmailMetadata	Extracts information from Microsoft Outlook messages (MSG) and Internet Mail Messages (EML), and populates email specific fields in the Content Server. This process occurs when users check in files using the Content Server Contribution Folders functionality in Microsoft Outlook, Lotus Notes, or Windows Explorer. This also occurs when checking in MSG or EML files using the web browser interface.
ExtendedUserAttributes	Enables administrators to add extended security attributes to Content Server users. The extended security attributes are merged into pre-existing user attributes and enable additional flexibility in managing users.
ExtranetLook	Enables customization of the out-of-box Oracle WebCenter Content default behavior for anonymous users. Anonymous users will be restricted in access to key pages and have reduced experience when visiting those pages
FileStoreProvider	Enables the Content Server to have more control over how files are stored. Files can either be stored in the database or on the file system. The component has extension options where you can write components that store files in other types of storage repositories. When files are stored on the file system, the component allows additional flexibility in path computations. For web-viewable paths, the types of paths allowed are restricted.
FoldersStructureArchive	Enables administrators to configure a Content Server Archive to archive the Contribution Folder structure as well as its associated content. The structure of the Contribution Folders is archived using database table replication.
FormEditor	Provides system functionality to process <code>hcsw</code> files into <code>hcsf</code> files.
FrameworkFolders	Provides a hierarchical folder interface, similar to a conventional file system, for organizing and locating some or all of the content in the Content Server repository.
Imaging	Acts as the interface for any IPM Documents checked into Content Server and tools such as ADF Viewer use functionality and services provided by this component.
IpmRepository	Adds functionality to the content server to allow Oracle WebCenter Content: Imaging to store documents and metadata in the content server.
InboundRefinerySupport	Allows the Content Server to use Inbound Refinery for the conversion of files. Without this component the Content Server cannot use Inbound Refinery.
iTextComponent	Provides an iText library that allows components to create and manipulate PDF documents
JpsUserProvider	Enables integration with the Oracle Java Platform Security (JPS) framework.
LinkManager	Extracts URL links of indexed documents, evaluates, filters and parses the URLs according to a pattern engine, and then stores the results in a database table. Because the link extraction occurs during the indexing cycle, only the links of released documents are managed.

Table 9-1 (Cont.) Content Server Components

Component	Description
Localization	Contains localizations for Content Server, Inbound Refinery, Records, and a number of other components. Allows administrator to control Locales that are enabled on Content Server.
MetadataSet	Provides functionality to create additional custom metadata that can store additional auxiliary information outside of DocMeta table. Auxiliary metadata is often associated with different but specific properties of the item it represents, such as a image size, video file length, or the character encoding of a document. The same Auxiliary metadata set UI is used for creating, editing, and deleting custom fields of Retention Category, Retention Folders, and Physical Content.
MsofficeHtmlConverterSupport	Enables the Content Server and Inbound Refinery to convert select Microsoft Office formats to HTML using the native application.
NativeOsUtils	(Required) Provides the native JNI calls needed by the Content Server instance. The Content Server can run without this component enabled, but it loses some functionality. The two noticeable degradations are as follows: <ul style="list-style-type: none"> • In schema publishing, all files are rewritten instead of using hard links to have new files link back to existing files when the content does not change. • When a component is installed that has native executables, the executable bit on the files is not toggled properly. This can affect components such as ContentAccess.
OCM	Collects the list of components that are enabled and disabled in the Content Server instance and provides the data to the Configuration Manager.
OracleAdvancedSecurityConfig	Handles all the security configurations. This component is enabled by default along with the other security features. It also adds a database table to the schema to maintain the state of security configuration flags.
OpssPolicyStore	Integrates Content Server with OPSS policy store.
OracleCleanContent	Contains clean content libraries and generates descriptions of the documents for use by the DesktopTag component.
OracleDocumentsFolders	Enables Content Server to seamlessly integrate with OCE. It allows users to store and retrieve documents stored in OCE. It also provides the ability to copy content stored in the Content Server to OCE. Note: Make sure that the FrameworkFolders component is enabled before enabling this component.
OracleLocalization	Enables Content Server to parse, sort, and format date, number, and decimal in locally sensitive way.
OracleQueryOptimizer	Aids in tuning queries against the Oracle database by allowing query hints to be added to ensure that the best execution plan is used.
PDFWatermark	Enables watermarks to be applied to PDF files generated by the Inbound Refinery PDFConverter component and returned to the Content Server. PDF files already residing on the Content Server also can be watermarked. Dynamic watermarks are generated on-the-fly and can contain variable information.
PopUpCalendar	Causes a calendar icon to be opened to the right of all date fields on the Content Server's check-in and update pages. Clicking the icon pops up a calendar window where the user can click a date to select it. The calendar loads the selected date into the associated input field on the parent page. May also be configured to open the dialog using JavaScript without opening a window.

Table 9-1 (Cont.) Content Server Components

Component	Description
ProxyConnections	Provides the capability to perform archive replication of content items over HTTP or HTTPS. Enables better restriction of access to Content Server instances by using named passwords to target master server proxy connections. Provides a user interface for creating password-protected connections to a Content Server instance or for creating credential maps.
RecordsManagement	Provides core records management functionality.
RelatedContent	Provides various ways to link or relate documents. For example: It allows documents to be related as Peer-to-Peer (Renditions), Chained List (Supersedes), Parent-Child (Supporting Content), Cross Reference link (Cross Reference).
ReportPublisher	Generates reports using Oracle BI Publisher.
RetentionManager	Contains configurations for Records Management on Oracle Content Server.
RmaEmail	Provides functionality to manage email records.
RMFeatureConfig	Used to select various records management feature level.
RoleEntityACL	Integrates Content Server with OPSS access control list permissions. Ensure that the role names are either under 30 characters in length or are unique within the first 30 characters.
SecurityProviders	Provides Secure Sockets Layer (SSL) encryption and authentication on the Content Server incoming and outgoing socket providers.
SiebelECMIntegration	Part of Siebel Adapter for Oracle WebCenter Content that enables Siebel CRM users to store and retrieve attachments stored in a Content Server repository.
SiebelFilter	An optional part of the Siebel Adapter for Enterprise Content Management. It enables filtering of the attachments list based on metadata such as Document Type, Author, and security Group.
SiebelIntegrationSearchDisplay	Displays Oracle WebCenter Content documents as managed attachments to Siebel entities in an iFrame within the Siebel application.
SiebelSearchExtensions	Determines whether documents not yet released are displayed in the Siebel attachments list. If enabled, all documents in the system are displayed, including those waiting to be indexed, in the Inbound Refinery conversion process, or in workflow. If not enabled, only released documents are displayed in the Siebel attachments list. This component is an optional part of the Siebel Adapter for Oracle WebCenter Content. NOTE: This feature is available only when Metadata Only Search is configured on the Content Server instance.
SiebelSearchExtraParams	Enables the passing of additional Siebel metadata values to the Content Server Siebel Adapter components. If enabled, the configured extra Siebel parameters are added as metadata settings on the New or Scan attachment forms. This component is an optional part of the Siebel Adapter for Oracle WebCenter Content.
SiteStudio	A powerful, flexible web development application suite that offers a comprehensive approach to designing, building, and maintaining enterprise-scale websites. It offers both website creation and content management.
SiteStudioExternalApplications	Extends Site Studio functionality in a website environment where the application server or website is disconnected from the Content Server instance. Also provides functionality for reuse of SiteStudio files in other application environments through support of the VCR services.
SiteStudioPublisher	Provides functionality to build static copies of Site Studio websites and deploy them to a "live" location.

Table 9-1 (Cont.) Content Server Components

Component	Description
TaskPanel	A dashboard for an administrator and users to organize their tasks and information in one place so that they can access actions and information quickly and efficiently from one place.
ThreadedDiscussions	Enables the ability to create discussion documents about another document. It takes any content item and adds "_d" to the document ID to create a new hcsp style document that is focused on discussion about the originating document.
TiffConverterSupport	Enables Content Server and Inbound Refinery to convert tiff files to searchable PDF files.
UIEnhancements	Utility component required for records management component.
UrmAgent	The communications intermediary between Oracle WebCenter Content: Records and the Content Server repository. Content is stored in and remains in the Adapter server's content vault while Oracle WebCenter Content: Records server simultaneously enforces corporate retention policies, disposition processes, and legal holds on the stored content.
UserProfileSchemaLoader	Loads user profiles as a schema view.
WebCenterConfigure	Used to configure the Content Server instance by setting necessary configuration parameters and enabling WebCenter required components.
WebUrlMapPlugin	Enables mapping of URLs to other URLs in the Content Server using a simple substitution script for the mapping.
WsdIGenerator	Provides web services integration technologies to access the functionality of Content Server.
XMLConverterSupport	Enables Content Server and Inbound Refinery to convert various formats to FlexionDoc or SearchML as either the primary web rendition or an additional rendition. It also enables the Content Server and Inbound Refinery to perform XSLT transformations.
YahooUserInterfaceLibrary	(Required) Provides a wrapper for the Yahoo! User Interface Library (YUI) available under the BSD license. The Content Server adopted the YUI library for its user interface implementation because of its ability to implement folder move operations (move an item from one folder to another) and for its support of Accessibility (specifically keyboard operations). The YUI library is also used for its calendar control and its ability to support popup choice lists in type-ahead fields.

9.2 Using the Component Manager

This section describes the tasks you can perform with the Component Manager to manage Content Server and custom components.

- [Viewing Information about a Component Using the Component Manager](#)
- [Enabling or Disabling a Component Using the Component Manager](#)
- [Installing a Component Using the Component Manager](#)
- [Uninstalling a Component Using the Component Manager](#)
- [Downloading a Component Using the Component Manager](#)
- [Modifying a Component Configuration Using the Component Manager](#)

9.2.1 Viewing Information about a Component Using the Component Manager

To view a basic description of a component:

1. In the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager**.

The Component Manager page opens with a list of component categories and a list of component names

2. Select the category **All Components**.
3. On the Component Manager page, hover the cursor over the name of a component in the list of components.

A description is displayed in a window, whether or not the component is selected.

To view detailed information about a component:

1. In the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager**.

The Component Manager page opens with a list of component categories and a list of component names with brief descriptions.

2. On the Component Manager page, in the first paragraph click the underlined text **advanced component manager**.
3. On the Advanced Component Manager page, select a component name either in the list of **Enabled Components** or **Disabled Components**.

Information about the component is displayed in a pane next to the list, including component name, description, tags, location, feature extension, and more.

9.2.2 Enabling or Disabling a Component Using the Component Manager

To enable or disable a component:

1. In the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager**.

2. On the Component Manager page, select **All Components**.

All components from the Document Management, Folders, Inbound Refinery, Integration, and Web Content Management categories are listed.

3. Select the check box for the component you want to enable.

Deselect the check box for the component you want to disable.

If you do not see the component, verify that the appropriate filter check boxes are selected so the components are displayed. If you do not want to make the changes you selected, click **Reset**.

4. Click **Update**.

5. Restart the Content Server instance. This step is required for changes to take effect. For instructions on restarting the instance, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

The Content Server instance restarts, and the component is now enabled or disabled.

 **Note:**

When the Content Server instance is started, enabled components are loaded in the order shown in the Components list.

6. Navigate to the pages affected by the component to ensure that the addition or removal of the customization is working as you expected.

 **Note:**

Components also can be enabled or disabled using the Advanced Component Management page.

9.2.3 Installing a Component Using the Component Manager

To install a component:

 **Tip:**

Components can also be unpackaged using the Component Wizard. For details, see [Creating Components Using the Component Wizard](#).

1. In the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager**.
3. On the Advanced Component Manager page, click the **Browse** button next to the **Install New Component** field.
4. Navigate to and select the component zip file.
5. Click **Open**.

The path and file name appear in the **Install New Component** field.

6. Click **Install**.

The component files are unpackaged on the Content Server instance, and the name of the component appears in the Disabled Components list.

 **Note:**

Installing a component does not enable it; the component must be enabled. For details, see [Enabling or Disabling a Component Using the Component Manager](#).

7. If you are having difficulty uploading the component, check the Content Server output messages by selection **Administration**, then **System Audit Information**. Click **View Server Output** to see recent server actions.

9.2.4 Uninstalling a Component Using the Component Manager

To uninstall a component:

 **Tip:**

Components can also be uploaded (unpackaged) using the Component Wizard. For details, see [Creating Components Using the Component Wizard](#).

1. On the Content Server portal, choose **Administration**, then **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager**.
3. On the Advanced Component Manager page, choose a component from the **Uninstall Component** field menu.
4. With the component name to be uninstalled displayed in the **Uninstall Component** field, click **Uninstall**.

9.2.5 Downloading a Component Using the Component Manager

A component cannot be downloaded unless it meets these requirements:

- The component must exist outside of the `MW_HOME/WC_CONTENT_ORACLE_HOME/ucm/idc/system/` directory. This excludes all shipped components unless a patch has been uploaded to a component. The component must have a zip file with the appropriate name, located inside the component directory. Usually this occurs only when the component has been uploaded or installed manually.

To download a component:

1. In the WebCenter Content portal, choose **Administration**, then **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager**.
3. On the Advanced Component Manager page, select the component to be packaged from the **Download Component** field menu.
4. Click **Download**.
5. In the File Download window, select the **Save this file to disk** option and click **OK**.
6. In the Save As window, navigate to the directory where you want to save the component zip file.
7. Change the name of the component zip file as necessary.
8. Click **Save**.

The component is saved as a component zip file.

9.2.6 Modifying a Component Configuration Using the Component Manager

Several methods are available for modifying, or updating, the configuration of a component after it is installed.



Note:

Not all components can have their configuration changed.

9.2.6.1 Modifying a Component Using Component Manager

The Component Manager allows you to modify a component.

To modify a component using the Component Manager:

1. Choose **Administration**, then **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager**.
3. On the Advanced Component Manager page, select a component name from the **Update Component Configuration** field menu, then click **Update**.

The Update Component Configuration window for the component opens. The listed component parameters are those defined as being editable after the component is installed.

4. When you have finished modifying the component configuration, click **Update**. The Content Server instance does *not* need to be restarted.

9.2.6.2 Modifying a Component Using the Configuration for instance Page

The Configuration for instance Page allows you to modify a component.

To modify a component using the Configuration for instance page:

1. Choose **Administration**, then **Configuration for instance**.
2. Click **Enabled Components Details**.
3. Click **Configure** next to the name of the component to be configured.
 - If the component can be configured, the Update Component Configuration window for the component opens.
 - If the component cannot be configured, a message opens.
4. When you have finished modifying the component configuration, click **Update**. The Content Server instance does *not* need to be restarted.

9.3 Managing Components Using Fusion Middleware Control

This section describes the tasks you can perform with the Component Manager and Advanced Component Manager to manage WebCenter Content Server system and custom components using the Enterprise Manager Fusion Middleware Control interface:

- [Using the Component Manager](#)

- [Using the Advanced Component Manager](#)

9.3.1 Using the Component Manager

You can use Fusion Middleware Control to view and enable or disable components with the WebCenter Content Server Component Manager.

- [Viewing Component Information Using Fusion Middleware Control](#)
- [Enabling or Disabling a Component Using Fusion Middleware Control](#)

9.3.1.1 Viewing Component Information Using Fusion Middleware Control

You can view either basic information or detailed information about a component using Fusion Middleware Control.

9.3.1.1.1 Viewing basic information about a component

To view a basic description of a component:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).

The home page for your WebCenter Content Server instance appears.

4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Component Manager**.

The Component Manager page opens with a list of component categories and a list of component names.

5. On the Component Manager page, select the category **All Components**.
6. On the Component Manager page, hover the cursor over the name of a component in the list of components.

A description is displayed in a window, whether or not the component is selected.

9.3.1.1.2 Viewing detailed information about a component

To view detailed information about a component:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).

The home page for your WebCenter Content Server instance appears.

4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Advanced Component Manager**.

5. On the Advanced Component Manager page, select a component name either in the list of Enabled Components or Disabled Components.

Information about the component is displayed in a pane next to the list, including component name, description, tags, location, feature extension, and more.

9.3.1.2 Enabling or Disabling a Component Using Fusion Middleware Control

To enable or disable a component:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).

The home page for your WebCenter Content Server instance appears.

4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Component Manager**.
5. On the Component Manager page, select **All Components**.

All components from the Document Management, Folders, Inbound Refinery, Integration, and Web Content Management categories are listed.

6. Select the check box for the component you want to enable.

Deselect the check box for the component you want to disable.

If you do not see the component, verify that the appropriate filter check boxes are selected so the components are displayed. If you do not want to make the changes you selected, click **Revert**.

7. Click **Apply**.
8. Restart the WebCenter Content Server instance. This step is required for changes to take effect. For instructions on restarting the instance, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

 **Note:**

When the WebCenter Content Server instance is started, enabled components are loaded in the order shown in the Components list.

9. Navigate to the pages affected by the component to ensure that the addition or removal of the component is working as you expected.

 **Note:**

Components also can be enabled or disabled using the Advanced Component Management page.

9.3.2 Using the Advanced Component Manager

You can use Fusion Middleware Control to enable or disable, install or uninstall, download, and modify system and custom components with the WebCenter Content Server Component Manager.

- [Enabling or Disabling a Component Using Fusion Middleware Control](#)
- [Installing a Component Using Fusion Middleware Control](#)
- [Uninstalling a Component Using Fusion Middleware Control](#)
- [Downloading a Component Using Fusion Middleware Control](#)
- [Modifying a Component Configuration Using Fusion Middleware Control](#)

9.3.2.1 Enabling or Disabling a Component Using Fusion Middleware Control

To enable or disable a component:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
The home page for your WebCenter Content Server instance appears.
4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Advanced Component Manager**.
5. Select the Category Filter to display relevant components: standard, custom, and system.
6. For Additional Filtering, select **All Components**.
All components from the Document Management, Folders, Inbound Refinery, Integration, and Web Content Management categories are listed.
7. To view information about an enabled component, select the component name in the **Enabled Components** list.
8. To disable an enabled component, select the component name in the **Enabled Components** list, then click **Disable**.
9. To view information about a disabled component, select the component name in the **Disabled Components** list.
10. To enable a disabled component, select the component name in the **Disabled Components** list, then click **Enable**.
11. Restart the WebCenter Content Server instance. This step is required for changes to take effect. For instructions on restarting the instance, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

 **Note:**

When the WebCenter Content Server instance is started, enabled components are loaded in the order shown in the Components list.

12. Navigate to the pages affected by the component to ensure that the addition or removal of the component is working as you expected.

9.3.2.2 Installing a Component Using Fusion Middleware Control

To install a component:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).

The home page for your WebCenter Content Server instance appears.

4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Advanced Component Manager**.
5. On the Advanced Component Manager page, click the **Browse** button next to the **Install Component** field.
6. Navigate to and select the component zip file.
7. Click **Open**.

The path and file name appear in the **Install Component** field.

8. Click **Install**.

The component files are unpackaged in the WebCenter Content Server instance, and the name of the component appears in the **Disabled Components** list.

9. Restart the WebCenter Content Server instance. This step is required for changes to take effect. For instructions on restarting the instance, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).
10. If you are having difficulty installing the component, check the WebCenter Content Server output messages by clicking the **View Admin Output** link in the menu.

The Server Output page opens where you can verify the recent actions.

9.3.2.3 Uninstalling a Component Using Fusion Middleware Control

To uninstall a component:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`). The home page for your WebCenter Content Server instance appears.
4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Advanced Component Manager**.
5. On the Advanced Component Manager page, choose a component from the **Uninstall Component** field menu.

6. With the component name to be uninstalled displayed in the **Uninstall Component** field, click **Uninstall**.
7. Restart the WebCenter Content Server instance. This step is required for changes to take effect. For instructions on restarting the instance, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

9.3.2.4 Downloading a Component Using Fusion Middleware Control

A component cannot be downloaded unless it meets these requirements:

- The component must exist outside of the `MW_HOME/WC_CONTENT_ORACLE_HOME/ucm/idc/system/` directory. This excludes all shipped components unless a patch has been uploaded to a component. The component must have a zip file with the appropriate name, located inside the component directory. Usually this occurs only when the component has been uploaded or installed manually.

To download a component:

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).
2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).

The home page for your WebCenter Content Server instance appears.

4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Advanced Component Manager**.
5. On the Advanced Component Manager page, select the component to be packaged from the **Download Component** field menu.
6. Click **Download**.
7. In the File Download window, select the **Save this file to disk** option and click **OK**.
8. In the Save As window, navigate to the directory where you want to save the component zip file.
9. Change the name of the component zip file as necessary.
10. Click **Save**.

The component is saved as a component zip file.

9.3.2.5 Modifying a Component Configuration Using Fusion Middleware Control

To modify or update the configuration of a component after it is installed:



Note:

Not all components can have their configuration changed.

1. When you are logged in to Enterprise Manager Fusion Middleware Control, in the navigation tree expand the appropriate domain name (for example, `Content_base_domain`).

2. Expand **WebCenter**, then **Content**, then **Content Server**.
3. Select the WebCenter Content Server instance name (for example, `Oracle WebCenter Content - Content Server (UCM_server1)`).
The home page for your WebCenter Content Server instance appears.
4. On the WebCenter Content Server home page, from the **Content Server** menu choose **Configuration Pages**, then **Advanced Component Manager**.
5. On the Advanced Component Manager page, select a component name from the **Update Component Configuration** field menu, then click **Update**.
The Update Component Configuration window for the component opens with configuration selections specific to the component. The listed component parameters are those defined as being editable after the component is installed.
6. When you have finished modifying the component configuration, click **OK**. The WebCenter Content Server instance does *not* need to be restarted.
If you do not want to update the component configuration, click **Cancel**.

9.4 Managing Components Using the Command Line

The ComponentTool component enables administrators to use a command line to install, enable, and disable components in the Content Server instance. ComponentTool is installed (enabled) with the Content Server instance.

When Content Server is deployed, the ComponentTool launcher is installed by default for UNIX and Windows. The executable is located in the `DomainHome/ucm/cs/bin/` directory.

Windows

`ComponentTool.exe`

UNIX

`ComponentTool`

Component Tool supports the commands listed in [Table 9-2](#).

Table 9-2 Component Tool Commands

Task	Command
Install a component (also automatically enables the component)	<code>ComponentTool --install path/component_name</code>
Enable a component	<code>ComponentTool --enable component_name</code>
Disable a component	<code>ComponentTool --disable component_name</code>
List enabled components	<code>ComponentTool --list-enabled</code>
List disabled components	<code>ComponentTool --list-disabled</code>
List all components	<code>ComponentTool --list</code>
Access ComponentTool help	<code>ComponentTool --help</code>

9.5 Updating Component Configurations

You can update, or modify, the configuration of some Content Server components with the Advanced Component Manager or the Configure for Instance screen, whether the component is enabled or disabled. The Advanced Component Manager shows a list of the components whose configuration you can modify in the Update component configuration field. From the Configure for Instance screen, the Update Component Configuration screen opens for the selected component.

Not all components can have their configuration settings modified. If a component does not support modifying configuration settings using the Update Component Configuration page, a message appears.

Content Server has Update Component Configuration pages for these components:

- [Updating ContentTracker Component Configuration](#)
- [Updating DesktopIntegrationSuite Component Configuration](#)
- [Updating EmailMetadata Component Configuration](#)
- [Updating OCM Component Configuration](#)
- [Updating PDFWatermark Component Configuration](#)
- [Updating SiteStudio Component Configuration](#)

9.5.1 Updating ContentTracker Component Configuration

You can update configuration settings for the Content Tracker component with the Advanced Component Manager or the Configure for Instance screen, whether the component is enabled or disabled.

To update the configuration using the Advanced Component Manager:

1. Choose **Administration** from the Content Server tray or menu, then choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager** and choose **ContentTracker** from the **Update Component Configuration** list.
3. Click **Update**.

The Update Component Configuration page appears.

4. If the component is not enabled, look at the **Disabled Components** list to find the name of the component to configure, then select the component name and click **Enable**.
5. Make your configuration changes, then click **Update**.
If you want to cancel your changes, click **Reset**.
If you want to change the settings to their original configuration, click **Revert to Install Settings**.
6. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

**Note:**

You must restart the Content Server instance after making any component configuration change.

Element	Description
Track Content Access Only	If selected, specifies to track content access only. By default, the check box is selected.
Do Not Populate Access Log Columns	Specifies the access log columns to not populate.
Simplify User Agent String	If selected, simplifies the user agent string. By default, the check box is selected.
Maximum Days to Retain Data	Specifies the maximum number of days that data is retained. The default setting is 60.
Do Not Archive Expired Data	If selected, specifies to not archive expired data. By default, the check box is selected.
Enter Maximum URL Length	Enter the maximum number of characters for the length of URLs. The default setting is 3000.
Enter Maximum Proxy Name Length	Enter the maximum number of characters for the length of a proxy name. The default setting is 50.
Post Reduction Executable	Specifies a post-reduction executable. There is no default.
Web Beacon ID List	Specifies a list of web beacon IDs.

9.5.2 Updating DesktopIntegrationSuite Component Configuration

You can update configuration settings for the DesktopIntegrationSuite component with the Advanced Component Manager or the Configure for Instance screen, whether the component is enabled or disabled. DesktopIntegrationSuite handles core content management integration functions on the server.

To update configuration settings using the Advanced Component Manager:

1. Choose **Administration** from the Content Server tray or menu, then choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager** and choose **DesktopIntegrationSuite** from the **Update Component Configuration** list.
3. Click **Update**.
The Update Component Configuration page appears
4. If the component is not enabled, look at the **Disabled Components** list to find the name of the component to configure, then select the component name and click **Enable**.
5. Make your configuration changes, then click **Update**.
If you want to cancel your changes, click **Reset**.
If you want to change the settings to their original configuration, click **Revert to Install Settings**.
6. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

**Note:**

You must restart the Content Server instance after making any component configuration change.

Element	Description
Enable web browser search plug-in	If selected, allows users to add a web browser search provider for this content server instance. This enables them to perform a quick search on the server in their browser without going through the content server web interface.
Web browser search plug-in title	Search engine name for this content server instance as displayed in client web browsers. Make sure this name is unique across the enterprise.
Check-in dialog comment metadata field name	Name of the comments metadata field on this content server instance. The default is <code>xComments</code> .
Check-in dialog default comment	Default comment that is displayed in the check-in comment and close dialogs of Microsoft Office applications.
Check-in dialog comment service	Service to call to obtain the default check-in comment for Microsoft Office documents as they are checked out of the content server. If you leave this field empty, no service is called and the default comment specified above is used. Enter <code>DOC_INFO</code> to use the <code>xComment</code> value from the previous revision as the default check-in comment.
Maximum check-in dialog comment length	Maximum number of characters for comments in the check-in dialog of Microsoft Office applications on client computers. If you leave this field blank, then the limit is set by the maximum text length of the metadata field.

9.5.2.1 Configuring Windows Explorer Preview Pane

In the Desktop Integration Suite (DIS) environment, for documents with rendition information, you can configure the Windows Explorer to display either the actual image along with its data or the rendition page in the document preview pane instead of the default `DOC_INFO` page by configuring the `DISDefaultDocInfoTab` property.

To configure `DISDefaultDocInfoTab` property, open the `desktopintegrationsuite_environment.cfg` file and enter one of the following values:

- `DISDefaultDocInfoTab = IMAGE_DATA`: Set this value to configure the Windows Explorer preview pane to display the document image data page
- `DISDefaultDocInfoTab = RENDITION_INFO`: Set this value to configure the Windows Explorer preview pane to display the document rendition information page

9.5.3 Updating EmailMetadata Component Configuration

You can update the configuration for the EmailMetadata component with the Advanced Component Manager or the Configure for Instance screen, whether the component is enabled or disabled. The EmailMetadata component maps email message fields to email metadata fields and is also required for dragging and dropping email into content folders in Microsoft Outlook and Lotus Notes.

For example, to have the title always be the subject line and the file name be the message ID or UUID, first uncheck (set to false) the following settings:

- Always set content item title to e-mail subject line
- Always set content item file name to e-mail subject line
- Set file name to email subject line if title identical to file name

Then check (set to true) the following option: `Set title to e-mail subject line if identical to file name.`

To ensure that both the title and the file name are the message ID or UUID, uncheck (set to false) all the check boxes.

To update the configuration using the Advanced Component Manager:

1. Choose **Administration** from the Content Server tray or menu, then choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager** and choose **EmailMetadata** from the **Update Component Configuration** list.
3. Click **Update**.

The Update Component Configuration page appears.

4. If the component is not enabled, look at the **Disabled Components** list to find the name of the component to configure, then select the component name and click **Enable**.
5. Make your configuration changes, then click **Update**.

If you want to cancel your changes, click **Reset**.

If you want to change the settings to their original configuration, click **Revert to Install Settings**.

6. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).



Note:

You must restart the Content Server instance after making any component configuration change.

Element	Description
Show e-mail metadata mapping menu	If selected, the Configure Email Metadata menu option is displayed in the Administration tray or menu of the content server.
Always set content item title to e-mail subject line	If selected, the title of the checked-in content item is the subject line of the email message. Otherwise, the title will be the email message ID (for received messages, as retrieved from the header) or UUID (for drafts or sent messages), unless it is changed to the subject line based on the next configuration setting.
Set title to e-mail subject line if identical to file name	If selected, the title is set to the email subject line if the title is identical to the file name (without the file extension). Otherwise, the title will not be changed.

Element	Description
Always set content item file name to e-mail subject line	If selected, the file name of the checked-in content item is always the subject line of the email message. Otherwise, the file name will be the email message ID (for received messages, as retrieved from the header) or UUID (for drafts or sent messages), unless it is changed to the subject line based on the next configuration setting.
Set file name to e-mail subject line if title identical to file name	If selected, the file name is set to the email subject line if the title is identical to the file name (without the file extension). Otherwise, the file name will not be changed.
E-mail address separator	Character that separates the email addresses in messages sent to multiple recipients. The default is a semicolon.
Encoding for non-Unicode e-mail messages	Encoding for non-Unicode email messages. The default is the Java Virtual Machine default for the system running this content server instance (which is locale-dependent). You can also specify a different encoding as defined in the Java specification (typically, US-ASCII, ISO-8859-1, or UTF-8).
Encoding for Unicode e-mail messages	Encoding for Unicode email messages. The default is UTF-16LE.

9.5.4 Updating OCM Component Configuration

You can update configuration settings for the OCM component with the Advanced Component Manager or the Configure for Instance screen, whether the component is enabled or disabled. The OCM component collects the list of components that are enabled and disabled in the Content Server instance and provides the data to the Configuration Manager.

To update the configuration using the Advanced Component Manager:

1. Choose **Administration** from the Content Server tray or menu, then choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager** and choose **OCM** from the **Update Component Configuration** list.
3. Click **Update**.
The Update Component Configuration page appears.
4. If the component is not enabled, look at the **Disabled Components** list to find the name of the component to configure, then select the component name and click **Enable**.
5. Make your configuration changes, then click **Update**.
If you want to cancel your changes, click **Reset**.
If you want to change the settings to their original configuration, click **Revert to Install Settings**.
6. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

**Note:**

You must restart the Content Server instance after making any component configuration change.

Element	Description
Admin User ID	Admin user ID used by OCM when extracting component configuration. It must be a <i>local</i> Content Server admin user. Default: <code>sysadmin</code>

9.5.5 Updating PDFWatermark Component Configuration

You can update configuration setting for the PDFWatermark component with the Advanced Component Manager or the Configure for Instance screen, whether the component is enabled or disabled.

To update the configuration using the Advanced Component Manager:

1. Choose **Administration** from the Content Server tray or menu, then choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager** and choose **PDFWatermark** from the **Update Component Configuration** list.

3. Click **Update**.

The Update Component Configuration page appears.

4. If the component is not enabled, look at the **Disabled Components** list to find the name of the component to configure, then select the component name and click **Enable**.
5. Make your configuration changes, then click **Update**.

If you want to cancel your changes, click **Reset**.

If you want to change the settings to their original configuration, click **Revert to Install Settings**.

6. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).

**Note:**

You must restart the Content Server instance after making any component configuration change.

Element	Description
Use PDF optimizer	If selected, specifies to use PDF optimizer. By default, the check box is not selected.
Optimizer Command Line Template	Optimizer command line template.

9.5.6 Updating SiteStudio Component Configuration

You can update configuration settings for the Site Studio component with the Advanced Component Manager or the Configure for Instance screen, whether the component is enabled or disabled.

To update the configuration using the Advanced Component Manager:

1. Choose **Administration** from the Content Server tray or menu, then choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page, click **advanced component manager** and choose **SiteStudio** from the **Update Component Configuration** list.
3. Click **Update**.

The Update Component Configuration page appears.

4. If the component is not enabled, look at the **Disabled Components** list to find the name of the component to configure, then select the component name and click **Enable**.
5. Make your configuration changes, then click **Update**.

If you want to cancel your changes, click **Reset**.

If you want to change the settings to their original configuration, click **Revert to Install Settings**.

6. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).



Note:

You must restart the Content Server instance after making any component configuration change.

Element	Description
Fragment Library Content Type	Content type to be used for checking in the fragment libraries.
Custom Element Forms Content Type	Content type to be used for checking in the custom element forms.
Validation Scripts Content Type	Content type to be used for checking in the validation scripts.
Web Site Objects Content Type	Content type to be used for checking in the sample website objects.
Custom Configuration Scripts Content Type	Content type to be used for checking in the custom configuration scripts.
Initial Section ID	Initial value used to name website sections.

9.6 Creating Components Using the Component Wizard

This section describes how to use the Component Wizard to create components. It contains the following major sections:

- [Component Wizard Overview](#)

- Working with Java Code
- Editing the Readme File
- Creating a Component Using Component Wizard
- Additional Component Wizard Tasks



Note:

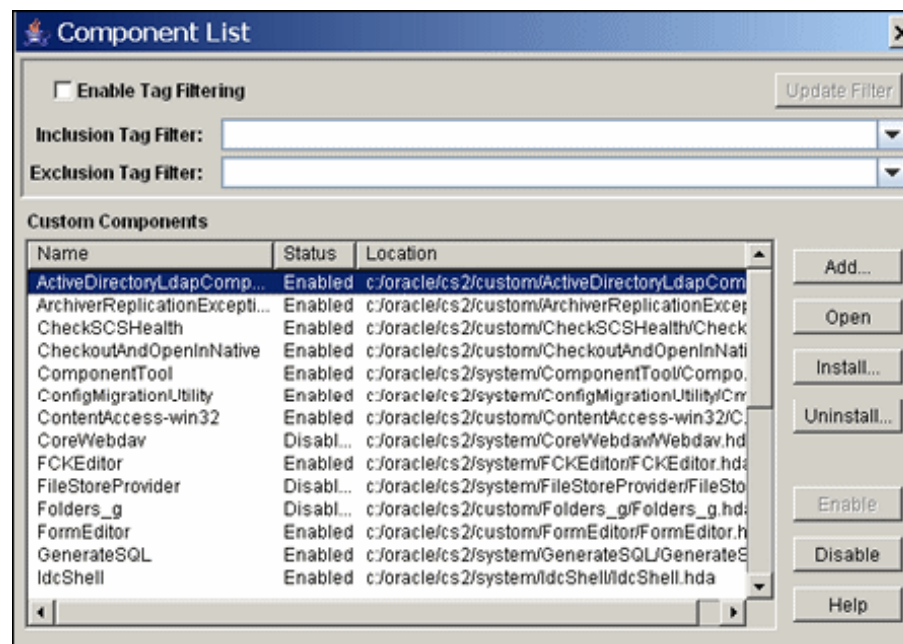
When using the Component Wizard with Red Hat Linux ES 3, set `UseCustomModaling=FALSE` in your `DomainHome/ucm/cs/bin/intradoc.cfg` file. This variable allows a modal dialog to lock only one frame, instead of all frames. Setting the variable in the `intradoc.cfg` file ensures that other applets are unaffected by this action. See `HTMLEditorPath` in *Configuration Reference for Oracle WebCenter Content*.

9.6.1 Component Wizard Overview

The following steps provide an overview on using the Component Wizard to create a custom component.

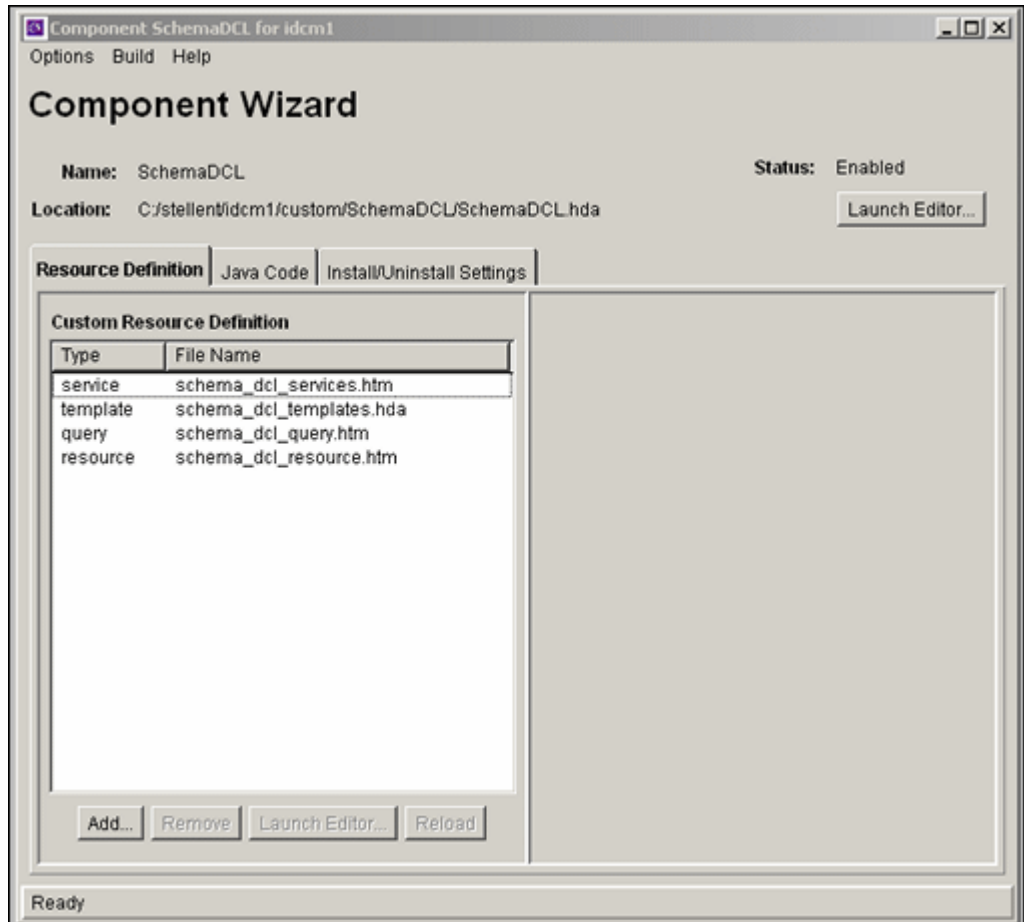
1. Launch the Component Wizard:
 - (Windows) From the **Start** menu, choose **Programs**, then **Content Server**, then **instance_name**, then **Tools**, then **Component Wizard**.
 - (UNIX) Navigate to the `DomainHome/ucm/cs/bin/` directory and run the ComponentWizard program: `./ComponentWizard`
2. If other components are already available, the Component List window opens. Select **Add**.

Figure 9-1 Components List



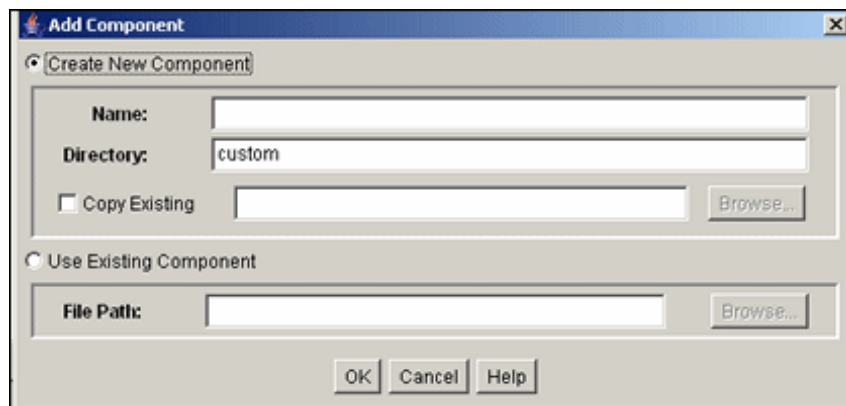
If no other components are available, the Component Wizard main window opens. Choose **Options**, then click **Add**.

Figure 9-2 Component Wizard



3. In the Add Component window, make sure the **Create New Component** option is selected, and enter the name of the new component.

Figure 9-3 Add Component



4. Click **OK**.

5. In the confirmation window, click **OK**.

The new component opens in the Component Wizard window, as indicated by its name in the **Location** field.

9.6.2 Working with Java Code

If your new component includes Java code, you can use the Java Code tab of the Component Wizard to view the contents of the ClassAliases table and the Filters table.

You can also remove classes and filters from the component glue file, although the file that is associated with the class or filter will not be deleted from your system. Select the class or filter and click the associated **Uninstall** button to remove it from the list.

9.6.3 Editing the Readme File

The Component Wizard provides a convenient way to create a Readme file for your custom component.

To edit a Readme file:

1. Open the component in the Component Wizard.
2. Choose **Options**, then **Edit Readme File**.

The text editor opens a `readme.txt` file, with the name of the component entered on the first line.

3. Enter text to document your component.
4. Save and close the file.

The `readme.txt` file is saved in the same directory as the component definition file, and will be included as a ComponentExtra entry if you use the Component Wizard to build a component zip file.

9.6.4 Creating a Component Using Component Wizard

To create a component using the Component Wizard:

1. Launch the Component Wizard.
 - (Windows) From the **Start** menu, click **Programs**, then choose **Content Server**, then **instance_name**, then **Tools**, then **Component Wizard**.
 - (UNIX) Navigate to the `DomainHome/ucm/cs/bin/` directory and run the ComponentWizard program: `./ComponentWizard`

For more information, see [Running Administration Applications in Standalone Mode](#).

2. The Component Wizard main window opens, or the Component List window opens if other components are already available. The Component List window shows installed components and their status (enabled or disabled).

Note:

If no components are installed, the Component List window does not appear.

3. If the Component List window opens, select **Add**.

If the Component Wizard main window opens, choose **Options**, then **Add**.

4. In the Add Component window, enter a name for the new component in the **Name** field.
5. Accept the default directory (`custom`), or enter a new location for the component. This can be either an absolute path or can be a path relative to the Content Server install directory. Typically, custom components are located in the `custom` directory.
6. To use an existing component definition file as a starting point for the new component, check **Copy Existing**, click **Browse**, then navigate to and select an existing definition (glue) file (`component_name.hda`).

The new component will be a copy of the existing component, including all resources and other component files. The new component must have unique name.

If you do not check **Copy Existing**, the new component will be created without any resource files

7. Click **OK**.

A new component definition (glue) file is created. If you copied an existing component, the resource files are renamed with the new component name and copied to the new component directory.

8. Add and edit custom resources and other files as necessary as described in these sections:
 - [Creating an Environment Resource for a New Component](#)
 - [Creating a Template Resource](#)
 - [Creating a Query Resource](#)
 - [Creating a Service Resource](#)
 - [Creating a HTML Include](#)
 - [Creating a String Resource](#)
 - [Creating a Dynamic Table Resource](#)
 - [Creating a Static Table Resource](#)

9.6.4.1 Creating an Environment Resource for a New Component

An environment resource defines configuration variables, either by creating new variables or replacing the value in existing variables.

To create an environment resource:

1. Make sure that the **Resource Definition** tab is selected in the Component Wizard main window, then click **Add**.
2. In the Add Resource window, select the **Environment** option for the type of resource to add.
3. Enter the file name for the resource file. The default file name is `componentname_templates.hda`.
 - If a resource file has been created, you can add to the file by selecting the file name. Any changes you make to the load order now will apply to the entire resource file.
 - To create a new resource file with a different file name, enter the file name.
4. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

5. Click **Finish**.

A dialog prompts you to launch the text editor to continue editing.

6. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).

The file appears in the **Custom Resource Definition** list.

 **Note:**

If a HTML editor is not defined, select **Options** then **Configuration** in the Component Wizard, and enter the path and file name of the desired editor, or click **Browse** and navigate to the executable of the desired editor. For details, see [Configuring the Default HTML Editor](#).

7. Save the file in the text editor.

The new environment resource opens in the Component Wizard window.

9.6.4.2 Creating a Template Resource

A template resource file defines names, types, and locations of custom templates to be loaded for the component. To add a template page:

1. Make sure that the **Resource Definition** tab is selected in the Component Wizard main window, then click **Add**.
2. In the Add Resource window, select the **Template** option.
3. In the Add Resource window, enter the file name for the resource file. The default file name is `componentname_templates.hda`.
 - You can enter `templates/` before the file name to create a new templates directory in your component directory.
 - If a template resource file has been created, you can append a new template table to the existing file by selecting the file name. Any changes you make to the load order now will apply to the entire resource file.
 - To create a new resource file with a different file name, enter the file name.
4. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

5. Click **Next**.

6. In the Add Template Table Information window, enter a name for the table that will be accessed for the template used in the component.
 - It is a good idea to leave the name of the component as a prefix.
 - Each template table in a component must have a unique name, even if the tables are in different resource files.
7. Select which standard table to merge the new template table into:
 - `IntradocTemplates`
 - `SearchResultTemplates`
8. Click **Next**.
9. In the Add/Edit Intradoc Template window, to start with an existing template definition:
 - a. Click **Select**.

The Resource Selection Dialog window opens with a list of the predefined templates.
 - b. To show the entire list of predefined templates, select **Show All**.
 - c. Select a template from the list.

The new template resource will be a copy of the existing template.
 - d. Click **OK**.

The template parameters are filled in.

 **Note:**

You can also use an existing custom template file as a starting point. Select **Copy From**, then click **Browse** and navigate to and select the template file. The template parameters will not be filled in automatically, but you could select a standard template to fill in the fields before selecting the template file.

10. Edit the template parameters as necessary.

 **Note:**

If you do not change the name of the template and this component is loaded last, the custom template will override the standard template and any other custom templates with the same name.

11. Click **Finish**.

A dialog prompts you to launch the text editor to continue editing.
12. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).

The file appears in the **Custom Resource Definition** list, and the template table appears in the **Table Name** list in the right pane.

 **Note:**

This function is unavailable if the minimum specifications have not been defined for the resource.

9.6.4.3 Creating a Query Resource

A query resource defines SQL queries, which are used to manage information in the database. Queries are used with services to perform tasks such as adding, deleting, or retrieving data from the database.

To add a query:

1. On the Component Wizard main page, click **Add in the Resource Definition pane**.
2. In the Add Resource window, select the **Query** option.
3. Enter the file name for the resource file. The default file name is `resources/componentname_query.htm`.
 - If a query resource file has been created with the default file name, the new default file name will have a number (1, 2, and so on) appended to it. You cannot append a query table to the existing default file unless you edit the resource file manually.
 - If a query resource file has been created with a file name other than the default, you can append a new query table to the existing file.
 - To create a new resource file with a different file name, enter the file name.
4. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

5. Click **Next**.
6. In the Add Query Table Information window, enter a name for the query table. It is a good idea to leave the name of the component as a prefix. The default is the name of the component followed by an underscore and the string *Queries*.

If you are appending to an existing query resource file, you must enter a new table name. You cannot append a query definition to the existing table unless you edit the resource file manually.
7. Click **Next**.
8. In the Add/Edit Query window, to start with an existing query definition:
 - a. Click **Select**.

The Resource Selection dialog opens with a list of predefined queries.
 - b. Select a query from the list.
 - c. Click **OK**.

The SQL Query expression and parameters appear and the **Name** field is filled in.

 **Note:**

If you do not change the name of the query and this component is loaded last, the custom query will override the standard query and any other custom queries with the same name.

9. Edit the query expression and parameters as necessary.
 - Parameters must appear in the **Parameters** list in the order they appear in the query expression. Use the **Up** and **Down** buttons to move the selected parameter.
 - To add a parameter, click **Add**. Enter a parameter Name, select the parameter Type, and click **OK**.
 - To edit a parameter type, select the parameter and click **Edit**. Select the parameter Type, and click **OK**.
 - To remove a parameter, select the parameter and click **Delete**.
10. Click **Finish**.
A dialog prompts you to launch the text editor to continue editing.

 **Note:**

This function is unavailable if the minimum specifications have not been defined for the resource.

11. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).
The query resource file appears in the **Custom Resource Definition** list, and the query table appears in the **Table Name** list in the right pane.

9.6.4.4 Creating a Service Resource

A service resource defines a function or procedure that is performed by the Content Server instance. To create a service resource using the Component Wizard.

1. In the Component Wizard, open the component for which the resource will be created.
2. On the **Resource Definition** tab, click **Add**.
3. In the Add Resource window, select the **Service** option.
4. Enter the file name for the resource file. The default file name is `resources/componentname_service.htm`.
 - If a resource file has been created for services, you can append the new service table to the existing file by selecting the file name. Any changes you make to the load order now will apply to the entire resource file.
 - To create a new resource file with a different file name, enter the file name.
5. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

6. Click **Next**.
7. In the Add Service Table Information window, enter the name of the service table that will be created for the new resource.
 - It is a good idea to leave the name of the component as a prefix.
 - The default is the name of the component followed by an underscore and the string *Services*.
 - Each service table in a component must have a unique name, even if the tables are in different resource files.
8. Click **Next**.
9. In the Add Service window, to start with an existing service definition:
 - a. Click **Select**.

The Resource Selection window opens with a list of commonly used predefined services.
 - b. To show the entire list of predefined services, select **Show All**.
 - c. Select a service from the list.
 - d. To view a service's details, click **Preview**.

Use the Preview Information for Service window to view information about the service and the service actions.
 - e. Click **OK**.

The service attributes and actions are filled in.

 **Note:**

If you do not change the name of the service and this component is loaded last, the custom service will override the standard service and any other custom services with the same name.

10. Edit the service attributes and actions as necessary.

Attributes include the Service Class, Template, Service Type, Access Level, Subjects Notified, and Error Message.

Actions are used to execute a SQL statement, perform a query, run code, cache the results of a query, or load an option list.

 - Actions must appear in the Actions list in order of execution. Use the **Up** and **Down** buttons to move the selected action.
 - To add an action, click **Add**. The Add Action window opens. Enter the action definition and click **OK**.
 - To edit an action, select the action and click **Edit**. Modify the action definition and click **OK**.

- To remove an action, select the action and click **Delete**.

11. Click **Finish**.

A dialog prompts you to launch the text editor to continue editing.

 **Note:**

This function is unavailable if the minimum specifications have not been defined for the resource.

12. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).

The service resource file appears in the **Custom Resource Definition** list, and the service table appears in the **Table Name** list in the right pane.

9.6.4.5 Creating a HTML Include

An *HTML include* is a piece of reusable code that is referenced from a placeholder in another file or from another location in the same file. An include resource defines pieces of code that are used to build the Content Server web pages. Includes are resolved by the Content Server instance each time a web page is assembled. For this reason, includes are sometimes called *dynamic content resources*.

To add a HTML include resource:

1. In the Component Wizard main window, on the **Resource Definition** tab, click **Add**.
2. In the Add Resource window, select the **Resource - HTML Include/String** option.
3. Enter the file name for the resource file. The default file name is `componentname_resource.htm`.
 - If a resource file has been created for includes, strings, or static tables, or both, you can append the include to the existing file by selecting the file name. Any changes you make to the load order now will apply to the entire resource file.
 - To create a new resource file with a different file name, enter the file name.
4. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

5. Click **Next**.
6. In the Add HTML Resource Include/String window, to specify a customized HTML resource or a customized string resource in a component, select the **Include** option.
7. To start with the code from an existing HTML include:
 - a. Click **Select**.

The Resource Selection window opens with a list of commonly used predefined includes.

- b. To show the entire list of predefined includes, select **Show All**.
- c. Select an include from the list.
- d. Click **OK**.

The include code appears and the **Name** field is filled in.

 **Note:**

If you do not change the name of the include and this component is loaded last, the custom include will override the standard include and any other custom includes with the same name.

8. Edit the include code as necessary.
9. Click **Finish**.
A dialog prompts you to launch the text editor to continue editing.
10. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).

The resource file appears in the **Custom Resource Definition** list, and the include appears in the **Custom HTML Includes** list.

9.6.4.6 Creating a String Resource

A string resource defines locale-sensitive text strings that are used in error messages and on Content Server web pages and apps. To create a string resource using the Component Wizard.

1. In the Component Wizard, open the component for which the resource will be created.
2. On the **Resource Definition** tab, click **Add**.
3. In the Add Resource window, select the **Resource - HTML Include/String** option.
4. Enter the file name for the resource file. The default file name is `componentname_resource.htm`.
 - If a resource file has been created for includes, strings, or static tables, or both, you can append the include to the existing file by selecting the file name. Any changes you make to the load order now will apply to the entire resource file.
 - To create a new resource file with a different file name, enter the file name.
5. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

6. Click **Next**.
7. In the Add HTML Resource Include/String window, to specify a customized HTML resource or a customized string resource in the component, select the **String** option.

8. Enter the name of the string in the **Name** field (for example, `myString`.)

 **Note:**

If you enter the name of an existing string and this component is loaded last, the custom string will override the standard string and any other custom strings with the same name.

9. Edit the string code as necessary (for example, `This is my string text`.)
10. Click **Finish**.
A dialog prompts you to launch the text editor to continue editing.
11. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).
The resource file appears in the **Custom Resource Definition** list, and the string appears in the **Custom Strings** list.

9.6.4.7 Creating a Dynamic Table Resource

A dynamic table provides dynamic (often changed) content in table format to the Content Server instance.

To create a dynamic table resource using the Component Wizard.

1. In the Component Wizard, open the component for which the resource will be created.
2. On the **Resource Definition** tab, click **Add**.
3. In the Add Resource window, select the **Resource - Dynamic Table (Hda Format)** option.
4. Enter the file name for the resource file. The default path and file name is `resources/componentname_resource.hda`.
 - If a resource file has been created for dynamic tables, you can append the new table code to the existing file by selecting the file name. Any changes you make to the load order now will apply to the entire resource file.
 - To create a new resource file with a different file name, enter the file name.
5. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

6. Click **Next**.
7. In the Add Dynamic Resource Table Information, enter a name for the dynamic table. It is a good idea to leave the name of the component as a prefix.
8. To merge the new table with an existing table, select **Merge To**, and select a target table from the list or enter the name of a custom table.
9. Click **Finish**.

- If you selected a table to merge to, a dialog prompts you to launch the text editor to continue editing.
- If you did not select a table to merge to, the Column Information window opens.
 - a. Enter a column name in the **Column Name** field.
 - b. Click **Insert**. Repeat these steps until all of the table columns have been entered.
 - c. Click **OK**.

A dialog prompts you to launch the text editor to continue editing.
 - d. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).

The resource file appears in the **Custom Resource Definition** list, and the table appears in the right pane of the **Resource Definition** tab.

9.6.4.8 Creating a Static Table Resource

To create a static table resource using the Component Wizard:

1. In the Component Wizard, open the component for which the resource will be created.
2. On the **Resource Definition** tab, click **Add**.
3. In the Add Resource window, select the **Resource - Static Table (HTML Format)** option.
4. Enter the file name for the resource file. The default file name is `componentname_resource.htm`.
 - If a resource file has been created for static tables, includes, or strings, or both, you can append the static table code to the existing file by selecting the file name. Any changes you make to the load order now will apply to the entire resource file.
 - To create a new resource file with a different file name, enter the file name.
5. If you want the new resource file to be loaded in a particular order, enter the number in the **Load Order** field.

 **Note:**

Unless you have a particular reason for the resource file to be loaded after other resources, you should leave the load order set to 1.

6. Click **Next**.
7. In the Add Static Resource Table Information window, enter a name for the static table. It is a good idea to leave the name of the component as a prefix.
8. To merge the new table with an existing table, select **Merge To**, and select a table from the list.
9. Click **Finish**.
 - If you selected a table to merge to, a dialog box asks if you want to launch the text editor to continue editing.
 - If you did not select a table to merge to, the Column Information window opens.
 - a. Enter a column name in the **Column Name** field.
 - b. Click **Insert**.

- c. Repeat steps a and b until all of the table columns have been entered.
- d. Click **OK**.
A dialog prompts you to launch the text editor to continue editing.
- e. Click **Yes** to open the resource file in the text editor (or click **No** to return to the Component Wizard).
The resource file appears in the **Custom Resource Definition** list, and the table appears in the **Resource Tables** list.

9.6.4.9 Enabling the Component

After creating a component, you should enable it and test it.

1. In the Component Wizard main window, choose **Options**, then **Enable**.
2. Restart the Content Server instance.
3. Test the newly created component.

9.6.5 Additional Component Wizard Tasks

In addition to creating custom components, you can use the Component Wizard to build zip files of your components and create custom installation parameters.

- [Building a Component Zip File](#)
- [Working with Installation Parameters](#)
- [Enabling and Disabling a Component](#)
- [Removing a Component](#)
- [Opening a Component](#)
- [Configuring the Default HTML Editor](#)
- [Unpackaging a Component](#)
- [Adding an Unpackaged Component](#)

9.6.5.1 Building a Component Zip File

The Build function of the Component Wizard enables you to build a component zip file (or *package*), which can then be saved as a backup or unpackaged to deploy the component on other Content Server instances.

To build a component zip file:

1. Open the component in the Component Wizard.
2. From the **Build** menu, choose **Build Settings**.
A Component entry for the definition (glue) file and a ComponentExtra entry for a `readme.txt` file are automatically created. You should not remove the glue file entry, but you can delete the `readme.txt` entry.
3. In the Build Settings window, click **Add**.
4. In the Add window, select an Entry Type.
5. In the **Sub Directory** or **File** field, enter the location of the files for the selected entry type.
 - For the Component entry type, this setting is the file name for the glue file.

- For other entry types, enter a path to select all files in a particular directory, or enter a path and file name to select an individual file.
- The location should be a path relative to the *DomainHome/custom/* directory. You can use an absolute path (such as *C:/DomainHome/custom/my_component/*), but then the component can only be installed on Content Server instances with the same installation directory path.

 **Note:**

Always use forward slashes in the path.

6. Continue adding entry types and specifying the subdirectories until all of the files of your component are included.
7. Click **OK**.
8. From the **Build** menu, choose **Build**.
9. In the main Build window, click **OK**.

The Component Wizard builds the component zip file in the *DomainHome/custom/component_name* directory.

9.6.5.2 Working with Installation Parameters

The Install/Uninstall Settings tab is used to create customized installation components that can include preference data parameters. These parameters can be user prompts and messages. Depending on how they are defined, the prompts and messages are displayed during the installation processes. These custom installation parameters allow the component author to ask for information from users before the component is installed.

To define custom installation parameters for a component:

1. In the Component List window, select the component to have custom installation parameters defined.
2. Click **Open**.
3. In the Add Preference window, select the **Install/Uninstall Settings** tab, then select the appropriate check boxes:
 - Has Install/Uninstall Filter
 - Has Install Strings

Generally, both options are used to create the desired installation parameters.

4. Click the **Launch Editor** for the Install/Uninstall Filter option to open a Java code template file. Edit the existing code and include additional Java code to the template as necessary to create the filter procedures.

Each filter procedure will run once during the component installation or uninstall procedure. The values of user responses are saved in the installation configuration (*install.cfg* and *config.cfg*) files. See Custom Installation Parameter Files in *Developing with Oracle WebCenter Content*.

5. Save and close the Install/Uninstall Filter Java code file.
6. In the Preference Data Setup pane, click the **Add** button to open the Add Preference window.

7. Click the **Launch Editor** for the Install Strings option to open a Java code template file. Edit the existing code and include additional Java code to the template as necessary to define the set up prompts or messages.

Keep both the Add Preference window and the Install Strings HTML template open to use simultaneously. Complete the fields on the Add Preference window as necessary. Add the actual message or prompt text to the Install Strings HTML.
8. Save and close the Install Strings Java code file.
9. Open the Build Settings window by choosing **Build Settings** from the **Build** menu.
10. Complete the fields on the Build Settings window as necessary.
11. If components have been specified to be included in the component zip file, they will need to be added as component extras using the Add window. Click the **Add** button to open the Add window.

Add each component individually.
12. Click **OK**.
13. If necessary, add more components to the zip file as component extras.
14. In the Build Settings window, click **OK** to create the component zip file.

The zip file can be shipped to clients and can be installed using either the Component Wizard or the Component Manager within the Content Server instance.

9.6.5.3 Enabling and Disabling a Component

Use one of the following procedures to enable or disable a component from the Component Wizard:



Tip:

Components can also be enabled and disabled using the Component Manager.

9.6.5.3.1 Option 1

1. Open the component in the Component Wizard.
2. In the Component Wizard main window, choose **Options**, then **Enable**.
3. Restart the Content Server instance.

The component is now enabled or disabled.
4. Navigate to the pages affected by the component to ensure that the addition or removal of the customization is working as you expected.

9.6.5.3.2 Option 2

1. Use either of the following methods to display the Component List window:
 - Start the Component Wizard.
 - In the Component Wizard main window, choose **Options**, then **Open**.
2. Select the component to be enabled or disabled.
3. Click **Enable** or **Disable** for the condition you want to set the component.

4. Restart the Content Server instance.
The component is enabled or disabled.
5. Navigate to the pages affected by the component to ensure that the addition or removal of the customization is working as you expected.

9.6.5.4 Removing a Component

To remove a component from the Content Server instance:



Note:

Removing a component means that the Content Server instance no longer recognizes the component, but the component files are not deleted from the file system.

1. Disable the component you want to remove.
If the component to be removed is open in the Component Wizard, open a different component or close and restart the Component Wizard. (A component cannot be removed if it is open.)
2. To display the Component List window:
 - Start the Component Wizard.
 - In the Component Wizard main window, choose **Options**, then **Open**.
3. From the Component List window, select the component to be removed.
4. Click **Uninstall**.
5. Click **Yes**.
The component no longer appears in the Component List.

9.6.5.5 Opening a Component

To open a component that has already been added to the Content Server instance:

1. To display the Component List window:
 - Start the Component Wizard
 - In the Component Wizard main window choose **Options**, then **Open**.
2. From the Component List window, select the component to open.
3. Click **Open**.
The component resources are shown in the **Custom Resource Definition** list on the Component Wizard main menu.

9.6.5.6 Configuring the Default HTML Editor

You can edit text-based component files directly from the Component Wizard by launching the HTML editor.

- (Windows) Microsoft WordPad (`wordpad.exe`) is the default editor.

- (UNIX) `vi` is the default editor.

 **Note:**

Specify a text editor (such as WordPad) rather than a graphical HTML editor. Graphical editors can insert or change HTML tags and might cause Idoc Script tags to be converted into a string of characters that will not be recognized by the Content Server instance.

To define the default HTML editor:

1. Display the Component Wizard main window.
2. Choose **Options**, then **Configuration**.
3. In the Component Configuration window, click **Browse**.
4. Navigate to and select the executable file for the HTML editor you want to use.
5. Click **Open**.
6. Click **OK**.

When you click any **Launch Editor** button in the Component Wizard, the file will open in the selected program.

9.6.5.7 Unpackaging a Component

To unpackage a component Zip file:

 **Note:**

If you unpackage a component with the same name as an existing component on the Content Server instance, the older component will be zipped and copied to the `DomainHome/ucm/cs/bin/` directory, with a file name beginning with `backup` and ending with a time stamp (such as `backup1008968718221.zip`).

1. Use either of the following methods to display the Install window:
 - In the Component Wizard main window, choose **Options**, then **Install**.
 - From the Component List window, click **Install**.
2. Click **Select**.
3. In the Zip File Path window, navigate to and select the component zip file.
4. Click **Open**.

The contents of the component zip file are listed on the Unpackage window.

5. Click **OK**.

The component files are copied to the correct locations (there might be a short delay while the files are unzipped), the Unpackage window closes, and the component resources are shown in the **Custom Resource Definition** list on the Component Wizard main window. The component also is added to the Component List.

 **Note:**

Unpackaging a component does not enable it. For more information, see [Enabling and Disabling a Component](#).

9.6.5.8 Adding an Unpackaged Component

To add an existing unpackaged component to the Content Server instance:

1. Use either of the following methods to display the Add Component window:
 - In the Component Wizard main window, from the **Options** menu choose **Add**.
 - From the Component List window, click **Add**.
2. Choose the **Use Existing Component** option.
3. Click **Browse**.
4. Navigate to and select the component definition (.hda) file (components.hda).
5. Click **Open**.

The path and file name are displayed in the **FilePath** field.

6. Click **OK**.

The component resources are shown in the **Custom Resource Definition** list on the Component Wizard main window. The component is also added to the Component List.

 **Note:**

Adding an existing component does not enable it.

10

Managing Search Features

This chapter describes how to configure the OracleTextSearch feature to use Oracle Text as the primary full-text search engine for Oracle WebCenter Content and how to configure full-text database searching.

This chapter also describes how to configure Elasticsearch which has reduced rebuild time significantly and how to configure OpenSearch.

This chapter covers the following topics:

- [Managing OracleTextSearch](#)
- [Configuring Full-Text Database Search Index](#)
- [Managing Elasticsearch](#)
- [Managing OpenSearch](#)

10.1 Managing OracleTextSearch

If you have a license to use the OracleTextSearch feature with Oracle Database, then you can configure OracleTextSearch to use the Oracle Text product as the primary full-text search engine for WebCenter Content. Oracle Text offers state-of-the-art indexing capabilities. Oracle Text has its own query syntax, which is intended more for use by applications or information professionals rather than casual end-users.

OracleTextSearch enables administrators to specify certain metadata fields to be optimized for the search index and to customize additional fields. This feature also enables a fast index rebuild and index optimization.

This section covers the following topics:

- [Considerations for Using OracleTextSearch](#)
- [Oracle Text Features and Benefits](#)
- [Configuring OracleTextSearch for Content Server](#)
- [Managing OracleTextSearch](#)
- [Searching with OracleTextSearch](#)
- [Using Metadata Wildcards](#)
- [Using Internet-Style Search Syntax](#)
- [Adjusting the Score on OracleTextSearch Results](#)
- [Customizing Search Results with OracleTextSearch](#)

10.1.1 Considerations for Using OracleTextSearch

The following items are important when considering use of the OracleTextSearch feature:

- WebCenter Content version 12c supports all languages supported by Oracle Text. OracleTextSearch can filter and extract content from different document formats in different languages. It supports a large number of document formats, including Microsoft Office file

formats, Adobe PDF, HTML, and XML. It also supports archive and compression file formats such as zip, zipx, and gz. It can render search results in various formats, including unformatted text, HTML with term highlighting, and original document format.

- Oracle Text runs on Oracle Database 12c. The Content Server database can be Oracle Database 12c, Microsoft SQL Server, or other databases as listed in the Oracle WebCenter Content 12c Certification Matrix. However, if the system database is not Oracle Database 12c, then an external provider for OracleTextSearch must be configured. For details on external providers, see [Configuring OracleTextSearch for Content Server](#).
- When using OracleTextSearch, Oracle Database version 11.1.0.7.0 or higher is required.
- Optimized fields for OracleTextSearch are created as SDATA fields, which have a maximum limit of 249 characters. This limit is imposed by Oracle Database and is reflected in Content Server by the OracleTextSearch component. Default SDATA fields include dDocName, dDocTitle, dDocType, and dSecurityGroup. The total number of SDATA fields is limited to 32 fields.
- While WebCenter Content provides numerous search options using a variety of databases (Oracle, Microsoft SQL Server, IBM DB2), by default the database that serves as the search index is the same system database used by WebCenter Content to manage metadata and other configuration information (users, security groups, and so on). The OracleTextSearch feature enables Oracle Text as a separate search collection instance on Oracle Database 12c for WebCenter Content, which allows the search collection to reside on a separate computer and not compete with WebCenter Content for processors and memory. This can improve indexing and search response time.
- The OracleTextSearch collection instance can be installed on a different platform than the WebCenter Content installation.
- If the OracleTextSearch feature is configured and running, and metadata fields are pushed in to the Content Server instance either by the administrator or by a component (requiring that the Content Server instance be restarted), then the OracleTextSearch index must be rebuilt before content using the new metadata fields can be checked in to the Content Server instance.

10.1.2 Oracle Text Features and Benefits

This section covers the following topics:

- [Indexing and Query Speeds and Techniques](#)
- [Fast Rebuild](#)
- [Query Syntax](#)
- [OracleTextSearch Operators](#)
- [Case Sensitivity and Stemming Rules](#)
- [Search Results Data Clustering](#)
- [Snippets](#)
- [Additional Changes](#)

10.1.2.1 Indexing and Query Speeds and Techniques

Using Oracle Text, WebCenter Content offers a significant increase in index speeds. Oracle Text indexing is transactional. Content Server sends a batch of document to Oracle Text, commits the batch, then starts the Oracle Text indexer. Content Server is notified of which documents failed to index and only those documents are resubmitted to be indexed. Additional

capabilities include an automatic Fast Optimization for every 5,000 documents added to the Content Server instance, and a Full Optimization for every 50,000 documents or 20% growth of the repository. Note that Content Server metadata-only search queries may degrade in performance when using Oracle Text.

WebCenter Content uses some of the newest Oracle Text features. For example, Content Server automatically creates a new search index zone for each text information field in order to provide better search speed. Using information zones enables Content Server to query data as if it were full-text data. All text-based information fields (text, long text, and memo) are automatically added to as separate zones. In addition to the zones created for text information fields, Content Server provides an extra zone named IdcContent, which enables custom components, Oracle WebCenter Content: Inbound Refinery components, applications, or users to create XML content with tags that will be indexed as full-text metadata fields.

WebCenter Content uses the SDATA section feature in Oracle Text to index important text, date, and integer fields and define them as Optimized Fields. The SDATA section is a separate XML structure managed by the Oracle Text engine that allows the engine to respond rapidly to requests involving data and integer ranges. Content Server can have up to 32 Optimized Fields, which includes data, integer, standard Content Server fields like dInDate, dOutDate, and fields selected to be optimized. All Optimized Fields are SDATA fields, which by default include dDocName, dDocTitle, dDocType, and dSecurityGroup.

**Note:**

If you want to change the set of Optimized Fields defined in Oracle Text, the maximum allowed number of Optimized Fields is 32.

To avoid errors when indexing, do not add non-existent metadata fields to the Configuration Manager DrillDownFields parameter, and do not add memo fields to an SDATA section or to the DrillDownFields parameter. See Understanding Management Tools in *Managing Oracle WebCenter Content*.

10.1.2.2 Fast Rebuild

OracleTextSearch provides an Indexer Rebuild window when you use the Collection Rebuild Cycle window on the Repository Manager application Indexer tab. The Fast Rebuild feature allows the search engine to add new information to the search collection without requiring a full collection rebuild. A Fast Rebuild is required in the following cases:

- Adding or removing information fields
- Changing any Optimized Field
- Changing an information field to be an Optimized Field

A Fast Rebuild does not cause all the information (metadata and full-text) to be re-indexed. It adds the changes throughout the collection and updates it. Content Server search functionality is not affected during a Fast Rebuild cycle.

For information on performing a fast rebuild, see [Performing a Fast Rebuild](#).

10.1.2.3 Query Syntax

Queries defined in Universal Query Syntax are supported and generally do not need any modification. This includes queries saved by users, queries defined in custom components, and queries defined in Site Studio pages.

10.1.2.4 OracleTextSearch Operators

Oracle Text supports the following defaults:

- CONTAINS
- MATCHES
- Has Word Prefix
- Range searches for dates and integers

10.1.2.4.1 Search Thesaurus

Certain queries, such as *stem* and *Related Term*, may be more effective if you use an Oracle Text thesaurus. Oracle Text enables you to create case-sensitive or case-insensitive thesauri which define synonym and hierarchical relationships between words and phrases. You can then search and retrieve documents that contains relevant text by expanding queries to include similar or related terms as defined in the thesaurus. For example, you can populate a thesaurus with specific product names, associated models, associated features, and so forth.

- **Default thesaurus:** If you do not specify a thesaurus by name in a query, by default, the thesaurus operators use a thesaurus named DEFAULT. However, Oracle Text does not provide a DEFAULT thesaurus.

As a result, if you want to use a default thesaurus for the thesaurus operators, you must create a thesaurus named DEFAULT. You can create the thesaurus through any of the thesaurus creation methods supported by Oracle Text:

- CTX_THES.CREATE_THESAURUS (PL/SQL)
- ctxload utility

- **Supplied thesaurus:** Oracle Text does not provide a default thesaurus, but Oracle Text does supply a thesaurus, in the form of a file that you load with `ctxload`, that can be used to create a general-purpose, English-language thesaurus.

The thesaurus load file can be used to create a default thesaurus for Oracle Text, or it can be used as the basis for creating thesauri tailored to a specific subject or range of subjects.



Note:

See the *Oracle Text Reference* to learn more about using `ctxload` and the `CTX_THES` package, and see the chapter, "Working With a Thesaurus in Oracle Text," in the *Oracle Text Application Developer's Guide*.

10.1.2.5 Case Sensitivity and Stemming Rules

Content Server automatically ensures that queries are executed as case-insensitive. By default, all full-text and text field search queries are case-insensitive. Content Server also handles case-insensitive search queries for information stored as Optimized Fields.

Stemming is an Oracle Text feature that uses the stem (\$) operator to search for terms that have the same linguistic root as the query term (the syntax is `$term`). For example, the input `$sing` would expand a search to include `sang sung sing`. *Stemming rules* can be used to have searches account for plurals, verbs, and so forth. Content Server does not apply any

stemming rules by default for Oracle Text, but a set of stemming rules can be created by using the stem (\$) operator. Other methods for implementing stemming rules include modifying the standard query definition in the `searchindexerrules` configuration file (which requires a custom component), and by making configuration changes in the Oracle Text engine (Oracle Database).

 **Note:**

For more information, see the chapter "Oracle Text CONTAINS Query Operators" in the *Oracle Text Reference*.

Content Server handles content in non-English languages by using the `WORLD_LEXER` feature in the Oracle Text engine. This enables Oracle Text to automatically identify the language and apply the proper tokenization rules.

10.1.2.6 Search Results Data Clustering

With the `OracleTextSearch` feature, Content Server retrieves additional information about a search result list and displays it in a new menu bar on the Search Results page. This information summarizes how many documents are attached to specific values in specific information fields. Content Server supports data clustering for up to four information fields (the default fields are Security Group and Document Type).

This can be useful if you have a query that returns many items. For example, a result set could include 200 content items, including 100 documents that belong to the Public security group, 75 that belong to the Sales group, and 25 that belong to the Marketing group. The menu option for Security Group will show you the list of values and how many documents belong to each value. You can select one of the values (Public, Sales, Marketing) from the menu and it will list only those documents in the result set that belong to that value.

10.1.2.7 Snippets

Content Server can retrieve document snippets as part of search results to show the occurrence of search terms in context of their usage. This feature is disabled by default. To enable this feature, although it can affect search query performance, set the following configuration entry in the `config.cfg` file:

```
OracleTextDisableSearchSnippet=false
```

10.1.2.8 Additional Changes

Additional changes because of the use of Oracle Text include:

- XML content is automatically indexed.
- There are no visible changes in the Search user interface other than removal of Substring as a search operator option. The default search operators are CONTAINS, MATCHES, and HAS WORD PREFIX. Substring-based queries still work.
- Queries using the MATCHES operator on a non-optimized field behave like a CONTAINS query. For example, if `xDepartment` is not optimized, then the query `xDepartment MATCHES 'Marketing'` behaves like `xDepartment CONTAINS 'Marketing'` and returns hits on content items that have an `xDepartment` value of 'Marketing Services' or 'Product Marketing'.

- Relevancy ranking can be changed in Oracle Text through use of an operator called `DEFINESCORE`. This operator can be added through a component to the `WhereClause` value of `OracleTextSearch` in the `SearchQueryDefinition` table (in the Oracle Text `searchindexerrules` configuration file). More information about this operator is available in the *Oracle Text Reference* document.
- Complicated queries that previously could be placed into the full-text search box should now be placed in the advanced options on the Query Builder Form. The Query Builder Form is documented in the *Using Oracle WebCenter Content*.
- If you need to specify an escape character, use the configuration variable `AdditionalEscapeChars=`. The default setting is:

```
AdditionalEscapeChars=_:#,-: #
```

The default sets an underscore (`_`) and a hyphen (`-`) as escape characters.

- The PDF Highlighting feature has been disabled.
- The Spell Checking feature can be enabled, but it requires a custom component just as it did with Autonomy VDK.

10.1.3 Configuring OracleTextSearch for Content Server

If you did not specify `OracleTextSearch` when first installing Content Server, to configure the feature:

1. Open the `config.cfg` file for the Content Server instance in a text editor. For example:
`MW_HOME/user_projects/domain/servers/ucm/config/config.cfg`
2. Set the following property value:

```
SearchIndexerEngineName=OracleTextSearch
```

Note:

If you are using ACLs, and `UseEntitySecurity=true` is set with `OracleTextSearch` as the search engine, then the following must also be set in the `config.cfg` file for the Content Server instance:

```
ZonedSecurityFields=xClbraUserList,xClbraAliasList
```

3. If you are using an external data source instead of the system database, change the value `SystemDatabase` in the following property setting to the external database provider name:

```
IndexerDatabaseProviderName=SystemDatabase
```

Note:

You can specify a separate Oracle Database as the value of `IndexerDatabaseProviderName`, instead of `SystemDatabase`.

If the Content Server database used with `OracleTextSearch` is not Oracle Database, then an external provider for `OracleTextSearch` must be configured. Obtain the driver and `fmwgenerictoken.jar` from `MW_HOME/oracle_common/modules/oracle.jdbc_11.1.1/ojdbc6dms.jar`.

4. Save the file.
5. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).
6. Rebuild the search index.

For more information on rebuilding the index, see [Working with the Search Index](#). For more information on configuring Content Server and OracleTextSearch during installation, see *FullText Search Option* in WebCenter Content Configuration Page in *Installing and Configuring Oracle WebCenter Content*.

If you originally configured Content Server to use an external provider with OracleTextSearch, but later need to switch to use `SystemDatabase`, you must manually run the `contentprocedures.sql` script against your system database schema. The script file is located in the `WC_CONTENT_ORACLE_HOME/ucm/idc/database/oracle/admin/` directory.

10.1.4 Managing OracleTextSearch

This section covers the following topics:

- [Determining Fields to Optimize](#)
- [Assigning/Editing Optimized Fields](#)
- [Performing a Fast Rebuild](#)
- [Modifying the Fields Displayed on Search Results](#)

10.1.4.1 Determining Fields to Optimize

Consider the following when determining the fields to optimize:

- Do you want an exact match in a query?
- Do you want that match to work faster in a search?
- Do you want to sort search results by field?

By default the OracleTextSearch feature optimizes the Content ID and Document Title metadata fields.

A maximum number of 32 fields can be defined as Optimized Fields with the OracleTextSearch feature. The Content Server instance can have up to 32 Optimized Fields, which includes data, integer, standard Content Server fields like `dInDate`, `dOutDate`, and fields selected to be optimized. All Optimized Fields are SDATA fields, which by default include `dDocName`, `dDocTitle`, `dDocType`, and `dSecurityGroup`.

The display of integer fields is dynamic and depends on the Content Server configuration.

10.1.4.2 Assigning/Editing Optimized Fields

You can select metadata Non-Optimized Fields and assign them to be Optimized Fields for search purposes, or edit Optimized Fields and make them Non-Optimized.

To assign or edit Optimized fields:

1. Choose **Administration**, then **Desktop Client Apps**.
2. Select **Configuration Manager**, then the **Information Fields** tab, then **Advanced Search Design**. For more information on Configuration Manager, see *Exporting Auxiliary Metadata Sets* in *Managing Oracle WebCenter Content*.

3. To make a metadata field Optimized, click **Edit Fields**. In the Advanced Options for "metadata_field" window, select **Is Optimized**.
4. To edit an Optimized Field and make it Non-Optimized, click **Edit Fields**. In the Advanced Options for "metadata_field" window, deselect **Is Optimized**.
5. When you have completed moving fields, use **Index Fast Rebuild** in Repository Manager to update the search collection to use the new and modified fields.



Note:

The Fast Rebuild does not function if a search collection rebuild is in progress.

10.1.4.3 Performing a Fast Rebuild

The Fast Rebuild feature allows the search engine to add new information to the search collection without requiring a full collection rebuild. A Fast Rebuild is required in the following cases:

- Adding or removing information fields
- Changing any Optimized Field
- Changing an information field to be an Optimized Field

To perform a fast rebuild:

1. Choose **Administration**, then **Desktop Client Apps**.
2. Choose **Repository Manager**, then select the **Indexer** tab.
3. In the Collection Rebuild Cycle part of the Repository Manager application Indexer tab, click **Start**.

The Indexer Rebuild window opens with a warning that rebuilding the search index is a time-consuming process. If you do not want to start a rebuild now, click **Cancel**; otherwise, continue with this procedure.

4. In the Indexer Rebuild window, click **OK**.

A Fast Rebuild of the search collection is performed.



Note:

A Fast Rebuild is not performed if a rebuild of the search collection is in progress.



Note:

The Fast Rebuild process does not create indexer counter values for Full Text, Meta Only, and Delete. To obtain indexer count statistics, you must perform a full collection rebuild.

10.1.4.4 Modifying the Fields Displayed on Search Results

The OracleTextSearch feature provides default menu options on the Search Results page (set by the Oracle Database configuration script):

```
DrillDownFields=dDocType, dSecurityGroup
```

Administrators can add one more option from the list of Optimized Fields to further customize the search results. Edit the configuration to add the option to the list of DrillDownFields. (This function does not support multi-value option lists.)

A Fast Rebuild must be performed after making any change in the DrillDownfields setting.

10.1.5 Searching with OracleTextSearch

Performing a search with OracleTextSearch is generally the same except there are no visible changes in the Search: Expanded Form other than removal of Substring as a search operator option. The default search operator is CONTAINS. Substring-based queries still work.

See Searching with Oracle Text Search in *Using Oracle WebCenter Content*.

The following table describes the default search operators.

Operator	Description	Example
CONTAINS	Finds content items with the specified whole word or phrase in the metadata field. This is available only for OracleTextSearch, or for Oracle Database and Microsoft SQL Server database with the optional DBSearchContainsOpSupport component enabled.	When <code>form</code> is entered in the Title field, the search returns items with the word <code>form</code> in their title, but does not return items with the word <code>performance</code> or <code>reform</code> .
MATCHES	Finds items with the exact specified value in the metadata field.	When <code>address change form</code> is entered in the Title field, the search returns items with the exact title of <code>address change form</code> . A query that uses the MATCHES operator on a non-optimized field behaves the same as a query that uses the CONTAINS operator. For example, if the <code>xDepartment</code> field is not optimized, then the query <code>xDepartment MATCHES 'Marketing'</code> behaves like <code>xDepartment CONTAINS 'Marketing'</code> , returning hits on documents that have an <code>xDepartment</code> value of <code>'Marketing Services'</code> or <code>'Product Marketing'</code> .

Operator	Description	Example
HAS WORD PREFIX	Finds all content items with the specified word at the beginning of the metadata field. No wildcard character is placed before or after the specified value.	When <code>form</code> is entered in the Title field, the search returns all items with the word <code>form</code> at the beginning of their title, but does not return an item whose title begins with the word <code>performance</code> or <code>reform</code> .

 **Note:**

We cannot use wildcards (`?` and `*`) to escape special characters when `CONTAINS` and `HAS WORD PREFIX` operators are used. For example, if we have a `dDocTitle` as `Webcenter_Content`, we cannot search with `Webcenter?Content` or `Webcenter*Content` with `CONTAINS` and `HAS WORD PREFIX` operators.

10.1.6 Using Metadata Wildcards

The following wildcards can be used in metadata search fields, even when using the Quick Search field.

- An asterisk (`*`) indicates zero or many characters. For example:
 - `form*` matches `form` and `formula`
 - `*orm` matches `form` and `reform`
 - `*form*` matches `form`, `formula`, `reform`, and `performance`
- A question mark (`?`) indicates one character. For example:
 - `form?` matches `forms` and `form1`, but not `form` or `formal`
 - `??form` matches `reform` but not `perform`

 **Note:**

If you want to search for an asterisk (`*`) or a question mark (`?`) without treating it as wildcard, you need to put quotation marks around your search term; for example: `"here*"`. Wildcard (`?`) do not work for the Security Group metadata field in OracleTextSearch. Also, metadata field values with underscore (`_`) do not work with wildcard (`?`).

10.1.7 Using Internet-Style Search Syntax

Search techniques common to the popular Internet search engines are supported in Content Server. For example, entering `new product` in the Quick Search field will search for `new <AND> product`, while entering `new, product` will search for `new <OR> product`.

To enable this style of search, set the variable `DoMetaInternetSearch=True`. To disable this style of search, set the variable `DoMetaInternetSearch=False`. This is the default. For more information, see `DoMetaInternetSearch` in *Configuration Reference for Oracle WebCenter Content*.

The following table lists how Content Server interprets common characters.

Character	Interpreted As
Space ()	AND
Comma (,)	OR
Minus (-)	NOT
Phrases enclosed in double-quotes (" <i>any phrase</i> ")	Exact match of entered phrase

The following table lists examples of how Content Server interprets Internet-style syntax in a full-text search.

Query	Interpreted As
new product	new <AND> product
(new, product) images	(new <OR> product) <AND> images
new product -images	(new <AND> product) <AND> <NOT> images
"new product", "new images"	"new product" <OR> "new images"

The following table lists examples of how Content Server interprets Internet-style syntax when searching title metadata using the substring operator.

Query	Interpreted As
new product	dDocTitle <substring> 'new' <AND> dDocTitle <substring> 'product'
new, product	dDocTitle <substring> 'new' <OR> dDocTitle <substring> 'product'
new -product	dDocTitle <substring> 'new' <AND> <NOT> 'product'
"new product"	dDocTitle <substring> 'new product'

10.1.8 Adjusting the Score on OracleTextSearch Results

When you use OracleTextSearch with Oracle Text as the search engine in WebCenter Content, the results of a search by Score are sorted based on the relevancy in documents. In theory, the more relevant the search term is to a document, the higher ranked Score it should receive. In practice, it's not entirely clear how the relevancy Score ranks the importance of some documents over others based on the search term. When a word appears a certain number of times within a document, the Score reaches a maximum at 100 and the top results can be difficult to discern from one another.

For example, if you searched for the term "vacation" in a set of documents, out of seven results, six of them might have a Score of "100" which means they are basically ranked the

same. Having many documents ranked the same doesn't make the sort by Score very meaningful.

Besides sorting by relevance, you can also tell Oracle Text to sort by occurrence. Sorting by occurrence can provide a much more predictable result in how documents would be ranked, and for many cases it can provide a more meaningful sorting of results than relevance.

To tell Oracle Text to sort by occurrence you must make a small component change to the SearchOperatorMap resource. By default, the query used for full-text searching looks like the following code:

```
&lt;td&gt; (ORACLETEXTSEARCH) fullText&lt;/td&gt;  
&lt;td&gt;DEFINESCORE((%V), <strong>RELEVANCE * .1</strong>)&lt;/td&gt;  
&lt;td&gt;text&lt;/td&gt;
```

Override this resource and change it to use OCCURRENCE instead of RELEVANCE. This change forces the resource to use occurrence (also note the change in scale from .1 to .01).

```
&lt;td&gt; (ORACLETEXTSEARCH) fullText&lt;/td&gt;  
&lt;td&gt;DEFINESCORE((%V), <strong> OCCURRENCE * .01</strong>)&lt;/td&gt;  
&lt;td&gt;text&lt;/td&gt;
```

If you run the same search and sort options as mentioned in the earlier example, the results come out differently and each of the seven documents has a unique Score. This provides a clearer understanding of how the items rank. Generally, if the search term appears three times more in one document than another, it has a better chance of being a document you are interested in examining.

 **Note:**

The occurrence ranking also has a maximum count of 100, so if a search term occurs in the document more than that count, the Score result stays at 100.

For your site, using relevance ranking may be more useful than occurrence ranking, however, this option provides an alternate method that might work better for your results.

10.1.9 Customizing Search Results with OracleTextSearch

When users run a search using the Search: Expanded Form, the Search Results page displays an additional menu bar with options that enable users to selectively view search results. The options represent categories used to filter the search results. The options can be context-sensitive, so if only one content item is returned for an option, then it shows only the one result in the menu itself, as shown in [Figure 10-1](#). The default set of options include Content Type, Security Group, and Account.

 **Note:**

Two default menu options on the OracleTextSearch menu for Search Results can be replaced by customized menu options: **Security Group** and **Document Type**.

Figure 10-1 Search Results with OracleTextSearch Default Menu

Search Results Found 11 items

Filter by Category: **Content Type:ADACCT** Security Group Account

Actions					
<input type="checkbox"/>	ID	Title	Date	Author	Actions
<input type="checkbox"/>	PPT_TEST1	PPTTestDoc1	6/6/08	sysadmin	
<input type="checkbox"/>	SEARCHINDEX_000021	TestDoc19	9/4/02	sysadmin	
<input type="checkbox"/>	SEARCHINDEX_000010	TestDoc8	9/4/02	sysadmin	
<input type="checkbox"/>	SEARCHINDEX_000013	TestDoc11	9/4/02	user1	
<input type="checkbox"/>	SEARCHINDEX_000011	TestDoc9	9/4/02	sysadmin	

If more than one content item is found for an option, an arrow is displayed next to the option name. When you move your cursor over the option name, a menu displays the list of the categories found in the search results for that option and the number of content items for each of the categories. You can click any category name on the menu to change the Search Results page to list only those items that match the category

Figure 10-2 shows a list of categories under **Security Group** and the number of items found in each category.

Figure 10-2 Search Results with Snippets Display and Expanded OracleTextSearch Menu

Search Results Found 24 items

Filter by Category: Content Type Security Group Account Author:sysadmin

Administration- (3) Marketing- (1) Public- (14) Secure- (5)
Production- (:)

<input type="checkbox"/>	Description	Content ID	Actions
<input type="checkbox"/>	Title: Chinese Test Author: sysadmin Content Type: ADACCT - Acme Accounting Department Account: MSP Security Group: Administration Native File Extension: doc Release Date: 6/19/08 4:20 PM Snippet: idcnnull SEARCHINDEX_000026 idcnnull sysadmin idcnnull N/A idcnnull idcnnull Score: 3	SEARCHINDEX_000026	
<input type="checkbox"/>	Title: Contemporary Resume RTF Author: sysadmin Content Type: ADACCT - Acme Accounting Department Account: MSP Security Group: Administration Native File Extension: rtf Release Date: 6/16/08 11:10 AM Snippet: idcnnull SEARCHINDEX_000025 idcnnull sysadmin idcnnull N/A idcnnull idcnnull Score: 3	SEARCHINDEX_000025	
<input type="checkbox"/>	Title: errortext Author: sysadmin Content Type: ADACCT - Acme Accounting Department Account: MSP Security Group: Public Native File Extension: txt	SEARCHINDEX_000024	

Element	Description
Filter by Category	Displays the categories used to filter the search results, for example: Content Type, Security Group, Account.

Element	Description
Content Type	(Default) Lists the types and the number of each type of content items in the search results. Clicking one of the content type names changes the Search Results to show only those items that match the content type.
Security Group	(Default) Lists the security groups and number of content items assigned to each group in the search results. Security groups include: Administration, Public, and Secure. Clicking one of the security group names changes the Search Results to show only those items that match the security group.
Account	(Default) Lists the account types and number of items assigned to each account in the search results. Clicking one of the account types changes the Search Results to show only those content items that match the account.

10.1.9.1 About Batch Load File Records

A batch load file is made up of *file records*, which are sets of name/value pairs that specify the action to perform, or the metadata for individual content items, or both.

Note:

Field names and parameters are case sensitive. They must appear in the batch load file exactly as they appear in the following sections. For example, `dDocName` is not the same as `ddocname`, `dDocname`, or `DDOCNAME`.

- Each file record ends with an `<<EOD>>` (end of data) marker.
- A pound sign (`#`) followed by a space at the beginning of a line indicates a comment. The comment character must be followed by a space. For example: `# primaryFile=test.txt` works properly, but `#primaryFile=test.txt` will cause errors.
- The following is an example of a file record:

```
# This is a comment
Action=insert
dDocName=Sample1
dDocType=Document
dDocTitle=Batch Load record insert example
dDocAuthor=sysadmin
dSecurityGroup=Public
primaryFile=links.doc
dInDate=8/15/2001
<<EOD>>
```

10.2 Configuring Full-Text Database Search Index

To set up and use full-text database searching and indexing for SQL Server and other databases:

1. Install WebCenter Content with the Content Server instance and configure it to work with the database.

2. Add the following entry to the `DomainHomeName\ucm\cs\config\config.cfg` file and save the file:

```
SearchIndexerEngineName=DATABASE.FULLTEXT
```

3. Restart the Content Server instance. For instructions, see [Restarting Content Server or Inbound Refinery Using Fusion Middleware Control](#).
4. Rebuild the search index using the Repository Manager.

See Starting the Repository Manager in *Managing Oracle WebCenter Content*.

 **Note:**

If you have difficulty rebuilding the full-text database search index after importing the OCS schema, the message `Unable to create Oracle text collection 'IdcText1'` might be displayed. If this occurs, the solution is to log in as (Content Server) Database administrator and drop the tables `IdcText1` and `IdcText2`.

See Recovering Oracle WebCenter Content in *Administering Oracle Fusion Middleware*.

10.3 Managing Elasticsearch

Let's learn about managing Elasticsearch with WebCenter Content. WebCenter Content communicates with Elasticsearch through REST APIs.

WebCenter Content supports a variety of search indexer engines including `DATABASE.METADATA`, `DATABASE.FULLTEXT`, and `ORACLETEXTSEARCH`. Out of these, `ORACLETEXTSEARCH` provides a rich searching capability including full-text searches with relevancy ranking, complex query structures, and improved performance compared to `DATABASE.FULLTEXT`. However, in a large enterprise setup where content items run into millions and ingestion is quite high, customers find rebuilding the `ORACLETEXTSEARCH` index to be time-consuming.

WebCenter Content communicates with Elasticsearch through REST APIs provided by Elasticsearch. WebCenter Content APIs/services exposed to users remain the same. While the APIs and user interfaces remain mostly untouched in Elasticsearch, rebuild time has reduced significantly. Users will also experience an improved and near real-time search response.

This section covers the following topics:

- [Elasticsearch Features and Benefits](#)
- [Configuring Elasticsearch](#)
- [Migrating Existing Search Indexes to Elasticsearch Server](#)

10.3.1 Elasticsearch Features and Benefits

Elasticsearch has features such as fast rebuild, full rebuild, reindex, sorting, facets, search operators, and searching.

This section covers the following topics:

- [How the Rebuild Feature Works in Elasticsearch?](#)
- [Fast Rebuild](#)

- [Full Rebuild](#)
- [Elasticserver ReIndex](#)
- [Sorting](#)
- [Facets](#)
- [Search Operators and Searching](#)
- [Stemming](#)
- [Snippets](#)
- [Highlighting](#)

10.3.1.1 How the Rebuild Feature Works in Elasticsearch?

Elasticsearch provides a new Rebuild option, Elasticsearch Reindex.

OracleTextSearch in WebCenter Content lets you perform Fast Rebuild or Full Rebuild (With extraction). So, now users can choose from Fast Rebuild, Full Rebuild (With extraction), and Elasticsearch Reindex (Full Rebuild from Elasticsearch).

With Elasticsearch, the Indexer Rebuild dialog has two check boxes: **Use fast rebuild** and **Full rebuild with content extraction**. You can access this dialog box through **Repository Manager** by selecting **Indexer**, then **Collection Rebuild Cycle**, and then **Start**.

10.3.1.2 Fast Rebuild

The Fast Rebuild feature allows the search engine to add new information to the search collection without requiring a full collection rebuild.

A Fast Rebuild is required when adding or removing searchable fields. You can open the Collection Rebuild Cycle window and select the **Use fast rebuild** checkbox and click **OK** to do the fast rebuild.

10.3.1.3 Full Rebuild

The Full Rebuild option rebuilds the search index.

It extracts content and pushes it to the new index in the OpenSearch server using the metadata. This is a time consuming task, and therefore, use with extreme caution.

You can open the Collection Rebuild Cycle window and select the **Full rebuild with content extraction** check box and click **OK** to do the full rebuild.

10.3.1.4 Elasticserver ReIndex

The Elasticserver ReIndex option uses the Elasticsearch API to reindex an existing collection to a new collection.

For reindexing, it reuses already extracted content and metadata available in the active collection. Since this option doesn't need to extract content, it's a faster alternative to **Full Rebuild**.

You can open the Collection Rebuild Cycle window and do not select any of the options. Click **OK** to do the Elasticsearch ReIndex.

There is an alternate option to do indexing. With this option, you can perform Elasticsearch ReIndex instead of Full rebuild with extraction. To invoke Elasticsearch ReIndex, select

Administration, then **Admin Actions**, then **Collection Rebuild Cycle (section)**, and then **Start**. In the current version, Indexer Counters are not implemented for Elasticsearch ReIndex. Also, note that the **Cancel** and **Suspend** buttons might not work.

10.3.1.5 Sorting

Elasticsearch can accept any existing searchable field as `SortField`, so in the search result searchable fields can be sorted.

You don't have to rebuild if you make a field sortable or not-sortable. Changing sortability of a field is required only for sorting results on the user interface. Even if you don't make a field sortable from Configuration Manager, if the field is passed as `SortField`, Elasticsearch sorts the search results by that field.

10.3.1.6 Facets

With WebCenter Content Elasticsearch, the default number of drilldown value is 50.

It is configurable via `MaxElasticSearchDrillDownValues` in configuration or can be passed in the binder. `MaxElasticSearchDrillDownValues` can be any positive integer.

10.3.1.7 Search Operators and Searching

The Search user interface now includes more search operators. The default search operators are: `Contains`, `Matches`, `Has Word Prefix`, `Starts`, `Ends`, `Substring`, and `Not Matches`.

Searching

- All search features supported with `OracleTextSearch` are supported with Elasticsearch as well.
- Elasticsearch does not have **Optimized** and **Zone** fields.
- With Elasticsearch, metadata field names are expected to be case-sensitive during search, but the `QueryText` is case-insensitive.
- Queries using the `MATCHES` operator matches for the case-insensitive exact match of the query text on all searchable fields.
- Elasticsearch does not throw any error if a non-existing field or metadata is searched for. Instead, it shows zero results.
- With Elasticsearch, WebCenter Content gives valid results without ignoring any special characters.
- In the search performed from WebCenter Content user interface, WebCenter Content trims the trailing spaces and then the trimmed value is used as query text. In WebCenter Content user interface, spaces at the end and/or at the start of the query text lead to different results compared to `OracleTextSearch`. In case of RIDC, Elasticsearch returns search results considering trailing spaces also.
- Text within HTML tags such as `<script>..</script>`, `<style>..</style>`, `<! -- -->` would not be tokenized and hence not searchable.
- WebCenter Content does not allow searching on non-existent or non-searchable fields. It would throw an error message "<fieldname> is not a searchable field".

Searching Stop Words

The stop words are commonly used words that are excluded from searches to help index and parse web pages faster. For the stop words, Elasticsearch does not create an index entry.

- This list is derived from the OTS stop words.
"Mr", "Mrs", "Ms", "a", "all", "almost", "also", "although", "an", "and", "any", "are", "as", "at", "be", "because", "been", "both", "but", "by", "can", "could", "d", "did", "do", "does", "either", "for", "from", "had", "has", "have", "having", "he", "her", "here", "hers", "him", "his", "how", "however", "i", "if", "in", "into", "is", "it", "its", "just", "ll", "me", "might", "my", "no", "non", "nor", "not", "of", "on", "one", "only", "onto", "or", "our", "ours", "s", "shall", "she", "should", "since", "so", "some", "still", "such", "t", "than", "that", "the", "their", "them", "then", "there", "therefore", "these", "they", "this", "those", "though", "through", "thus", "to", "too", "until", "ve", "very", "was", "we", "were", "what", "when", "where", "whether", "which", "while", "who", "whose", "why", "will", "with", "would", "yet", "you", "your", "yours".
- When you are searching with a stop word, Elasticsearch treats you as if you are searching with an empty string instead of that word.
- The stop words are applicable only on search queries that are `Full-Text Search`, `Quick Search`, `Contains`, `Has Word Prefix`.
- A query (`Full-Text Search`, `Quick Search`, and `Contains`) composed of a stop word or a phrase composed of only stop words would return all results as if it is an empty search. For example, a query on the word *this* returns all hits as *this* is defined as a stop word.
- A query (`Has Word Prefix`) composed of a stop word or a phrase composed of only stop words would return no results. For example, a query on the word *this* returns all hits as *this* is defined as a stop word.
- You can query on phrases that contain stop words as well as non-stop words. In such cases, the phrase is searched as if the stop word in the phrase does not exist. For example, a query on phrase *this title* returns hit as if you are only searching the word *title* as *this* is a stop word.

10.3.1.8 Stemming

Stemming is applicable only on text queries: `Contains`, `Has Word Prefix`, `Full Text Search`, and `QuickSearch`.

Stemming words differ from `OracleTextSearch` to `Elasticsearch` because internally the search engines use different dictionaries. For example, in `OracleTextSearch`, a search query for the word “find” returns *found*, *finds*, *finding* and for the word “make”, the query returns *make*, *made*, *makes*, *making*. In `Elasticsearch`, the search result for “find” shows *find*, *finds*, *finding* and for “make” the result shows *make*, *makes*, *making*. “Found” and “made” are not shown in `Elasticsearch` results, but they do in `OracleTextSearch`.

10.3.1.9 Snippets

You can enable the Snippets feature with `Elasticsearch` by setting the following configuration entry in the `config.cfg` file: `ElasticSearchDisableSearchSnippet=false`.

Keep in mind that this feature can affect search query performance. Snippets displayed with `Elasticsearch` are different from those that are displayed with `OracleTextSearch`. Look-and-feel of snippets in `Elasticsearch` is different from the look-and-feel of `OracleTextSearch` snippets. With `Elasticsearch` one complete sentence is equal to one snippet.

In an `Elasticsearch` result, if the document is resulted in search because of only metadata match but not from the extracted content of the document, only that metadata value is shown as snippet.

10.3.1.10 Highlighting

Elasticsearch highlights the search keywords but does not give pointers to the previous and next match.

OracleTextSearch highlights the search keywords along with pointers to next and previous match.

Elasticsearch highlights returns the extracted content of a document only when there is a match in the extracted content. Highlighting shows metadata of the document only if there is any match with that particular metadata value.

If the match is limited to metadata of the document, only the matched metadata fields are listed but not the extracted content.

10.3.2 Configuring Elasticsearch

In this section, you'll learn how you can configure Elasticsearch for WebCenter Content. Before configuring Elasticsearch for WebCenter Content, you'll need to secure nodes of the cluster, secure Elasticsearch, and start the Base node first and then other nodes.

To configure Elasticsearch for WebCenter Content, follow these steps:

 **Note:**

Indices in Elasticsearch are stored as files on disk. For Elasticsearch to work, it requires large amount of free disk space. For more information, contact [Oracle support](#).

1. Download and unzip 7.6 or newer 7.x versions of Elasticsearch from <https://www.elastic.co/downloads/past-releases#elasticsearch>.
2. Navigate to `<IdcHomeDir>/components/ElasticSearch/scripts`.

 **Note:**

WebCenter Content provides a script `SecureES.sh` or `SecureES.cmd` that automates the steps to secure the Elasticsearch nodes (one or more) of an Elasticsearch cluster. It is assumed that Elasticsearch cluster is installed on all the nodes of the cluster. It can be a single node cluster also. If it is multi-node cluster, it should have at least 3 master-eligible nodes.

3. Run script on all the nodes of the cluster. Before running a node, it should be secured first. Base node should be started first and then other nodes.

To download an Elasticsearch client JAR, follow these steps:

1. Go to <https://repo1.maven.org/maven2/org/elasticsearch/client/elasticsearch-rest-client/> and browse for the relevant version.
2. Download the required version of the JAR file in `<IdcHomeDir>/components/ElasticSearch/lib/`.

This section covers the following topics:

- [Updating ESnode.properties](#)
- [Using SecureES.sh on Unix](#)
- [Using SecureES.cmd on Windows](#)
- [Securing Elasticsearch](#)
- [Securing Other Nodes of Cluster](#)
- [Start Elasticsearch Cluster](#)
- [Configuring Elasticsearch for WebCenter Content](#)
- [Monitoring Elasticsearch Cluster Health](#)
- [Configuring Index Settings](#)

10.3.2.1 Updating ESnode.properties

The `ESnode.properties` file needs to be updated before setting up all the Elasticsearch nodes that would be secured as part of the initial cluster setup.

Update configuration for all the nodes that are going to be part of the setup before securing them. The `ESnode.properties` file should be present in the same folder where script file is residing. Follow these steps:

- **Configure individual nodes:** Configure all the nodes that are planned for the initial cluster setup. Provide the entries (`node1`, `node2`, `node3`,, `node{n}`) as the number of nodes being created as part of the setup.

```
node{n}_ES_HOME
node{n}_node_name
node{n}_http_port
```

Where `{n}` is the `n`th node in the setup. For example:

```
##Node1 (BASE NODE)
node1_ES_HOME=/ESuser/elasticsearch-7.6.0_1
node1_node_name=nodeA
node1_http_port=9201
```

```
##Node2
node2_ES_HOME=/ESuser/elasticsearch-7.6.0_2
node2_node_name=nodeB
node2_http_port=9202
```

- **Common configuration for all nodes:**
 - `BASE_ES_HOME`: This should be same as `node1_ES_HOME` or where `config/{certificate_name}` and `config/elasticsearch.keystore` are accessible to all nodes. For example, `BASE_ES_HOME=/ESuser/elasticsearch-7.6.0_1`.
 - `cluster_name`: Name of the cluster. For example, `cluster_name=wcc-elasticsearch`.
 - `certificate_name`: Certificate name (extension must be `.p12`) for which cluster will be secured. For example, `certificate_name=elastic-certificates.p12`.
 - `wcc_es_admin_user`: User with which WebCenter Content will communicate with Elasticsearch. For example, `wcc_es_admin_user=wccesadmin`.

- `cluster_initial_master_nodes`: All node names that are part of the initial cluster setup. For example, `cluster_initial_master_nodes=["nodeA", "nodeB", "nodeC", ..., "node{N}"]`.
- `discovery_seed_hosts`: All hostnames where these nodes are going to be configured. This is mandatory only if Elasticsearch cluster is horizontal. For example, `discovery_seed_hosts=["host1.example.com", "host2.example.com", "host3.example.com", ..., "host{n}.example.com"]`
- `WINDOWS_CURL_HOME`: It is required for windows and only for base node (node1). For example, `C:\curl-7.72.0_5-win64-mingw\bin\curl.exe` where `WINDOWS_CURL_HOME = C:\curl-7.72.0_5-win64-mingw`.

10.3.2.2 Using SecureES.sh on Unix

The script automates the steps to secure Elasticsearch cluster nodes on Unix.

Usage:

For help:

```
./SecureES.sh -h or --help
```

To run script:

```
./SecureES.sh -n <nodenumber>
```

For example, if you have 3 nodes to secure, it is mandatory to run the script on the first node and then other nodes.

```
./SecureES.sh -n 1
```

```
./SecureES.sh -n 2
```

```
./SecureES.sh -n 3
```

10.3.2.3 Using SecureES.cmd on Windows

The script automates the steps to secure Elasticsearch cluster nodes on Windows.

Usage:

To run the script:

```
SecureES.cmd -n <nodenumber>
```

For example, if you have 3 nodes to secure, it is mandatory to run the script on the first node and then other nodes.

```
SecureES.cmd -n 1
```

```
SecureES.cmd -n 2
```

```
SecureES.cmd -n 3
```

10.3.2.4 Securing Elasticsearch

Follow these steps to secure First (Base) Node:

1. Navigate to <ELASTIC_COMPONENT_DIR>/scripts.
2. Run the script. For windows, run `SecureES.cmd -n <nodenumber>` and for Unix, run `./SecureES.sh -n <nodenumber>`.
3. You will be asked to enter the name of the certificate. If you don't enter, it will take the default name `elastic-certificates.p12`. Certificate should have the extension `p12`.

```
*****Create certificate for secured Communication*****
Enter certificate name (extension must be .p12) > [elastic-certificates.p12]

WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by org.bouncycastle.jcajce.provider.drbg.DRBG
 (file:/elasticsearch/7.6.0/cluster/elasticsearch-7.6.0-test/lib/
b/tools/security-cli/bcprov-jdk15on-1.61.jar) to constructor sun.security.provid
er.Sun()
WARNING: Please consider reporting this to the maintainers of org.bouncycastle.j
cajce.provider.drbg.DRBG
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflect
ive access operations
WARNING: All illegal access operations will be denied in a future release
Enter password for elastic-certificates.p12 : █
```

Give a password for the certificate.

```
*****Add certificate password to keystore*****
The elasticsearch keystore does not exist. Do you want to create it? [y/N]y
Created elasticsearch keystore in /elasticsearch/7.6.0/cluster/
elasticsearch-7.6.0-test/config
```

4. Add the certificate password to the keystore. If a elasticsearch keystore is not present, it will ask you to create one. Press `y` to create the keystore and proceed. Note that choosing `N` here will not secure the node.

```
*****Create certificate for secured Communication completed*****
*****
*****Add certificate password to keystore*****
The elasticsearch keystore does not exist. Do you want to create it? [y/N]y█
```

You will be asked to enter the password 4 times. Enter the above used certificate password.

```
Created elasticsearch keystore in /elasticsearch/7.6.0/cluster/
elasticsearch-7.6.0-test/config
Enter value for xpack.security.transport.ssl.keystore.secure_password:
Enter value for xpack.security.transport.ssl.truststore.secure_password:
Enter value for xpack.security.http.ssl.keystore.secure_password:
Enter value for xpack.security.http.ssl.truststore.secure_password:
```

5. Set up the password for the reserved user, `elastic`. Enter a password for the user `elastic`. This will be used in later step to create a user to communicate with WebCenter Content.

```
*****Setup bootstrap password for user 'elastic'*****
Enter value for bootstrap.password:
*****Setting Bootstrap password completed*****
```

6. Create a user to communicate with the WebCenter Content. You will be asked to enter a user name and password. Enter the name or press ENTER to use the default name `wccesadmin`.

```
*****Create an user to communication with UCM server*****
Enter username to communicate with UCM > [wccesadmin]
Enter password to communicate with UCM >
Enter host password for user 'elastic':█
```

Enter the password set to the user `elastic`.

```
*****Create an user to communication with UCM server*****
Enter username to communicate with UCM > [wccesadmin]
Enter password to communicate with UCM >
Enter host password for user 'elastic':
response code -> 200
User created -> wccesadmin
*****User creation completed*****
```

7. Once the setup is done, you will see the setup complete message.
8. Do not start the node now.

10.3.2.5 Securing Other Nodes of Cluster

You need to run the script to secure the nodes of a cluster.

Follow these steps to secure other nodes of cluster:

1. Navigate to `<ELASTIC_COMPONENT_DIR>/scripts`.
2. Run the script. The cluster name should be same for all the nodes. The node names should be unique.
For Unix:

```
./SecureES.sh -n 2
```


For Windows:

```
SecureES.cmd -n 2
```

3. Once the setup is done, you will see the setup complete message.
4. Do not start the node now.

10.3.2.6 Start Elasticsearch Cluster

After securing or configuring all the nodes of the cluster, you can start all the nodes.

After securing all the nodes, go to `<ES_HOME>/bin` of each node and run

```
./elasticsearch
```

Start the base node (node1) first and then start other nodes.

You should start the BASE NODE (node1) first and then start other nodes.

After nodes are started, you can access each node with `wccesadmin`.

```
https://<hostname>:<nodeport>
```

10.3.2.7 Configuring Elasticsearch for WebCenter Content

Before you configure Elasticsearch for WebCenter Content, you need to do the mandatory initial configuration settings along with enabling the Elasticsearch search indexer.

To configure Elasticsearch for WebCenter Content, follow these steps:

1. Start the WebCenter Content managed server.
2. Select **Administration**, then **Elasticsearch**, and then **Elasticsearch Configuration**.
3. In the Elasticsearch Configuration page, enter the values for the following fields as shown in the figure below:
 - **Elasticsearch Nodes to connect** - comma-separated list of Elasticsearch nodes of a cluster
 - **Username** - user name to connect to Elasticsearch
 - **Password** - user password
 - **Certificate Path** - absolute path of the certificate using the cluster which is secured
 - **Password** - certificate password

Elasticsearch Nodes to connect* Comma-separated list of Elasticsearch master eligible nodes of a cluster (Ex:host1:port1,host2:port2).	<input type="text" value="node-1@example.com, node-2@example.com, node-3@example.com"/>
Username* Username to connect to Elasticsearch.	<input type="text" value="wccesadmin"/>
Password* User Password.	<input type="password" value="*****"/>
Certificate Path Full file path of the certificate using which the cluster is secured.	<input type="text" value="/elasticsearch/7.6.0/cluster/elasticsearch-7.6.0-test"/>
Password Certificate Password.	<input type="password" value="*****"/>
<input type="button" value="Update"/>	

10.3.2.8 Monitoring Elasticsearch Cluster Health

For WebCenter Content to function properly, it is important to have a good Elasticsearch cluster health.

This feature is introduced to monitor Elasticsearch health at an interval of 1 hour. If the status of the Elasticsearch health issue is Red or connection is down, then an alert will be added and monitored every minute until Elasticsearch health status turns Green or Yellow. Once the status of the Elasticsearch health turns Green or Yellow, health alert will be removed automatically and continue to monitor every hour thereafter.

The figure below is showing Elasticsearch connection is down temporarily.

Alert

- Elasticsearch connection seems to be down temporarily. Please check again.

Search

Title:

Content ID:

Release Date: From To

Full-Text Search:

Sort By:

10.3.2.9 Configuring Index Settings

You can configure shards and replicas for different indexes as per the required data.

This new feature allows to customize shards and replica counts for each Elasticsearch index. As per Elasticsearch design, each index in Elasticsearch would be mapped to a security group in WebCenter Content. The indexes will be created during:

- server startup
- new Security Group is added to the system
- collection rebuild or reindex
- migration from other search engines to Elasticsearch

Shards and replicas will be allotted to the indexes when they are created in the system based on the user configuration. Any updates to these settings will be reflected only after next Full Rebuild or Reindex cycle. You can set limit on the shards and replicas counts.

Shards count: It should be an integer value ranging from 5 to 300. The default value is 5.

Replicas count: It should be either 1 or 2. The default value is 1.

If connection with Elasticsearch is not established and no indexes are created yet, an additional optional alert will appear along with the existing Elasticsearch alerts.

Alert

- To change default index settings, Please do ElasticSearch index settings configuration (Optional).
- Please complete the ElasticSearch server configuration.

On clicking this alert message, you will be redirected to ElasticSearch Index Settings page where you can customize shards and replicas for each security group (index) existing in the system.

Indexes with these customized settings will be created when successful connection with Elasticsearch is established. In case of migration to Elasticsearch from other search engines, migration needs to be successful for these indexes to get created with the customized settings.

For already configured Elasticsearch instances, the indexes are created with the default index settings.

To configure index settings:

1. Select **Administration**, then **ElasticSearch**, and then **ElasticSearch Index Settings**.
2. In the Configure Index Settings page, you (admin) can configure indexes with desired shards and replicas count. The updated shard and replica settings will be reflected after:
 - next Full Rebuild or Reindex cycle
 - establishing successful connection in a fresh instance
 - migration if you are switching over from a different search engine

You can not update specific indexes. Once the **Update** button is clicked, all the records will be updated.

Configure Index Settings

By default the indices are created with default number of shards(5) and replicas(1). This form allows users to update shards and replica count of indices. Updated values will be reflected in Elasticsearch only after next full rebuild/reindex cycle.

ES Index	Shard Count	Replica Count
public	6	1
secure	5	2
testgroup	6	2

3. To view all the active indexes and their shard and replica settings retrieved from the Elasticsearch server, select the Active Index Settings tab.

View Active Index Settings

This page allows users to view all the active indices and their shards, replica settings retrieved from Elasticsearch server.

ElasticSearch Active Indices

	ES Index	Shard Count	Replica Count
1	es1_public	6	1
2	es1_secure	5	2
3	es1_testgroup	6	2

Adding New Security Group

If a new security group is added after successful connection to the Elasticsearch server from WebCenter Content, its corresponding index will be created in Elasticsearch with default shard (5) and replica (1) counts.

If you want to customize its settings, you can do it from the ElasticSearch Index Settings page, but they will be reflected only after next rebuild or reindex cycle.

10.3.3 Migrating Existing Search Indexes to Elasticsearch Server

When you migrate from the active search index to the Elastic server, the active index is changed to es1.

 **Note:**

During the migration of 5 million records from OTS to Elasticsearch, for every text field, you need to create 4 types of mappings for various search operations in Elasticsearch. Elasticsearch considers these mappings as different fields. For example, A text field `dDocTitle` will have `dDocTitle`, `dDocTitle.normalize`, `dDocTitle.keyword`, `dDocTitle.stem`, and they are considered as 4 fields, not one field. So, if you have 250 text fields, Elasticsearch will consider them as $250 * 4 = 1000$ fields. For metadata other than text fields, there is only one mapping. After deleting unwanted metadata fields, you will be able to perform the migration activity.

If an existing WebCenter Content instance is configured to use the ORACLETEXTSEARCH (OTS) search engine, then the active index `ots1/ots2` will be used to fetch the already extracted content. A successful migration activity will change the active search index to the Elastic server, `es1`.

Select **Administration** and then Configuration for <hostname with port> page is displayed. It will display `ots1/ots2` as an active index as shown below:

```
Search Engine:: ELASTICSEARCH
Index Engine Name: ELASTICSEARCH
Active Index: ots1
```

To migrate, select **Administration** and then **ElasticSearch**. The ElasticSearch Migration page is displayed. Select the appropriate search engine from the **Search Engine to Migrate** drop-down menu as shown below:

ElasticSearch Migration Page

[Administration](#) --> ElasticSearch Migration

ElasticSearch Migration Config

Search Engine to Migrate
The search engine to migrate to elasticsearch server. ORACLETEXTSEARCH ▼

Migration Batch Size
Number of content items to be considered in each batch. To avoid memory issues, it is advisable to choose wisely when extracted content is part of migration data. 25 ▼

Migrate Metadata Only
If only the metadata should be migrated to elasticsearch server. False ▼

Migration Batch Size determines the number of documents batched together to push to the Elasticsearch server. We need to carefully choose the batch size, as in case of the full-text search engines like ORACLETEXTSEARCH, the batch will also include the text-extracted content of the documents along with its metadata.

Migrate Metadata Only indicates whether we need to push the text-extracted content to the Elasticsearch server. In case of the full-text search engines like ORACLETEXTSEARCH, this should be always set to **False**. It means the text-extracted content is also pushed to the Elasticsearch server.

Upon starting a migration activity, a table of all recent migration jobs and its status details will be listed as shown below:

ElasticSearch Migration Status

*The operations performed will act only on the latest migration run.

Run	User	Start Date	Last Updated Dat	Status	Migrating Index	Batch Size	IsMetaOnly	ElasticServer	Total Items	Processed Items	Failed Items
1	weblogic	1/17/20 5:09 PM	1/17/20 5:09 PM	Running	ots1	25	0	localhost:9200	5000	0	0

You can pause or resume an on-going migration activity and can retry the latest failed migration activity, if any. A completed migration activity details are shown below:

ElasticSearch Migration Status

Run	User	Start Date	Last Updated Dat	Status	Migrating Index	Batch Size	IsMetaOnly	ElasticServer	Total Items	Processed Items	Failed Items
1	weblogic	1/17/20 5:09 PM	1/17/20 5:10 PM	Completed	ots1	25	0	localhost:9200	5000	5000	0

A successful migration activity will switch active index to **es1** as shown below:

Search Engine:: ELASTICSEARCH
Index Engine Name: ELASTICSEARCH
Active Index: **es1**



Note:

A successful migration activity will remove the migration alert banner.

10.4 Managing OpenSearch

Let's learn about managing OpenSearch with WebCenter Content.

Oracle Cloud Infrastructure (OCI) Search Service with OpenSearch is an insight engine offered as an Oracle-managed service. Without any downtime, Oracle automates patching, updating, upgrading, backing up, and resizing the service. You can store, search, and analyze large volumes of data quickly and see results in near real-time.

WebCenter Content communicates with OpenSearch through REST APIs. WebCenter Content APIs or services exposed to the users remain the same.

This section covers the following topics:

- [OpenSearch Features and Benefits](#)
- [Configuring OpenSearch](#)
- [Migrating Existing Search Indexes to OpenSearch](#)

10.4.1 OpenSearch Features and Benefits

OpenSearch has features such as fast rebuild, full rebuild, reindex, sorting, facets, search operators, and searching.

This section covers the following topics:

- [How the Rebuild Feature Works in OpenSearch?](#)
- [Fast Rebuild](#)
- [Full Rebuild](#)
- [OpenSearch ReIndex](#)
- [Sorting](#)
- [Facets](#)
- [Search Operators and Searching](#)
- [Stemming](#)
- [Snippets](#)
- [Highlighting](#)

10.4.1.1 How the Rebuild Feature Works in OpenSearch?

OpenSearch provides a new Rebuild option, OpenSearch Reindex.

OpenSearch in WebCenter Content lets you perform Fast Rebuild or Full Rebuild (With extraction). So, now users can choose from Fast Rebuild, Full Rebuild (With extraction), and OpenSearch Reindex (Full Rebuild from Elasticsearch).

With OpenSearch, the Indexer Rebuild dialog has two check boxes: **Use fast rebuild** and **Full rebuild with content extraction**. You can access this dialog box through **Repository Manager** by selecting **Indexer**, then **Collection Rebuild Cycle**, and then **Start**.

10.4.1.2 Fast Rebuild

The Fast Rebuild feature allows the search engine to add new information to the search collection without requiring a full collection rebuild.

A Fast Rebuild is required when adding or removing searchable fields. You can open the Collection Rebuild Cycle window and select the **Use fast rebuild** checkbox and click **OK** to do the fast rebuild.

10.4.1.3 Full Rebuild

The Full Rebuild option rebuilds the search index.

It extracts content and pushes it to the new index in the OpenSearch server using the metadata. This is a time consuming task, and therefore, use with extreme caution.

You can open the Collection Rebuild Cycle window and select the **Full rebuild with content extraction** check box and click **OK** to do the full rebuild.

10.4.1.4 OpenSearch ReIndex

The OpenSearch ReIndex option uses the OpenSearch API to reindex an existing collection to a new collection.

For reindexing, it reuses already extracted content and metadata available in the active collection. Since this option doesn't need to extract content, it's a faster alternative to **Full Rebuild**.

You can open the Collection Rebuild Cycle window and do not select any of the options. Click **OK** to do the OpenSearch ReIndex.

There is an alternate option to do indexing. With this option, you can perform OpenSearch ReIndex instead of Full rebuild with extraction. To invoke OpenSearch ReIndex, select **Administration**, then **Admin Actions**, then **Collection Rebuild Cycle (section)**, and then **Start**. In the current version, Indexer Counters are not implemented for OpenSearch ReIndex. Also, note that the **Cancel** and **Suspend** buttons might not work.

10.4.1.5 Sorting

OpenSearch can accept any existing searchable field as `SortField`, so in the search result searchable fields can be sorted.

You don't have to rebuild if you make a field sortable or not-sortable. Changing sortability of a field is required only for sorting results on the user interface. Even if you don't make a field

sortable from Configuration Manager, if the field is passed as `SortField`, OpenSearch sorts the search results by that field.

10.4.1.6 Facets

With WebCenter Content OpenSearch, the default number of drilldown value is 50.

It is configurable via `MaxOpenSearchDrillDownValues` in configuration or can be passed in the binder. `MaxOpenSearchDrillDownValues` can be any positive integer.

10.4.1.7 Search Operators and Searching

The Search user interface now includes more search operators. The default search operators are: `Contains`, `Matches`, `Has Word Prefix`, `Starts`, `Ends`, `Substring`, and `Not Matches`.

Searching

- All search features supported with `OracleTextSearch` are supported with `OpenSearch` as well.
- `OpenSearch` does not have **Optimized** and **Zone** fields.
- With `OpenSearch`, metadata field names are expected to be case-sensitive during search, but the `QueryText` is case-insensitive.
- Queries using the `MATCHES` operator matches for the case-insensitive exact match of the query text on all searchable fields.
- `OpenSearch` does not throw any error if a non-existing field or metadata is searched for. Instead, it shows zero results.
- With `OpenSearch`, WebCenter Content gives valid results without ignoring any special characters.
- In the search performed from WebCenter Content user interface, WebCenter Content trims the trailing spaces and then the trimmed value is used as query text. In WebCenter Content user interface, spaces at the end and/or at the start of the query text lead to different results compared to `OracleTextSearch`. In case of `RIDC`, `OpenSearch` returns search results considering trailing spaces also.
- Text within HTML tags such as `<script>..</script>`, `<style>..</style>`, `<! -- -->` would not be tokenized and hence not searchable.
- `OpenSearch` does not allow searching on non-existent or non-searchable fields. It would throw an error message "`<fieldname> is not a searchable field`".

Searching Stop Words

The stop words are commonly used words that are excluded from searches to help index and parse web pages faster. For the stop words, `OpenSearch` does not create an index entry.

- This list is derived from the OTS stop words.
"Mr", "Mrs", "Ms", "a", "all", "almost", "also", "although", "an", "and", "any", "are", "as", "at", "be", "because", "been", "both", "but", "by", "can", "could", "d", "did", "do", "does", "either", "for", "from", "had", "has", "have", "having", "he", "her", "here", "hers", "him", "his", "how", "however", "i", "if", "in", "into", "is", "it", "its", "just", "ll", "me", "might", "my", "no", "non", "nor", "not", "of", "on", "one", "only", "onto", "or", "our", "ours", "s", "shall", "she", "should", "since", "so", "some", "still", "such", "t", "than", "that", "the", "their", "them", "then", "there", "therefore", "these", "they", "this", "those", "though", "through", "thus", "to", "too", "until", "ve", "very", "was", "we", "were", "what", "when", "where", "whether", "which", "while", "who", "whose", "why", "will", "with", "would", "yet", "you", "your", "yours".

- When you are searching with a stop word, OpenSearch treats you as if you are searching with an empty string instead of that word.
- The stop words are applicable only on search queries that are `Full-Text Search`, `Quick Search`, `Contains`, `Has Word Prefix`.
- A query (`Full-Text Search`, `Quick Search`, and `Contains`) composed of a stop word or a phrase composed of only stop words would return all results as if it is an empty search. For example, a query on the word *this* returns all hits as *this* is defined as a stop word.
- A query (`Has Word Prefix`) composed of a stop word or a phrase composed of only stop words would return no results. For example, a query on the word *this* returns all hits as *this* is defined as a stop word.
- You can query on phrases that contain stop words as well as non-stop words. In such cases, the phrase is searched as if the stop word in the phrase does not exist. For example, a query on phrase *this title* returns hit as if you are only searching the word *title* as *this* is a stop word.

10.4.1.8 Stemming

Stemming is applicable only on text queries: `Contains`, `Has Word Prefix`, `Full Text Search`, and `QuickSearch`.

Stemming words differ from OracleTextSearch to OpenSearch because internally the search engines use different dictionaries. For example, in OracleTextSearch, a search query for the word “find” returns *found*, *finds*, *finding* and for the word “make”, the query returns *make*, *made*, *makes*, *making*. In OpenSearch, the search result for “find” shows *find*, *finds*, *finding* and for “make” the result shows *make*, *makes*, *making*. “Found” and “made” are not shown in OpenSearch results, but they do in OracleTextSearch.

10.4.1.9 Snippets

You can enable the Snippets feature with OpenSearch by setting the following configuration entry in the `config.cfg` file: `OpenSearchDisableSearchSnippet=false`.

Keep in mind that this feature can affect search query performance. Snippets displayed with OpenSearch are different from those that are displayed with OracleTextSearch. Look-and-feel of snippets in OpenSearch is different from the look-and-feel of OracleTextSearch snippets. With OpenSearch one complete sentence is equal to one snippet.

In an OpenSearch result, if the document is resulted in search because of only metadata match but not from the extracted content of the document, only that metadata value is shown as snippet.

10.4.1.10 Highlighting

OpenSearch highlights the search keywords but does not give pointers to the previous and next match.

OracleTextSearch highlights the search keywords along with pointers to next and previous match.

OpenSearch highlights returns the extracted content of a document only when there is a match in the extracted content. Highlighting shows metadata of the document only if there is any match with that particular metadata value.

If the match is limited to metadata of the document, only the matched metadata fields are listed but not the extracted content.

10.4.2 Configuring OpenSearch

In this section, you'll learn how to configure OpenSearch for WebCenter Content, monitor cluster health, and configure index settings.

The WebCenter Content connects to an existing OCI OpenSearch cluster.

This section covers the following topics:

- [Configuring OpenSearch for WebCenter Content with OCI](#)
- [Configuring OpenSearch for WebCenter Content](#)
- [Monitoring OpenSearch Cluster Health](#)
- [Configuring Index Settings](#)

10.4.2.1 Configuring OpenSearch for WebCenter Content with OCI

To configure OpenSearch for WebCenter Content with OCI, follow these steps:

1. For WebCenter Content instance, open a shell logged in as the user that owns WebCenter Content domain files and directories (typically user `oracle`).
2. Change the directory to `<WCC domain path>`.
3. To get the OpenSearch certificate, in a shell of WebCenter Content instance, run the following command:

```
openssl s_client -showcerts -connect <OpenSearch private IP>:9200 </dev/
null
| sed -n -e '/-BEGIN/,/-.END/ p' > cert.pem
```

4. To test the connection from WebCenter Content instance to the OpenSearch cluster:

```
/usr/bin/curl -u <username>:<password> https:<OpenSearch private IP>:9200 -
insecure
```

This is merely a simple test to see if WebCenter Content instance can reach the OS cluster. If successful, it will return the following:

```
[oracle@wccctestinstance ~]$ /usr/bin/curl -u <username>:<password> https://
<OpenSearch private IP>:9200
{
  "name" : "opensearch-master-0",
  "cluster_name" :
"amaaaaaa16hvfiquqzmbvklzsowhydlrvpdfa544kitmgdymnugepq5nkwq",
  "cluster_uuid" : "EtrnIgjXQmmuK4gBdf02xg",
  "version" : {
    "distribution" : "opensearch",
    "number" : "2.11.0",
    "build_type" : "tar",
    "build_hash" : "unknown",
    "build_date" : "2024-05-28T05:20:26.940869407Z",
    "build_snapshot" : false,
    "lucene_version" : "9.7.0",
    "minimum_wire_compatibility_version" : "7.10.0",
```

```

    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}

```

5. In the shell, change the directory to <WCC domain path>/ucm/cs/config. If this is a clustered WebCenter Content, the `config.cfg` file will be located under the file share used by the WebCenter Content.
6. Edit the `config.cfg` file. Add the following entry:

```
SearchIndexerEngineName=OPENSEARCH
```

If `SearchIndexerEngineName` is set to `OracleTextSearch` or `DATABASE.METADATA`, either delete or comment out those lines.

7. Save and exit the file.
8. Restart the WebCenter Content managed server(s).
9. Open the WebCenter Content page.
10. Select **Administration**, then **OpenSearch**, and then **OpenSearch Configuration**.
11. In the OpenSearch Configuration page, enter the values for the fields as explained in [Configuring OpenSearch for WebCenter Content](#). Click the **Update** button.

If the WebCenter Content connects to OpenSearch, it will show the following status:

- Green: OpenSearch was configured for three master and data nodes.
- Yellow: OpenSearch was configured for single node cluster. This is due to the single node not being able to distribute its replicate shards. It can be ignored, it won't affect indexing and searches.

The initial configuration for OpenSearch doesn't require an initial collection rebuild. Once the parameters in the OpenSearch Configuration page are completed and the WebCenter Content is connected to OpenSearch, a collection rebuild isn't required.

As part of the configuration, the OpenSearch indices (based on WebCenter Content security groups) will be created. Items can be checked in and searched for. If items were checked in before, they also are searchable.

Note:

If a new metadata field is to be created or if fields from another WebCenter Content instance will be migrated using CMU, after the creation or CMU import, immediately run the Fast Rebuild.

Until the Fast Rebuild is run:

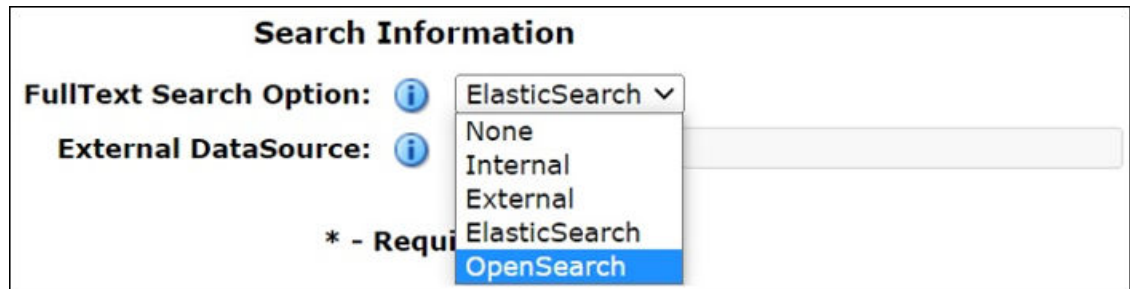
- Do not check in new content with the new field value populated.
- Do not archive import content that have the field value populated.

The Fast Rebuild will take a very long time to complete if it has to index field values in fields that didn't already have that field in the index. For more details, see [ElasticSearch Fast Rebuild Takes a Long Time to Complete](#).

10.4.2.2 Configuring OpenSearch for WebCenter Content

Before you configure OpenSearch for WebCenter Content, you need to do the mandatory initial configuration settings along with enabling the OpenSearch search indexer.

The initial configuration settings are shown in the figure below:



If the above step is not done, stop the WebCenter Content managed server and set the below parameter in the `config.cfg` file:

```
SearchIndexerEngineName=OPENSEARCH
```

Now, start the WebCenter Content managed server.

To configure OpenSearch for WebCenter Content, follow these steps:

1. Start the WebCenter Content managed server.
2. Select **Administration**, then **OpenSearch**, and then **OpenSearch Configuration**.
3. In the OpenSearch Configuration page, enter the values for the following fields as shown in the figure below:
 - **OpenSearch Cluster** - comma-separated list of OpenSearch nodes of a cluster
 - **OpenSearch Certificate Type to connect** - certificate type to connect to OpenSearch
 - **Root Certificate Path** - absolute path of the root certificate
 - **Authorization** - method to communicate with OpenSearch

 **Note:**

You need to use **Basic Auth** as the authorization method if you are using OpenSearch 2.x.

Search Index migration completion status
If the migration of search indices to OpenSearch server completed successfully (Info-Only).

OpenSearch Cluster*
OpenSearch cluster node to connect (e.g. host:port)

OpenSearch Certificate Type to connect*
Certificate Type to use to connect with OpenSearch

Root Certificate Path*
Full path of the Root Certificate (must be .pem file).

Authorization*
Authorization Method to communicate with OpenSearch

OpenSearch Server Properties

Property Name	Property Value
Cluster Name	opensearch
Status	GREEN
Version	[1.2.4]
Total Number of Nodes	6
Master-eligible Nodes	3
Data Nodes	3
Ingest Nodes	3
Coordinating only Nodes	0

10.4.2.3 Monitoring OpenSearch Cluster Health

For WebCenter Content to function properly, it is important to have a good OpenSearch cluster health.

This feature is introduced to monitor OpenSearch health at an interval of 1 hour. If the status of the OpenSearch health issue is Red or connection is down, then an alert will be added and monitored every minute until OpenSearch health status turns Green or Yellow. Once the status of the OpenSearch health turns Green or Yellow, health alert will be removed automatically and continue to monitor every hour thereafter.

10.4.2.4 Configuring Index Settings

You can configure shards and replicas for different indexes as per the required data.

This new feature allows to customize shards and replica counts for each OpenSearch index. As per OpenSearch design, each index in OpenSearch would be mapped to a security group in WebCenter Content. The indexes will be created during:

- server startup
- new Security Group is added to the system
- collection rebuild or reindex
- migration from other search engines to OpenSearch

Shards and replicas will be allotted to the indexes when they are created in the system based on the user configuration. Any updates to these settings will be reflected only after next Full Rebuild or Reindex cycle. You can set limit on the shards and replicas counts.

Shards count: It should be an integer value ranging from 5 to 300. The default value is 5.

Replicas count: It should be either 1 or 2. The default value is 1.

If connection with OpenSearch is not established and no indexes are created yet, an additional optional alert will appear along with the existing OpenSearch alerts.

On clicking the alert message, you will be redirected to OpenSearch Index Settings page where you can customize shards and replicas for each security group (index) existing in the system.

Indexes with these customized settings will be created when successful connection with OpenSearch is established. In case of migration to OpenSearch from other search engines, migration needs to be successful for these indexes to get created with the customized settings.

For already configured OpenSearch instances, the indexes are created with the default index settings.

To configure index settings:

1. Select **Administration**, then **OpenSearch**, and then **OpenSearch Index Settings**.
2. In the Configure Index Settings page, you (admin) can configure indexes with desired shards and replicas count. The updated shard and replica settings will be reflected after:
 - next Full Rebuild or Reindex cycle
 - establishing successful connection in a fresh instance
 - migration if you are switching over from a different search engine

You can not update specific indexes. Once the **Update** button is clicked, all the records will be updated.

Configure Index Settings

OS Index	Shard Count	Replica Count
public	5	1
secure	5	1

3. To view all the active indexes and their shard and replica settings retrieved from the OpenSearch server, select the Active Index Settings tab.

OpenSearch Active Indices

	OS Index	Shard Count	Replica Count
1	os2_public	5	1
2	os2_secure	5	1

Adding New Security Group

If a new security group is added after successful connection to the OpenSearch server from WebCenter Content, its corresponding index will be created in OpenSearch with default shard (5) and replica (1) counts.

If you want to customize its settings, you can do it from the OpenSearch Index Settings page, but they will be reflected only after next rebuild or reindex cycle.

10.4.3 Migrating Existing Search Indexes to OpenSearch

If the WebCenter Content server was previously configured with other search engines (like OTS, FULLTEXT, Elasticsearch) and now the search engine has changed to OpenSearch, content should be migrated.

To migrate, select **Administration**, then **OpenSearch**, and then **OpenSearch Migration**. The figure below is showing the migration from Elasticsearch to OpenSearch. While migrating from

Elasticsearch to OpenSearch, only the **METADATA** option is available in the **Search Engine to Migrate** drop-down menu.

Search Engine to Migrate
The search engine to migrate to opensearch server

METADATA ▾
METADATA

Migration Batch Size
Number of content items to be considered in each batch
To avoid memory issues, it is advisable to choose wisely
when extracted content is part of migration data.

25 ▾

Migrate Metadata Only
If only the metadata should be migrated to opensearch server

False ▾

Migrate

Migration Batch Size determines the number of documents included as a batch together to be pushed to the OpenSearch server. We need to carefully choose the batch size, the batch will also include the text-extracted content of the documents along with its metadata.

Migrate Metadata Only indicates whether we need to push the text-extracted content to the OpenSearch server. In case of the full-text search engines like OpenSearch, this should be always set to **False**. It means the text-extracted content is also pushed to the OpenSearch server.

Upon starting a migration activity, a table of all recent migration jobs and its status details will be listed.

11

Configuring the Search Index

This chapter describes how to configure the Oracle WebCenter Content Server search index. Content Server interfaces with a variety of indexing tools such as commercial search engines and databases.

This chapter includes the following topics:

- [Variances in Indexing Tools and Methods](#)
- [Configuring the Search Index for Databases](#)
- [Working with the Search Index](#)
- [Managing Zone Text Fields](#)
- [Searching Content Using Oracle Query Optimizer](#)
- [Improving Search Performance](#)

11.1 Variances in Indexing Tools and Methods

Content Server interfaces with a variety of indexing tools such as commercial search engines and databases. The indexing tool to use is chosen before installation based on the purpose and environment in which the Content Server instance performs.

Each indexing tool provides full-text indexing and metadata-only indexing. Full-text indexing means that every word in a file is indexed, not only its metadata. Full-text indexing takes longer than metadata indexing; however, it can return a more comprehensive result set. Metadata-only indexing means that every word in the stored content information is indexed. Metadata-only indexing is faster than full-text indexing. By default the Content Server instance is configured to use metadata-only indexing.

11.2 Configuring the Search Index for Databases

If your system is set up to provide indexing and searching capabilities with databases, your system integrator would have added one of the following lines in the *IntradocDir/config/config.cfg* file:

- **Metadata Searching Only:**

```
SearchIndexerEngineName=DATABASE.METADATA
```

DATABASE.METADATA is supported in all databases supported by Oracle Fusion Middleware 12c release.

- **Full-text Searching:**

```
SearchIndexerEngineName=ORACLETEXTSEARCH
```

ORACLETEXTSEARCH is supported in Oracle Database version 11.1.0.7 and newer.

- **Full-text Searching:**

```
SearchIndexerEngineName=DATABASE.FULLTEXT
```


DATABASE.FULLTEXT is supported in SQL Server, and in Oracle Database (all supported versions).

The `dbfulltextsearch` script appropriate for the supported database would then be run.

- By default, full-text indexing is applied to all converted files.
- By default, the Content Server full-text indexes files that are passed through or converted to any of the following formats:

Oracle Supported Formats

- * pdf
- * html
- * htm
- * xls
- * hcsp
- * text
- * txt
- * doc
- * rtf
- * ppt

MS SQL Supported Formats

- * text
- * txt
- * htm
- * html
- * doc
- * msword
- * ms-word
- * ms-powerpoint
- * ppt
- * ms-excel
- * xls

For example, if you want to convert your Microsoft Word (`.doc`) files to text files instead of PDF, you can specify this with the Configuration Manager. That is, when you use the File Formats option to map the `.doc` file extension to a text format, then this defines how the file is converted to a web-viewable format. In this case, the text file is fully indexed before it is passed to the website.

See Managing Native Content Conversion in *Managing Oracle WebCenter Content*.

- You can enable contributors to specify whether to full-text index a file by enabling the format override feature with the System Properties utility. See [Configuring General Options](#).

For example, if you have used the Configuration Manager's File Formats option to map Corel WordPerfect (`.wpd`) files to use a text format and a contributor selects the **use default** option in the **Format** field on the check-in page, the file will be converted to

text and full-text indexed. If the contributor selects **Corel WordPerfect Document**, the file will be passed through in its native format and will not be full-text indexed.

- When you use full-text searching, a search is case sensitive for metadata, and case insensitive for full text. For Content ID, however, lowercase letters are converted to uppercase letters, so Content ID cannot be searched with lowercase letters.

 **Note:**

To avoid errors when indexing, do not add non-existent metadata fields to the Configuration Manager `DrillDownFields` parameter, and do not add memo fields to an SDATA section or to the `DrillDownFields` parameter. See *Metadata Fields in Developing with Oracle WebCenter Content*.

The following sections provide instructions for additional search index configurations:

- [Configuring Metadata Search with All Databases](#)
- [Configuring Full-Text Search with SQL Server](#)
- [Configuring Full-Text Search with OracleTextSearch](#)
- [Optimizing Full Text Search](#)
- [Configuring Database-Supported File Formats](#)
- [Modifying Default Indexing](#)

11.2.1 Configuring Metadata Search with All Databases

To set up and use metadata-only searching and indexing in all databases:

1. Ensure that Content Server is installed and configured to work with the database.
2. Add the following entry to the `DomainHomeName/ucm/cs/config/config.cfg` file and save the file:

```
SearchIndexerEngineName=DATABASE.METADATA
```

3. Restart the Content Server instance.

11.2.2 Configuring Full-Text Search with SQL Server

To set up and use full-text database searching and indexing in SQL Server and in Oracle Database (all supported versions):

1. Ensure that Content Server is installed and configured to work with the database.
2. Add the following entry to the `DomainHomeName/ucm/cs/config/config.cfg` file and save the file:

```
SearchIndexerEngineName=DATABASE.FULLTEXT
```

3. Restart the Content Server instance.
4. Rebuild the search index using the Repository Manager.
 - To access the Repository Manager, choose **Administration**, then **Desktop Client Apps**, then **Repository Manager**.

- Click **Start** in the Collection Rebuild Cycle part of the Indexer tab. The search index is entirely rebuilt, and the old index collection is replaced with a new index collection when the rebuild is successfully completed.

11.2.3 Configuring Full-Text Search with OracleTextSearch

To set up and use full-text searching and indexing with OracleTextSearch, which is supported in Oracle Database version 11.1.0.7 and newer:

1. Ensure that Content Server is installed and configured to work with the database.
2. Add the following entry to the `DomainHomeName/ucm/cs/config/config.cfg` file and save the file:

```
SearchIndexerEngineName=ORACLETEXTSEARCH
```
3. Restart the Content Server instance.
4. Rebuild the search index using the Repository Manager.
 - To access the Repository Manager, choose **Administration**, then **Desktop Client Apps**, then **Repository Manager**.
 - Click **Start** in the Collection Rebuild Cycle part of the Indexer tab. The search index is entirely rebuilt, and the old index collection is replaced with a new index collection when the rebuild is successfully completed.

For more information on OracleTextSearch, see [Managing OracleTextSearch](#).

11.2.4 Optimizing Full Text Search

When using full text search in WebCenter Content, with either of the following two settings, the database uses Oracle Text Index to manage the data for searching.

```
SearchIndexerEngineName=OracleTextSearch  
SearchIndexerEngineName=DATABASE.FULLTEXT
```

When using Oracle Text Index, the index on the database must be maintained in order to keep the disk from becoming fragmented. To avoid fragmentation, an `optimize_index` procedure should be run weekly. This procedure should be scheduled by the database administrator for WebCenter Content.

Determine the Active Index

To determine what is the active index on your WebCenter Content system, log in to the WebCenter Content system and select **Administration**, then **Configuration for instance**. On the Configuration page, for Oracle Text Search you will see something like the following information:

```
Search Engine::ORACLETEXTSEARCH  
Index Engine Name:ORACLETEXTSEARCH  
Active Index:ots2
```

For full text database, you will see something like the following information:

```
Search Engine::DATABASE.FULLTEXT  
Index Engine Name:DATABASE.FULLTEXT  
Active index:IdcColl1
```

The Active Index values tell you the table and index active in the database.

SearchIndexerEngineName	Active Table	Database Table	Database Index
OracleTextSearch	ots1	IDCTEXT1	FT_IDCTEXT1
OracleTextSearch	ots2	IDCTEXT2	FT_IDCTEXT2
DATABASE.FULLTEXT	IdcColl1	IDCCOLL1	FT_IDCCOLL1
DATABASE.FULLTEXT	IdcColl2	IDCCOLL2	FT_IDCCOLL2

Determine if Oracle Text Index Needs Optimization

To determine if an Oracle Text Index is fragmented and possibly in need of optimization, a report called `INDEX_STATS` from the `CTX_REPORT` package can provide a useful view into the WebCenter Content indexes used for Oracle Text Search. For information on the `CTX_REPORT` package, see the *Oracle Text Reference Guide*.

Implement the `optimize_index` Procedure

Request that the database administrator schedule a job on the database to run the `optimize_index` procedure weekly (usually best run on weekends or whenever usage is lower) or as needed based on the database administrator's recommendation. The parameters can be tuned as needed in the call to the procedure, but the default execution uses the parameters in this example:

```
begin
CTX_DDL.OPTIMIZE_INDEX('FT_IDCTEXT1','FULL',parallel_degree=>'1');
end;
```

In some cases, running the `optimize_index` procedure for the first time can cause a large amount of redo logs to be created on the database. If `optimize_index` cannot complete, or the log files on the database are filling up, restart the database in `NOARCHIVELOG` mode and run the `optimize_index` procedure. When the optimization procedure is complete, restart the database in `ARCHIVELOG` mode.

11.2.5 Configuring Database-Supported File Formats

If you define a file format to `PASSTHRU` in the native format, and the format name contains one of the types listed above (such as `application/ms-excel.native`), the passed through native file will be full-text indexed by default.

Alternatively, you can use configuration variables to control whether a document is full-text indexed. To manage the full-text indexing and search of specific document format types, add applicable entries to `IntradocDir/config/config.cfg` and save the file. Full-text indexing configuration variables include:

- [FormatMap](#)
- [ExceptionFormatMap](#)

11.2.5.1 FormatMap

The `FormatMap` configuration variable controls whether files of a specific format should be included in the full-text search index. It is a comma-delimited list of all the formats that will be full-text indexed. The decision is made by taking the MIME type assigned to a file, splitting the MIME type apart at any slash (/) or period (.), and then checking if that value is in the `FormatMap` list.

For example, `application/vnd.msword` will turn into a list of three items:

- application
- vnd
- msword

If FormatMap has `msword` in its list, then the indexer engine will attempt to full-text index the file. the comparison test is not case sensitive.

11.2.5.2 ExceptionFormatMap

The ExceptionFormatMap configuration variable is used to exclude document formats from the FormatMap test. Any format that satisfies the ExceptionFormatMap test will *not* be full-text indexed. This test is done after splitting the MIME format at slashes (/), but not periods(.). For example, if `msword` is included in the exceptions list, then the MIME format `application/msword` is excluded but not `application/vnd.mssword`.

11.2.6 Modifying Default Indexing

Depending on the search engine used, Content Server indexes metadata only or both metadata and the content item's full-text. By default, full-text indexing is performed based on the file format of the content item and several other file-related considerations.

Before a content item is forwarded to the search index, Content Server executes the `std_indexable_format_script` resource. To modify the default indexing criteria, you can create a custom component to modify the `std_indexable_format_script` resource. For example, you can selectively include or exclude full-text indexing for content items based on their MIME types or based on the value of any metadata field, including custom metadata fields.

This section cover the following topics:

- [Indexing Resource Defaults](#)
- [Indexing Resource Include Example](#)

See *Creating Custom Components in Developing with Oracle WebCenter Content*.

11.2.6.1 Indexing Resource Defaults

The default script for the `std_indexable_format_script` resource is as follows:

```
<@dynamichtml std_indexable_format_script@>

<loop DocIndexableFormats$>
<if DocIndexableFormats.fileSize <= MaxIndexableFileSize and
  DocIndexableFormats.fileSize >= MinIndexableFileSize$>
  <indexableFilePath = DocIndexableFormats.filePath$>
  <indexableFileSize = DocIndexableFormats.fileSize$>
  <indexableFileURL = DocIndexableFormats.url$>
  <if isFalse(DocIndexableFormats.allowDirectIndex) and
    isTrue(DocIndexableFormats.allowConversion)$>
    <indexerConversionHandler = DocIndexableFormats.conversionHandler$>
  <endif$>
  <if isTrue(DocIndexableFormats.useMap)$>
    <indexerUseMap = "1"$>
    <indexerMapExtension = DocIndexableFormats.mapExtension$>
  <endif$>
  <$break$>
<endif$>
```

```
<endloop$>
<end@>
```

The script compares the content item to the list of indexable formats. If it finds a match, it determines whether the file is within established size boundaries and sets a number of index-related values for the content item.

11.2.6.2 Indexing Resource Include Example

Scenario 1:

When a user checks in specific document types, they can choose to either index the content item using metadata only or using both metadata and full text.

Solution 1:

To allow users to specify whether a document is indexed using metadata only or using both metadata and full text, you can create a custom metadata field (for example, `xIsFullTextSearchable`) with a list that has two values: `Yes` and `No` with `Yes` as the default. When a user checks in a document that contains accounting data and, therefore, should not be indexed using full text, they set the value of `xIsFullTextSearchable` to `No`.

To implement this solution, create a custom component that encloses the default resource code in a new IF statement that checks the value of the custom field:

```
<@dynamichtml std_indexable_format_script@>
<$if strEquals(xIsFullTextSearchable, "Yes") $>
<$loop DocIndexableFormats$>
  .
  .
  .
<endloop$>
<$endif$>
<end@>
```

Scenario 2:

Do not perform a full-text index for web-viewable renditions of content items that are themselves indexed.

Solution 2:

To implement this solution, create a custom component that encloses the default resource code in a new IF statement that checks the value of `FormatType` to determine if the item is a native file (`FormatType="vault"`) or a web-viewable rendition (`FormatType="webviewable"`):

```
<@dynamichtml std_indexable_format_script@>
<$if strEquals(FormatType, "vault") $>
<$loop DocIndexableFormats$>
  .
  .
  .
<endloop$>
```

<\$endif\$>
<@end@>

11.3 Working with the Search Index

This section covers these topics:

- [About the Search Index](#)
- [Updating the Search Index](#)
- [Rebuilding the Collection](#)
- [Configuring the Search Index Update or Collection Rebuild](#)
- [Full-Text Indexing](#)
- [Disabling Full-Text Indexing](#)
- [Indexing Native Files by Default](#)
- [Indexing Email and Attachments](#)

11.3.1 About the Search Index

The Repository Manager utility provides an Indexer tab which administrators can use to perform actions on the search index.

To access the Repository Manager, choose **Administration**, then **Desktop Client Apps**, then **Repository Manager**. You can also access the Repository Manager as a standalone application. For details, see [Running Administration Applications in Standalone Mode](#).

The Indexer tab on the Repository Manager window enables administrators to perform these actions:

- **Update the Search Index:** Incrementally updates the index database. This is usually not necessary because the index is automatically updated approximately every five minutes by the server.
- **Rebuild the Collection:** The search index is entirely rebuilt, and the old index collection is replaced with a new index collection.
- **Suspend an Update or a Rebuild:** Stops the update or rebuild temporarily. You can restart the process by clicking the appropriate Start button.
- **Cancel Update Search:** Index update process terminates, and only files processed to that point are accessible to the search engine.
- **Cancel Rebuild Collection:** Index rebuild process terminates, and the previous index database continues to be used by the search engine.

See Managing Content in *Managing Oracle WebCenter Content*.

11.3.2 Updating the Search Index

1. In the Repository Manager window, click the **Indexer** tab.
2. Click **Start** in the Automatic Update Cycle area.

11.3.3 Rebuilding the Collection

1. In the Repository Manager window, click the Indexer tab.

2. Click **Start** in the Collection Rebuild Cycle area.

 **Note:**

OracleTextSearch provides a Fast Rebuild function, which you can use through the Repository Manager Indexer function if your site uses the OracleTextSearch feature. For details, see [Fast Rebuild](#).

11.3.4 Configuring the Search Index Update or Collection Rebuild

To set the parameters for a search index update or collection rebuild:

1. In the Repository Manager window, click the **Indexer** tab.
2. Click **Configure in either the Automatic Update Cycle portion of the screen or the Collection Rebuild Cycle portion**. Either the Automatic Update Cycle window or the Collection Rebuild Cycle window opens.
3. Specify the number of content items (files) per indexer batch. This is the maximum number of files that the search index will process simultaneously.

The default is 25. For example, 25 files are indexed together, then the next 25 files are indexed. However, if one item fails, then the batch is processed again.
4. Specify the content items (files) per checkpoint. This is the number of files that will go through all relevant indexing states at a time. You can have multiple batches of files indexed per checkpoint.
5. Specify the indexer debug level. This is the amount of information pertaining to each file to display in the server window. The more debug information is listed in the server window, the slower the indexing progresses. The levels include:
 - **none**: No information for each file access is displayed, and no log will be generated.
 - **verbose**: Displays information for each file accessed. Indicates indexed, ignored, or failed, and generates a full report.
 - **debug**: Displays the medium level of information, which is specifically functional.
 - **trace**: Displays the lowest level of information for each activity performed.
 - **all**: Displays the highest level of debug information.
6. If you selected **Automatic Update Cycle**, the **Indexer Auto Updates** check box is available. Select this if you want the index database to be updated automatically.
7. Click **OK**.

11.3.5 Full-Text Indexing

If you have configured the Content Server instance to use DATABASE.FULLTEXT or ORACLETEXTSEARCH as your indexing engine, Content Server uses the Outside In Content Access module to export content to a text file upon check-in. The text file is then passed to the full-text indexer for full-text indexing.

 **Note:**

When the Outside In Content Access module converts a PostScript file, the conversion process produces text that contains extra characters. Unfortunately, this creates a file that is full-text indexed but cannot be full-text searched.

If you use DATABASE.FULLTEXT, a full-text search can be problematic on large documents. By default, the maximum document size that is indexed is 10MB. This can be changed by setting the MaxIndexableFileSize configuration variable in the Content Server repository. The default is MaxIndexableFileSize=10485760. If larger documents require full-text indexing, the value of MaxIndexableFileSize should be increased.

For information on optimizing your search collection when you are using full-text searching with the Oracle database, which would apply to both OracleTextSearch and DATABASE.FULLTEXT search methods, see [Optimizing Full Text Search](#) and also [Full-text indexing? You must read this.](#)

11.3.6 Disabling Full-Text Indexing

You might want to disable full-text indexing if, for example, you want to conserve file space or if you do not require full-text searching for specific content types. Even if you disable full-text indexing, metadata is still indexed.

To disable full-text indexing on specific files:

1. Define a format named **application/noindex** on the Configuration Manager page.
2. Enable the **Allow Override Format on Check In** setting. For more information, see [Configuring General Options](#).
3. When a user checks in a file that they do not want to be indexed, they should select the **application/noindex** format. This applies to standard files, batch loads, and archived revisions.

11.3.7 Indexing Native Files by Default

The search index uses weblayout files for indexing by default. In certain situations it may be useful to index native files by default instead of weblayout files. For example, if a converted PDF file cannot be extracted and indexed because of processing issues, the native Word document or an alternate type of document could be extracted and indexed. Another example is if the primary file cannot be indexed because it is an .exe file, but it has an alternate .txt file, then the alternate file could be indexed.

To have the search index use native files for indexing by default, set the following parameter in the Content Server instance:

```
UseNativeFormatInIndex=true
```

11.3.8 Indexing Email and Attachments

Content Server supports indexing of email and email attachments (such as original files and zip files). Email messages are indexed by default, and if a message contains an attachment it is extracted and indexed as full text. There is no change on what gets returned on search result: if a search finds information in a document, the document metadata is returned. All email attachments supported by Outside In Technology are supported by the search index.

11.4 Managing Zone Text Fields

The functionality described in this section is only available if you have installed and enabled the Database Search Contains Operator feature.



Note:

This feature is not required in the OracleTextSearch component.

This section covers these topics:

- [About Zone Text Fields](#)
- [Enabling and Disabling Zone Text Fields](#)
- [Changing the Minimum Length of Text Fields](#)
- [Disabling Database Search Contains Operator](#)

11.4.1 About Zone Text Fields

The Database Search Contains Operator feature enables you to use the Contains search operator to search text fields when performing Database and Database Full Text searches on SQL Server and Oracle. You must first enable the text fields that can be queried using the Contains search operator. These text fields are called **zone text fields**.

When a text field is added as a zone text field, the text within the field is parsed and a full-text index for the field is created in the database. The database performs all the work of creating the index, and the index is dropped from the database if the text field is disabled as a zone text field. Therefore, there is no need to rebuild the collection after enabling or disabling text fields as a zone text fields.



Important:

Changing a text field to a zone text field can be a very time-consuming operation. The amount of time it takes to parse the text and create the full-text index depends on the number of content items in the Content Server repository and the amount of text stored in the text field. However, after the text field has been indexed, you should not experience significant performance issues when updating and adding content items.

When a text field has been enabled as a zone text field, the CONTAINS search operator is available for the text field on the Advanced Search page. It is represented as the *Has Word* option in the list next to the text field.

Figure 11-1 Has Word Option

Title	Has Word	<input type="text"/>
Type	Substring	<input type="text"/> <input type="text"/>
Security Group	Substring	<input type="text"/> <input type="text"/>
Author	Substring	<input type="text"/>
Release Date	From	<input type="text"/> To <input type="text"/>
Expiration Date	From	<input type="text"/> To <input type="text"/>
Comments	Has Word	<input type="text"/>

11.4.2 Enabling and Disabling Zone Text Fields

Note:

The functionality described here is only available if you have installed and enabled the Database Search Contains Operator feature. The *zone text fields* feature is not required in the OracleTextSearch component.

When enabling and disabling zone text fields, consider the following:

- Custom text fields (the **Comments** field and any customer created text fields) are shared between the Database and Database search engines, and therefore changing the status of these text fields for one search engine also applies the changes to the other search engine.
- Standard text fields (**Author**, **Content ID**, **Content Type**, **Title**, and so on) can be enabled or disabled independently for each search engine.
- The database performs all the work of creating the indexes, and the indexes are dropped from the database if the text fields are disabled as zone text fields. Therefore, there is no need to rebuild the collection after enabling or disabling text fields as zone text fields.
- You must disable a zone text field before the field can be deleted from the Content Server instance using Configuration Manager. If you delete an enabled zone text field using Configuration Manager and then click **Update Database Design**, you will receive an error.

Disabling the zone text field drops the index for the field from the database, allowing the field to be deleted from the database. As an alternative to disabling the zone text field, you could log in to the database and issue a command to drop the index for the field, and then delete the field.

- You might want to disable all zone text fields before uninstalling the feature. Otherwise, you are not able to delete the zone text fields from the Content Server instance unless you reinstall the feature to disable the zone text fields or drop the indexes for the zone text fields from the database manually.

To enable and disable zone text fields:

1. Choose **Administration**, then **Zone Fields Configuration**.

Figure 11-2 Zone Fields Configuration

The screenshot shows the 'Zone Fields Configuration' window. At the top, there is a 'Search Engine:' dropdown menu set to 'Database'. Below this are two main sections: 'Zone Text Fields' and 'Text Fields'. The 'Zone Text Fields' list contains 'Comments' and 'Title'. The 'Text Fields' list contains 'Account', 'Author', 'Content ID', 'Content Type', 'Format', 'Original Name', and 'Security Group'. Between these two lists are two arrow buttons: a right-pointing arrow and a left-pointing arrow. At the bottom of the window are two buttons: 'Update' and 'Reset'.

 **Note:**

Custom text fields (the **Comments** text field and any customer-created text fields) are shared between the Database and DatabaseFullText search engines. Therefore, changing the status of these text fields for one search engine also applies the changes to the other search engine. Standard text fields (**Author**, **Content ID**, **Content Type**, **Title**, and so on) can be enabled or disabled independently for each search engine.

2. In the Zone Fields Configuration window, select the search engine to be used to search the zone text fields (either `Database` or `DatabaseFullText`).
3. To enable text fields as zone text fields:
 - a. Select the text fields (for the selected search engine) in the Text Fields list. You can press the **Ctrl** and **Shift** keys on your keyboard to select multiple fields.

By default, text fields with a field length of 20 characters or less are not included in the Text Fields list. You can change this setting by modifying the `MinFullTextFieldLength` configuration variable. For details, see [Changing the Minimum Length of Text Fields](#).
 - b. Click the left arrow button to move the text fields to the Zone Text Fields list.
 - c. Click **Update**. This action enables the text fields in the Zone Text Fields list as zone text fields, and disables text fields in the Text Field list. This action also parses the text within all zone text fields and creates a full-text index that can be queried using the `Contains` search operator.

 **Important:**

Changing a text field to a zone text field can be a very time-consuming operation. The amount of time it takes to parse the text and create the full-text index depends on the number of content items in the Content Server repository and the amount of text stored in the text field. However, when the text field has been indexed, you should not experience significant performance issues when updating and adding content items.

4. To disable zone text fields:
 - a. Select the zone text fields in the Zone Text Fields list. You can press the **Ctrl** and **Shift** keys on your keyboard to select multiple fields.
 - b. Click the right arrow button to move the text fields to the Text Fields list.
 - c. Click **Update**.
5. If you start making changes to the lists and you then want to revert to the last saved lists, click **Reset**.

11.4.3 Changing the Minimum Length of Text Fields

 **Note:**

The functionality described here is only available if you have installed and enabled the Database Search Contains Operator feature. The *zone text fields* feature is not required in the OracleTextSearch component.

By default, text fields with a field length of 20 characters or less are not included in the Text Fields list. You can change this setting by modifying the `MinFullTextFieldLength` configuration variable. To change this variable:

1. Using a text editor, open the `config.cfg` file located in the `IntradocDir/config/` directory.
2. Add the `MinFullTextFieldLength` configuration variable, and set its value (the default value is 21). For example:

```
MinFullTextFieldLength=16
```
3. Save your changes to the `config.cfg` file.
4. Restart the Content Server instance.

11.4.4 Disabling Database Search Contains Operator

 **Note:**

The functionality described here is only available if you have installed and enabled the Database Search Contains Operator feature. The *zone text fields* feature is not required in the OracleTextSearch component.

Before disabling the Database Search Contains Operator feature, you might want to disable all zone text fields. The database contains an index for each enabled zone text field (the indexes are dropped when the zone text fields are disabled). If the database contains an index for a field, it will not let you delete the field from your Content Server instance using Configuration Manager. For more information, see [Enabling and Disabling Zone Text Fields](#).

If you disable the feature and later want to delete a field that is enabled as a zone text field, you can use one of the following options:

- Reinstall the feature, disable the zone text field, use Configuration Manager to delete the field, and uninstall the feature.
- Log in to the database and issue a command to drop the index for the field, then use Configuration Manager to delete the field.

11.5 Searching Content Using Oracle Query Optimizer

The OracleQueryOptimizer component is installed (enabled) by default with the Content Server instance. The functionality only works with the Oracle database.

This section covers these topics:

- [About Oracle Query Optimizer](#)
- [Query Optimization Process](#)
- [How Reformatted Queries Optimize Searches](#)
- [Types of Recognized Hints](#)
- [Query Hints Syntax](#)
- [Additional Supported Sort Constructs](#)
- [Hint Rules Table](#)
- [Edit Hint Rules Form](#)
- [The Hint Cache](#)
- [Using Hint Rules](#)
- [Using the Query Converter](#)
- [Updating the Hint Cache](#)

11.5.1 About Oracle Query Optimizer

Oracle database does not automatically select the best execution plan for certain types of user queries. To counter this, the Oracle Query Optimizer adds hints to queries that force Oracle database to perform searches more efficiently.

The hints are based on an intrinsic knowledge of Content Server table data distribution and its index selectivity. To take advantage of this knowledge, Oracle Query Optimizer uses a pre-defined Hint Rules Table to analyze the database query and then add appropriate hints to the query. In turn, the added hints improve Oracle's search performance.

Oracle Query Optimizer takes advantage of Content Server data distribution in database tables and its index selection preferences. Based on these characteristics, the Hint Rules Table included with Oracle Query Optimizer contains pre-defined rules. The feature uses these rules to analyze a database query and to add one or more appropriate hints to the query to optimize the search performance.

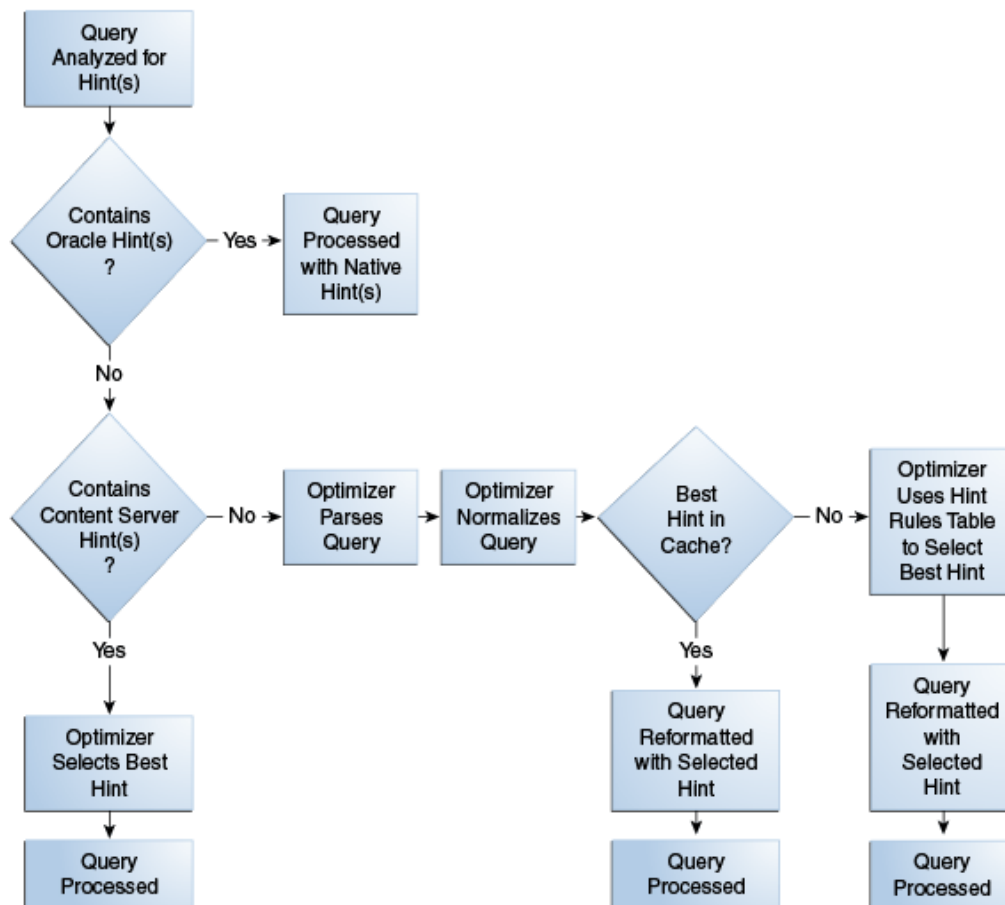
In very large collections containing millions of content items, the Content Server software generally has a difficult time selecting an appropriate optimization strategy to resolve even simple queries. To counteract this problem, Oracle Query Optimizer examines the submitted query and, based on its analysis, reformats the query by adding appropriate hints to optimize the search process. To add hints, the feature uses Content Server hints, the Hint Rules TableHint Rules Table, and the Hint Cache.

11.5.2 Query Optimization Process

The stages of the optimization process are completed in the following sequence:

1. The submitted query is analyzed to verify if it contains one or more hints and, if so, determine the type of hint. For more information, see [Stage 1: Query Analysis](#).
2. If the query's WHERE clause does not contain a hint, the optimization feature must parse out the WHERE clause. For more information, see [Stage 2: Parsing](#).
3. After parsing, each condition in the query's WHERE clause is evaluated against the Hint Rules Table in an attempt to qualify the condition and normalize the query. For more information, see [Stage 3: Normalization](#).
4. After the WHERE clause conditions are qualified and the query is normalized, a hint is selected or retrieved from the hint cache. For more information, see [Stage 4: Select Hint](#).
5. The query is reformatted using the selected hint. For more information, see [Stage 5: Reformat Query](#).

Figure 11-3 Optimization Process Sequence



11.5.2.1 Stage 1: Query Analysis

In this stage, a query is checked for both Oracle (native) and Content Server hints. This is determined based on the hint syntax: [Query Hints Syntax](#). A query that contains Oracle hints is passed through. A query that contains Content Server hints bypasses [Stage 2: Parsing](#) and [Stage 3: Normalization](#). If a query contains multiple Content Server hints, the best hint is chosen. Queries that do not contain any hints must be parsed and normalized.

11.5.2.2 Stage 2: Parsing

In this stage, a query that does not contain any hints is sent through the query parser and the WHERE clause is parsed out. A WHERE clause consists of one or more conditions joined with either AND or OR conjunctions. For each condition, the field name, operator, and field value are extracted. The AND/OR conjunctions of the clause are preserved; the parentheses are dropped. Conditions must use the following format:

fieldname operator value

For example, a properly formatted condition would be `dID = 3`. An incorrect condition would be `3 = dID`.

11.5.2.3 Stage 3: Normalization

In this stage, normalization simplifies conditions, finalizes query operators, and provides a stable view of the WHERE clause for additional steps. The result of the normalization process produces a base for generating the cache key and the list of fields to use to search for hints.

**Note:**

To establish which database tables and columns have indexes, the Hint Rules Table is defined on Content Server resources and on the running system.

- **Qualifying WHERE Clause Conditions:**

Each condition in the WHERE clause is checked against the Hint Rules Table. If a condition's field name is included in the Hint Rules Table, then it is qualified and the condition is considered to be normalized. The condition contains its table name and alias. Then the normalized conditions are sorted to ensure that the same set of conditions is always listed consistently.

- **Discarding WHERE Clause Conditions During Normalization:**

During normalization, the following conditions are not considered relevant and are eliminated from further processing:

- Join conditions.
- Conditions that contain subqueries.
- Conditions whose field names do not have entries in the Hint Rules Table and cannot be qualified.
- OR conditions that contain more than one field. For example:

```
(dSecurityGroup = 'Secure' or dDocAccount LIKE 'prj%')
```
- Conditions that contain the LIKE operator whose value begins with a wildcard.

- **Reformatting WHERE Clause Conditions:**

In the normalization step, the query conditions are rewritten to consolidate complex query conditions. OR conditions are reevaluated as follows:

- If all the fields are the same and all the operators are equal (or all the operators are LIKE and no values begin with a wildcard), the conditions are combined and changed to an IN query.
- If the fields are the same but have different operators, the conditions are combined and the generic operator is assigned.
- If the fields are different, the conditions are dropped.

For example, during normalization, the following condition is reformatted:

```
(dReleaseState = 'Y' OR dReleaseState = 'O')
```

It is reformatted as follows:

```
dReleaseState IN ('Y', 'O')
```

- **Finding Potential Range Queries:**

The parsed query is analyzed to find potential range queries that are then consolidated during the normalization process. For example, the conditions `dInDate > date1` and `dInDate < date2` are changed to one condition with the operator 'range'.

11.5.2.4 Stage 4: Select Hint

In this stage, the normalized conditions are checked against the hint cache. If one or more conditions have applicable hints in the cache, they are included. If applicable hints are not found in the cache, the conditions are analyzed and the preference orders are compared to determine the best possible hint.

11.5.2.5 Stage 5: Reformat Query

In this stage, the query is reformatted by adding in the selected hint. For more information about how reformatting queries with hints helps to optimize searches and some examples of reformatted queries, see [How Reformatted Queries Optimize Searches](#).

11.5.3 How Reformatted Queries Optimize Searches

The majority of queries in a Content Server instance involve a small, targeted set of content items or return a hundred rows, at most. Content Server software can easily scale to millions of content items. However, testing on an Oracle database with a collection containing 10 million content items indicates that the execution plan that Oracle selects is not the most efficient. Oracle generally does not choose the best optimization strategies to resolve many queries, even some that are trivial. The following examples explain this issue:

- [Example 1: Reformatting a Query by Adding a Single Hint](#)
- [Example 2: Reformatting a Query by Adding Multiple Hints](#)

11.5.3.1 Example 1: Reformatting a Query by Adding a Single Hint

In the environment described above, Oracle does not resolve the following query as efficiently as possible:

```
SELECT *  
FROM Revisions, Documents, DocMeta
```

```
WHERE Revisions.dID = Documents.dID
      AND Revisions.dID = DocMeta.dID
      AND Revisions.dRevClassID = 333
Order By Revisions.dID
```

Because a fairly selective index is available (dRevClassID_2 for Revisions.dRevClassID), this query should access dRevClassID_2 and perform a sort on the rows that match the dRevClassID. However, in this query example, Oracle chooses to use the Revisions.dID index.

This choice is actually worse than performing a full table scan on the Revisions table because it does a full index scan and accesses the table to obtain the dRevClassID for each row. Obviously, resolving the query using this execution plan does not work well when the Content Server repository has over 10 million content items. In this case, it requires approximately 500 seconds to return the results.

However, the performance improves dramatically when the query is modified by adding a hint as follows:

```
SELECT /*+ INDEX(Revisions dRevClassID_2)*/ *
FROM Revisions, Documents, DocMeta
WHERE Revisions.dID = Documents.dID
      AND Revisions.dID = DocMeta.dID
      AND Revisions.dRevClassID = 333
Order By Revisions.dID
```

The query is modified by adding the following hint to the SELECT clause:

```
/*+ INDEX(Revisions dRevClassID_2)*/
```

This forces Oracle database to choose the dRevClassID_2 index instead of the index for Revisions.dID. Because no more than a few content items share dRevClassID in this example, the modified query returns the results instantly.

11.5.3.2 Example 2: Reformatting a Query by Adding Multiple Hints

In a typical Content Server instance, most documents have a 'Y' (released) status for the dReleaseState with a dInDate earlier than the current date. However, only a few documents have a 'N' (new, not yet indexed) status for the dReleaseState. The following query is searching for content items that have not yet been released:

```
SELECT dID
FROM Revisions
WHERE Revisions.dReleaseState = N'N' AND Revisions.dStatus in
      (N'DONE', N'RELEASED', N'DELETED')
      AND Revisions.dInDate<={ts '2005-02-23 17:46:38.321'}
```

The optimized result for the query uses the index for dReleaseState:

```
SELECT/*+ LEADING(Revisions) INDEX (Revisions dReleaseState)*/
      dID
FROM Revisions
WHERE Revisions.dReleaseState = N'N' AND Revisions.dStatus in
      (N'DONE', N'RELEASED', N'DELETED')
      AND Revisions.dInDate<={ts '2005-02-23 17:46:38.321'}
```

11.5.4 Types of Recognized Hints

Content Server queries can be static queries defined in various resources, data sources with additional dynamic WHERE clauses, and dynamic queries that are ad-hoc or defined in the application such as Archiver. Static queries can be updated with Oracle database hints.

However, it is nearly impossible to predefine hints for ad-hoc queries and dynamic WHERE clauses.

Content Server hints use a database-neutral hint syntax that supports multiple hints in the same query. A Content Server hint can be used in any query, data source, and WHERE clause. However, it cannot be combined with an Oracle database hint. If a query contains both types of hints, Oracle Query Optimizer will retain the Oracle database hint and ignore the Content Server hint.

11.5.5 Query Hints Syntax

During the optimization processing stages, Oracle Query Optimizer recognizes the distinct syntaxes of both types of hints and correspondingly processes the submitted query. For more information on the optimization process, see [Query Optimization Process](#).

11.5.5.1 Oracle Hint Syntax

An Oracle hint uses the following format:

```
/*+ hint */
```

For example:

```
/*+ Index(Revisions dID)*/
```

11.5.5.2 Content Server Hint Syntax

The Content Server hint syntax is database neutral and can support multiple Content Server hints in the same query. During the optimization process, Content Server hints are evaluated and the best hints are formatted and added back to the query.

During the optimization process, a query that includes one or more Content Server hints is not parsed. Only Content Server hints are considered when choosing indexes.

- **Content Server Hint Syntax:**

When a query undergoes the optimization process, Content Server hints are added to the reformatted query using the following syntax:

```
/*$tableName[ aliasName]:columnName[:operator [:<value>]][, ...]*/
```

Where:

- Values enclosed in angle brackets (<value>) are required.
- Values enclosed in brackets ([value]) are optional.
- Ellipses (...) indicates a repetition of the previous expression(s).

- **Query Before Optimization Process:**

```
SELECT *
FROM Revisions, DocTypes, RoleDefinition
WHERE /*$Revisions:dStatus*/(Revisions.dStatus<>'DELETED' AND
Revisions.dStatus<>'EXPIRED' AND Revisions.dStatus<>'RELEASED') AND
Revisions.dDocType = DocTypes.dDocType AND
/*$Revisions:dReleaseState*/Revisions.dReleaseState<>'E' AND
(Revisions.dSecurityGroup = RoleDefinition.dGroupName AND
RoleDefinition.dRoleName = ? AND RoleDefinition.dPrivilege > 0
```

- **Reformatted Query with Content Server Hints Added:**

After the query has undergone the optimization process, both indexes are used and are added to the native indexes.

```
SELECT/*+ LEADING(revisions) INDEX (revisions dStatus dReleaseState)*/ *
FROM Revisions, DocTypes, RoleDefinition
WHERE (Revisions.dStatus<>'DELETED' AND Revisions.dStatus<>'EXPIRED' AND
Revisions.dStatus<>'RELEASED') AND Revisions.dDocType = DocTypes.dDocType AND
Revisions.dReleaseState<>'E' AND (Revisions.dSecurityGroup =
RoleDefinition.dGroupName AND RoleDefinition.dRoleName = ? AND
RoleDefinition.dPrivilege > 0)
```

11.5.6 Additional Supported Sort Constructs

Using Oracle sort constructs in search query clauses allows users greater flexibility when performing a query. Sort constructs specify the row data in two or more tables to be extracted, sorted, and combined. Essentially, the sort constructs serve the purpose of limiting the number of rows that are returned. Oracle Query Optimizer recognizes the following sort constructs:

- **Group by:** Sorts a set of records and specifies how to group the results.
- **Order by:** Sorts a set of records and specifies whether the results are to be returned in ascending or descending order.
- **Inner join:** Sorts a set of records by looking for and returning those that match.
- **Outer join:** Sorts a set of records by looking for and returning those that do not match.

11.5.7 Hint Rules Table

The Hint Rules Table contains the rules that the optimization feature uses to determine the proper hints to add to dynamic queries or data sources during the optimization process. Using the Edit Hint Rules form, a hint rule can be defined for a particular field and operator. A hint rule can also be defined based on values or date/number ranges. The hint rule table is extensible by other components, and can be updated while the Content Server instance is running.

Figure 11-4 Hint Rules Table

Key	Table	Column	Operator	Index	Order	Values	AllowMultiple Disabled
PK_Revisions	Revisions	dID	equal	PK_Revisions	5		false
dDocName	Revisions	dDocName	equal	likedDocName_Revisions	5		false
RevdRevClassID	Revisions	dRevClassID	equal	dRevClassID_2_Revisions	5		false

Several default hint rules included with Oracle Query Optimizer are described in the following text. For more detailed descriptions of the table columns, see [Hint Rules Table](#). The content of the Hint Rules Table is available on the Hint Rules Configuration page that is accessed through the Administration tray.

The Hint Rules Table is scheduled to reload every night, and when a rule is added or modified. The hint value is recalculated at each reload.

! Important:

Although the Hint Rules Table includes a column allowing multiple indexes to be used with each other, in Oracle only the bitmap index can be combined. This is because the Hint Rules Table was designed for core Content Server functionality.

Therefore, it might not be sufficient for a system with components that create additional tables or add additional metadata fields, or both. However, the Hint Rules Table can be extended or overwritten by other components to provide knowledge of additional tables, indexes and fields.

- **Explanation of First Hint Rule:**

For this rule, if the WHERE clause contains the following condition the PK_Revisions index is used and added as a hint to the optimized query:

```
Revisions.dID = some_value
```

- **Explanation of Second Hint Rule:**

For this rule, if the WHERE clause contains either of the following conditions the dDocName index is used and added as a hint to the optimized query:

```
Revisions.dDocName = some_value  
Revisions.dDocName LIKE 'some_value'
```

- **Explanation of Third Hint Rule:**

For this rule, if the WHERE clause contains the following condition the condition does not meet the requirements and cannot be qualified:

```
dStatus = 'DONE'
```

However, if the WHERE clause contains the following condition the dStatus index is used and added as a hint to the optimized query.:

```
dStatus = 'RELEASED'
```

The following sections describe the following columns in the Hint Rules Table:

- [Key](#)
- [Table](#)
- [Column](#)
- [Operators](#)
- [Index](#)
- [Order](#)
- [Values](#)
- [AllowMultiple](#)
- [Disabled](#)

11.5.7.1 Key

This column contains the unique name to identify the rule. A component can use the unique key to overwrite a particular rule. This key is usually identical to its index name because the index name is unique in the same database schema.

By default, Oracle uses a B+ Tree (binary tree) as the indexing structure to provide efficient access to logical records. B+ Tree indexes are most useful for queries involving a small number of result rows or when the user needs to execute queries using varying criteria (such as equality and range conditions). Because B+ Tree indexes store the indexed data values, these indexes are useful as sources of data if the requested value is the stored value.

However, bitmapped indexes offer substantial performance improvements with minimal storage cost compared to the default B+ Tree indexes. Bitmapped indexes are particularly effective for searching columns with poor selectivity due to having very few distinct values. Also, a bitmap is built for each value including the NULL value (which means the NULL is indexed). Overall, using bitmapped indexes is very efficient because the index lookup process is a bit-level operation and allows access to multiple indexes.

 **Note:**

Because hint rules can be overwritten, Oracle Query Optimizer does not allow you to add a hint rule using an existing key. Therefore, it is important when you are creating your bitmapped indexes for columns that you assign unique keys.

Oracle recommends that you use bitmapped indexes for the table columns listed below, and set the index name to the corresponding column name.

- Revisions table:
 - dIndexerState
 - dReleaseState
 - dProcessingState
 - dIsCheckedOut
 - dSecurityGroup
 - dStatus
- WorkflowDocuments table:
 - dWfDocState

11.5.7.2 Table

This column identifies the specific database table.

11.5.7.3 Column

This column identifies the specific column within the database table listed in the Table column.

11.5.7.4 Operators

This column is a comma-delimited list of allowable operators. For more information about the valid operator options, see the **Operators** field and menu on the Hint Rules Configuration page. The hint rule's operator is important in the decision of whether a hint rule will be applied to a condition.

For example, if the WHERE clause contains the following condition using the PK_Revisions index would be a very valuable hint to include in an optimized query:

```
Revisions.dID = 3
```

However, if the WHERE clause contains the following condition then using the PK_Revisions index would not be useful:

```
Revisions.dID > 3
```

11.5.7.5 Index

This column identifies the specific index to use in the optimized query if the condition meets the hint rule requirements.

11.5.7.6 Order

This column contains the preferred order to use when the rule is included in the Hint Rules Table. The highest ordered rules in a query are given precedence when deciding which hint to use.

The order values include:

- **5:** This value indicates that the specified index is unique or does not match more than 50 rows for any value. For example, specifying dID with the Revisions, Documents, or DocMeta tables.
- **4:** This value indicates that the specified index should be somewhat less selective. The specified value should typically match a few rows and, at the very most, several hundred rows. For example, specifying dDocTitle with the Revisions table.
- **3:** This value indicates that the specified index matches less than a thousand rows. For example, specifying dInDate or dOutDate.
- **2:** This value indicates that the specified index matches less than ten thousand rows.
- **1:** This value indicates that the specified index matches more than ten thousand rows.

11.5.7.7 Values

This column is Idoc scriptable. This column can only be defined when the Operators column value is one of the following:

- **in** or **notin**: When you use either of these operators, the value should be a comma-delimited list enclosed in parenthesis.
- **range**: When you use this operator, the value must use one of the following formats:

- **Format 1:**

```
([<lowValue>],range[,<highDateValue>])
```

Examples of acceptable values include:

```
('Y', 'O')
(,7d)
({ts '2004-12-11 12:03:23.000'}, 2d, <$dateCurrent()$>)
```

- **Format 2:**

```
#[d|h]
```

For example, a range of five days is 5d and seven hours is 7h.

 **Note:**

The operators **in** or **notin** can substitute for the operators **equal** and **notEqual**, respectively, along with their matching values. For more information about operator options, see the **Operators** field and menu on the Edit Hints Rule form.

The following use cases demonstrate how this column provides additional flexibility to the hint rules:

- **Use Case 1: State or Status Table Columns**

Table columns that indicate a state or status such as `dReleaseState` or `dStatus` are biased regarding the finished states. For example, `dReleaseState` is predisposed for 'Y' (released) or 'O' (old version). Likewise, `dStatus` is predisposed for `RELEASED`. Therefore, in `WHERE` clauses, conditions such as `dReleaseState = Y` or `dStatus = RELEASED` match the majority of rows in the Revisions table. Thus, indexes for these two columns are almost useless. Conversely, the condition `dReleaseState = N` (new, not yet indexed) matches only a few rows. Consequently, indexes on this column would be very helpful.

- **Use Case 2: Date or Number Table Columns**

Table columns that indicate a date or number exhibit similar behavior to state or status. For example, the condition `dInDate < <$dateCurrent()$>` matches most of the table rows and makes indexes on this field irrelevant. However, the combined conditions `dInDate < <$dateCurrent()$> AND dInDate > <$dateCurrent(-1)$>` usually match only a small set of rows and would benefit from using the corresponding index as a hint.

11.5.7.8 AllowMultiple

This column indicates whether the defined index is used with other indexes. In Oracle, only the bitmap index can be combined.

11.5.7.9 Disabled

This column indicates whether a hint rule has been disabled. Any rule in the table can be enabled/disabled. If you disable a hint rule, a value of 'Y' is displayed. Existing rules can be disabled to match the current Content Server state.

For example, if a Content Server instance contains only a few distinct content `revClasses`, each `revClass` may have thousands of revisions. Therefore, the `dRevClass_2` index is not very effective. In this case, this corresponding hint rule should be disabled and you should add one or more new rules with different preference orders.

 **Note:**

Although any rule in the table can be enabled or disabled, only the rules that are added using the Edit Hints Rule form can be removed. The default hint rules that are included with the Oracle Query Optimization feature can only be disabled; they cannot be removed.

11.5.8 Edit Hint Rules Form

The Edit Hint Rules Form provides a way to add, remove, enable, or disable rules using the Hint Rules Configuration page. You can add a new rule to reflect new tables and indexes. Existing rules can be removed or disabled to match the current state of the Content Server instance. If you select a hint rule from the hint rule table, the Edit Hint Rules Form fields are automatically populated with the applicable values.

The Edit Hint Rules Form is displayed next to the hint rules configuration table on the Hint Rules Configuration page.

The hint rules configuration table is scheduled to reload every night and whenever a new rule is added or an existing rule is modified. The hint value is recalculated at each reload.

Although any rule in the table can be enabled or disabled, only the rules that are added through the Edit Hint Rules Form can be removed. The default hint rules that are included with the OracleQueryOptimizer component can only be disabled; they cannot be removed.

11.5.9 The Hint Cache

Oracle Query Optimizer also contains a hint cache to store dynamically generated hints. For example, a hint derived from a parsed query or data source is cached to maintain persistence. In this way, the hint cache provides stability for queries and data sources.

The hint cache is used during the optimization process to select hints for queries that do not contain Oracle or Content Server hints. The hint cache provides a mechanism to fine tune query hints. In addition, administrator can check/edit cache and change hint for queries at run time.

The hint cache is stored to disk every two hours and is reloaded when the Content Server instance is started.

The characteristics of the hint cache include:

- [Reusing Hint Cache Entries](#)
- [Hint Cache Management](#)
- [Default Capacity Algorithm](#)
- [Origin of Hint Cache Keys](#)
- [Hint Cache Persistence](#)

11.5.9.1 Reusing Hint Cache Entries

The same query matches the same cache entry regardless of its values unless the new value does not satisfy the hint rule conditions. Two examples are included below to demonstrate how the same hint cache entry can and cannot be used for multiple queries.

Example 1: Using Similar Hint Cache Entries

In the following two queries, the same hint cache entry is used because both queries match the hint rule requirements.

- **QueryA:**

```
SELECT *
FROM Revisions
WHERE dDocName = 'name1'
```

- **QueryB:**

```
SELECT *
FROM Revisions
WHERE dDocName = 'name2'
```

Example 2: Using Different Hint Cache Entries

In the following two queries, the same hint cache entry cannot be used because QueryB violates the requirements for the dReleaseState hint rule. The dReleaseState hint rule requires that the dReleaseState values are neither Y (released) nor O (old revision).

- **QueryA:**

```
SELECT *
FROM Revisions
WHERE dReleaseState = 'U' AND dStatus = 'DONE'
```

- **QueryB:**

```
SELECT *
FROM Revisions
WHERE dReleaseState = 'Y' AND dStatus = 'DONE'
```

11.5.9.2 Hint Cache Management

In the hint cache, you can add a new entry, edit an existing entry, or remove an existing entry using the Hint Cache Updater page. When adding or editing hint cache entries, you must use the [Content Server Hint Syntax](#). The ability to manage the hint cache is very useful for fine tuning query hints. The example below demonstrates the benefits of fine tuning a hint cache entry.

Example: Batchloading Unindexed Content

If you have just batchloaded 100K content items in to the Content Server and they are not yet indexed, the index-based query used above ([Example 2: Using Different Hint Cache Entries](#)) would match all of the batchloaded documents.

- **QueryA:**

If most of the batchloaded documents have not been indexed, the dReleaseState index that is used in this query is not the best choice. For the best results in this case, you should fine tune the hint cache entry to use both the dReleaseState and the dStatus indexes. Use the Hint Cache Updater page to update hint cache entries.

```
SELECT dID
FROM Revisions
WHERE Revisions.dReleaseState = N'N' AND Revisions.dStatus in (N'DONE', N'RELEASED',
N'DELETED') AND Revisions.dInDate<={ts '2005-02-23 17:46:38.321'}
```

- **QueryB:**

After updating the hint cache entry, the new optimized query is:

```
SELECT/** LEADING(revisions) INDEX (revisions dReleaseState dStatus)*/ dID
FROM Revisions
WHERE Revisions.dReleaseState = N'N' AND Revisions.dStatus in (N'DONE', N'RELEASED',
N'DELETED') AND Revisions.dInDate<={ts '2005-02-23 17:46:38.321'}
```

11.5.9.3 Default Capacity Algorithm

By default, the hint cache has a maximum capacity of 1000 hints. The hint cache uses the midpoint insertion least-recently-used (LRU) algorithm which is similar to the one used by

Oracle and MySQL. A new entry is inserted in to the middle of the queue and each subsequent execution moves the entry up one spot.

When the number of hints in the cache exceed the maximum capacity, the entry at the bottom of the queue is removed from the cache. Thus, the LRU algorithm ensures that the most recently executed query hints are in the upper levels of the queue.

11.5.9.4 Origin of Hint Cache Keys

The hint cache key is generated from the normalized query; for more information, see [Stage 3: Normalization](#). The cache key consists of the qualified columns (columns that are qualified by table/alias names) and columns that have a hint rule defined. The cache key excludes conditions that contain joins or subqueries.

The following example illustrates how the cache key is generated from a given query:

```
SELECT DocMeta.*, Documents.*, Revisions.*
FROM DocMeta, Documents, Revisions
WHERE DocMeta.dID = Revisions.dID AND Revisions.dID=Documents.dID AND
Revisions.dDocName='abc' AND Revisions.dStatus<>'DELETED' AND
(Revisions.dReleaseState='U' OR Revisions.dReleaseState='I' OR
Revisions.dReleaseState='Y') AND Documents.dIsPrimary<>0
```

The generated cache key is as follows:

```
documents.dIsPrimary:notequal:documents|revisions.dDocName:equal:revisions|
revisions.dReleaseState:in:revisions|revisions.dStatus:notequal:revisions
```

11.5.9.5 Hint Cache Persistence

The hint cache is designed to be persistent. To ensure the persistence, the hint cache is saved to the file system every two hours. The persisted hint cache is reloaded when the Content Server instance is started.

11.5.10 Using Hint Rules

The following tasks are involved in using hint rules:

- [Adding and Enabling New Hint Rules](#)
- [Editing Existing Hint Rules](#)
- [Disabling Hint Rules](#)
- [Enabling Hint Rules](#)
- [Removing Hint Rules](#)

To access the Edit Hint Rules Form, choose **Administration**, then **Oracle Query Optimizer**, then **Hint Rules Configuration**. The Hint Rules Configuration page opens, which includes the Edit Hint Rules Form.

11.5.10.1 Adding and Enabling New Hint Rules

To add a new hint rule to the Hint Rules Table:

1. Choose **Administration**, then **Oracle Query Optimizer**, then **Hint Rules Configuration**.
2. In the Edit Hint Rules Form, complete the fields. For more detailed explanations of each field, see [Hint Rules Table](#).

3. Click **Add**. The new hint rule is added to the Hint Rules Table and is effective immediately.

11.5.10.2 Editing Existing Hint Rules

To edit an existing hint rule in the Hint Rules Table:

1. Choose **Administration**, then **Oracle Query Optimizer**, then **Hint Rules Configuration**.
2. Select the desired hint rule in the Hint Rules Table on the Hint Rules Configuration page. All of the applicable fields in the Edit Hint Rules Form are populated with the hint rule's values.
3. Edit the fields as desired. For more details on each field, see [Hint Rules Table](#).
4. Change the key.
5. Click **Add**. The Hint Rules Table is refreshed and the new hint rule is added. The modifications are effective immediately.
6. Delete the old hint rule. For additional information, see [Removing Hint Rules](#).

11.5.10.3 Disabling Hint Rules

Although any rule in the table can be enabled/disabled, only the rules that are added through the Hint Rules Configuration page can be removed. The default hint rules that are included with the Oracle Query Optimization feature can only be disabled; they cannot be removed.

To disable a hint rule in the Hint Rules Table:

1. Choose **Administration**, then **Oracle Query Optimizer**, then **Hint Rules Configuration**.
2. Select the desired hint rule in the Hint Rules Table on the Hint Rules Configuration page. All of the applicable fields in the Edit Hint Rules Form are populated with the hint rule's values.
3. Click **Disable**. The Hint Rules Table is refreshed and 'Y' is displayed in the Disabled column, indicating that the hint rule is deactivated.

11.5.10.4 Enabling Hint Rules

Although any rule in the table can be enabled/disabled, only the rules that are added through the Hint Rules Configuration page can be removed. The default hint rules that are included with the Oracle Query Optimization feature can only be disabled; they cannot be removed.

To enable a disabled hint rule in the Hint Rules Table:

1. Choose **Administration**, then **Oracle Query Optimizer**, then **Hint Rules Configuration**.
2. Select the desired hint rule in the Hint Rules Table on the Hint Rules Configuration page. All of the applicable fields in the Edit Hint Rules Form are populated with the hint rule's values.
3. Click **Enable**. The Hint Rules Table is refreshed and the Disabled column is clear, indicating that the hint rule is reactivated.

11.5.10.5 Removing Hint Rules

Although any rule in the table can be enabled or disabled, only the rules that are added through the Hint Rules Configuration page can be removed. The default hint rules that are included with the Oracle Query Optimization feature can only be disabled; they cannot be removed.

To delete a hint rule from the Hint Rules Table:

1. Choose **Administration**, then **Oracle Query Optimizer**, then **Hint Rules Configuration**.
2. Select the desired hint rule in the Hint Rules Table on the Hint Rules Configuration page. All of the applicable fields in the Edit Hint Rules Form are populated with the hint rule's values.
3. Ensure that the hint rule is enabled. If the hint rule is disabled it cannot be removed. To reactivate a disabled hint rule, see [Hint Rules Table](#).
4. Click **Remove**. The Hint Rules Table is refreshed and the selected hint rule is removed.

11.5.11 Using the Query Converter

The Query Converter can be used to view the result of a converted query and to modify a converted query by adding, editing, or deleting conditions from the WHERE clause. Modifying a converted query enables you to see exactly what will be executed when the query is submitted. Converted queries optionally can include data sources.

The following tasks are involved when you use the Query Converter:

- [Converting a Data Source](#)
- [Converting a Query](#)
- [Editing a Converted Data Source or Query](#)

11.5.11.1 Accessing the Query Converter Page

To access the Query Converter page:

1. Choose **Administration**, then **Oracle Query Optimizer**.
2. Click **Query Converter**.

11.5.11.2 Converting a Data Source

To convert a data source query:

1. If applicable, on the Query Converter page select **Use Data Source**. The data source-related fields are displayed on the Query Converter page.
2. Select the desired data source from the **DS Name** menu. The data source query is displayed in below the **DS Name** field.
3. Enter the applicable information for additional parameters and WHERE clauses.
4. Click **Convert Query**. The data source is converted and the results are displayed in a text area above the **Use Data Source** check box. To view an example of a converted data source query, see [Figure 11-5](#).

11.5.11.3 Converting a Query

To convert a query:

1. If applicable, on the Query Converter page deselect **Use Data Source**. The data source-related fields are hidden from the Query Converter page.
2. Enter the applicable information for the query.

3. Click **Convert Query**. The query is converted and the results are displayed in a text area above the Use Data Source check box. To view an example of a converted query, see [Figure 11-6](#).

Figure 11-5 Example of Converted Data Source Page

Converted Data Source

Name Documents

Query

```
SELECT Revisions.*, DocMeta.*, Documents.* FROM Revisions, DocMeta, Documents WHERE Revisions.dID = Documents.dID AND Revisions.dID = DocMeta.dID AND Documents.dIsPrimary <> 0
```

Where Clause

Use Data Source

DS Name Documents

Additional Parameters

Where Clause

Convert Query

Figure 11-6 Example of Converted Query Page

Converted Query
select * from revisions where did = 3

Use Data Source

Query

Convert Query

11.5.11.4 Editing a Converted Data Source or Query

After the data source or query is converted, the results are displayed above the Use Data Source check box. Because the conversion process clears the fields, the converted query can only be modified by entering new information in the fields. To edit information for a data source or query, see the applicable sections in [Converting a Data Source](#).

11.5.12 Updating the Hint Cache

The following tasks are involved when updating the hint cache:

- [Accessing the Hint Cache Updater Page](#)
- [Checking the Hint Cache from a Data Source](#)
- [Checking from a Query](#)

- [Modifying an Existing Hint Cache Query Using Data Source](#)
- [Modifying an Existing Hint Cache Using a Query](#)
- [Removing a Hint Cache Data Source Entry](#)
- [Removing a Hint Cache Query](#)

11.5.12.1 Accessing the Hint Cache Updater Page

To access the Hint Cache Updater page:

1. Choose **Administration**, then **Oracle Query Optimizer**.
2. Click **Hint Cache Updater**.

11.5.12.2 Checking the Hint Cache from a Data Source

To check the hint cache using a data source:

1. On the Hint Cache Update page, select **Use Data Source**. The data source-related fields are displayed on the Hint Cache Updater page.
2. Select the desired data source from the **DS Name** menu. The data source query is displayed in below the **DS Name** field.
3. Enter the applicable information for the additional parameters, WHERE clause, and hints.
4. Click **Check Cache**. The results are displayed above the Use Data Source check box. To view an example of an unsuccessful hint search, see [Figure 11-7](#).

Figure 11-7 Example of Hint Cache Updater Results with Data Source

Hint Not Found	data source	Documents
	where clause	revisions.dreleasestate = n'n'
	cache key	revisions.dreleasestate:notin:('y','o'):revisions
	message	Hint does not exist in cache.

Use Data Source

DS Name Documents

SELECT Revisions.*, DocMeta.*, Documents.* FROM Revisions, DocMeta, Documents WHERE Revisions.dID = Documents.dID AND Revisions.dID = DocMeta.dID AND Documents.dIsPrimary < > 0

Additional Parameters

Where Clause

Hints

Check Cache Update Cache Remove

11.5.12.3 Checking from a Query

To check the hint cache using a query:

1. On the Hint Cache Update page, ensure the **Use Data Source** check box is unselected. The data source-related fields are hidden from the Query Converter page.

2. Enter the applicable information.
3. Click **Check Cache**. The results are displayed above the Use Data Source check box. To view an example of an unsuccessful hint search, see [Figure 11-8](#). To view an example of a successful hint search, see [Figure 11-9](#).

Figure 11-8 Example of Hint Cache Updater Results without Data Source

Hint Not Found	query	SELECT Revisions.*, DocMeta.*, Documents.* FROM Revisions, DocMeta, Documents WHERE Revisions.dID = Documents.dID
	message	Hint does not exist in cache.

Use Data Source

Query

Hints

Check Cache Update Cache Remove

Figure 11-9 Hint Found in Hint Cache

Hint Found	query	SELECT dID FROM Revisions WHERE Revisions.dReleaseState = N'N' AND Revisions.dStatus in (N'DONE', N'RELEASED', N'DELETED') AND Revisions.dInDate<={ts '2005-05-25 05:34:34.432'}
	cache key	Revisions revisions.dindate:le:revisions revisions.dreleasestate:notin:('y','o'):revisions revisions.dstatus:in:revisions
	old hint	Revisions Revisions:dReleaseState:dReleaseState:3:('y','o'):1:Revisions

Use Data Source

Query

Hints

Check Cache Update Cache Remove

11.5.12.4 Modifying an Existing Hint Cache Query Using Data Source

To modify a hint cache query using a data source:

1. On the Hint Cache Updater page, select **Use Data Source**. The data source-related fields are displayed on the Hint Cache Updater page.
2. Select the desired data source from the **DS Name** menu. The data source query is displayed below the **DS Name** field.
3. Enter the applicable information for the additional parameters, WHERE clause, and hints.
4. Click **Update Cache** to overwrite the previous hint cache. The results are displayed in a text box above the **Use Data Source** check box. To see an example of successfully adding

a new hint to a query and updating the hint cache, see the page capture included in this section.

11.5.12.5 Modifying an Existing Hint Cache Using a Query

To modify a hint cache using a query:

1. On the Hint Cache page, ensure that the **Use Data Source** check box is unselected. The data source-related fields are hidden from the Query Converter page.
2. Enter the applicable information.
3. Click **Update Cache** to overwrite the previous hint cache. The results are displayed above the Use Data Source check box. On the page capture note that the new hint was added and the hint cache was updated.

Figure 11-10 New Hint Added, Hint Cache Updated

query	SELECT dID FROM Revisions WHERE Revisions.dReleaseState = N'N' AND Revisions.dStatus in (N'DONE', N'RELEASED', N'DELETED') AND Revisions.dInDate<={ts '2005-05-25 05:34:34.432'}
Updated cache key	Revisions revisions.dindate:le:revisions revisions.dreleasestate:notin:('y','o'):revisions revisions.dstatus:in:revisions
old hint	Revisions Revisions:dReleaseState:dReleaseState:3:('y','o'):1:Revisions
new hint	Revisions:dInDate:dInDate:3:(,7d):0:revisions
message	Hint cache is updated

Use Data Source

Query

Hints

11.5.12.6 Removing a Hint Cache Data Source Entry

To remove a hint cache data source entry:

1. On the Hint Cache Updater page, select **Use Data Source**. The data source-related fields are displayed on the Hint Cache Updater page.
2. Select the desired data source from the **DS Name** menu. The data source query is displayed below the **DS Name** field.
3. Enter the applicable information for the additional parameters, WHERE clause, and hints.
4. Click **Remove**. The information entered in to the fields is removed. To see an example of successfully removing a hint from a query and the hint cache, see the page capture included in this section.

11.5.12.7 Removing a Hint Cache Query

To remove a hint cache query:

1. On the Hint Cache Updater page, ensure that the **Use Data Source** check box is unselected. The data source-related fields are hidden from the Query Converter page.

2. Enter the applicable information for the query and hints.
3. Click **Remove**. The results are displayed above the **Use Data Source** check box. On the page capture note that the previously added hint was deleted from the query and hint cache.

Figure 11-11 Example of a Deleted Hint from Cache

Removed	query	SELECT dID FROM Revisions WHERE Revisions.dReleaseState = N'N' AND Revisions.dStatus in (N'DONE', N'RELEASED', N'DELETED') AND Revisions.dInDate<={ts '2005-05-25 05:34:34.432'}
	cache key	Revisions[revisions.dindate:le:revisions[revisions.dreleasestate:notin: ('y','o'):revisions[revisions.dstatus:in:revisions
	old hint	Revisions:dInDate:dInDate:3:(,7d):0:revisions
	message	Hint is removed from cache.
<p>Use Data Source <input type="checkbox"/></p> <p>Query <input type="text"/></p> <p>Hints <input type="text"/></p> <p style="text-align: center;"> <input type="button" value="Check Cache"/> <input type="button" value="Update Cache"/> <input type="button" value="Remove"/> </p>		

11.6 Improving Search Performance

This section contains information about improving search performance.

11.6.1 Improving Database Search on the Title Field

if you frequently search on the Title field and your site has more than 1 million records, and you are using database search, it is recommended that you create an index based on dDocTitle and dReleaseState.

11.6.2 Reducing Unnecessary SQL Queries

If you find that you have unnecessary SQL queries being triggered because each query is determining the folder path for every entry part of the search result set, and you do not need the folder path information, you can improve performance by turning off the `FolderPathInSearchResults` configuration variable in the Additional Configuration Variables portion of the `config.cfg` file.

12

Managing a File Store System

This chapter describes how to configure the Oracle WebCenter Content Server file store system and use the File Store Provider.

This chapter includes the following topics:

- [Introduction to the File Store System](#)
- [About the File Store Provider Upgrade](#)
- [Managing the File Store Provider](#)
- [Sample Implementations of File Store Provider](#)
- [Using Sun Storage Archive Manager](#)

Note:

Oracle supports the Sun Storage Archive Manager (SAM-QFS) with the WORM option as an alternative to the Content Server standard file store system. For details, see [Using Sun Storage Archive Manager](#).

Once you have configured Content Server to use SAM-QFS, you cannot revert to using the standard file store system.

12.1 Introduction to the File Store System

With the release of version 11R1, Content Server implemented a file store system for data management, replacing the traditional file system for storing and organizing content. The FileStoreProvider component exposes the file store functionality in the Content Server interface and allows additional configuration options. For example, you can configure the Content Server instance to use binary large object (BLOB) data types to store content in a database, instead of using a file system. This functionality offers several advantages:

- Integrates repository management with database management for consistent backup and monitoring processes.
- Helps overcome limitations associated with directory structure and number of files per directory in a file system approach.
- Aids in distributing content more easily across systems, for better scaling of Content Server.
- Allows for different types of storage devices not commonly associated with a file system, for example, content addressed storage systems and write-only devices necessary in some business uses.

With a huge volume of data to manage in a database, one solution to keeping the database running is to use database partitions for your content repository. This requires careful planning. For more information, see the "Partitioned Repository for WebCenter Content using Oracle Database 11g" blog.

▲ Caution:

The FileStoreProvider component is installed, enabled, and upgraded by default during Content Server deployment. It should not be uninstalled or disabled after the default file store is upgraded. For more information on upgrading, see [About the File Store Provider Upgrade](#).

If you have an earlier version of Content Server software where you have not yet upgraded the default file store, you can disable the component following the procedure in [Enabling or Disabling a Component Using the Component Manager](#).

This section covers the following topics:

- [Data Management](#)
- [File Store Provider Features](#)

12.1.1 Data Management

Content Server manages content by tracking the storage of electronic files and their associated metadata. It provides the ability for users to store and access their checked in files, any associated information, and any associated renditions. This section discusses the data management methods historically used by Content Server and how they are addressed with the FileStoreProvider component.

- [File Management](#)
- [Metadata Management](#)
- [File Stores](#)

12.1.1.1 File Management

The first half of data management is storing electronic files checked in to a Content Server repository. With Content Server, file storage has typically been done with a traditional file system, storing electronic files in a hierarchical directory structure that includes vault and weblayout directories. By using the revision information specified by the content type, security group, and account (if used), files and their associated renditions are placed into particular directories within the vault and weblayout directories. For example, the primary and alternate files specified at check in are stored in subdirectories in the vault directory. The specific file location is defined to be the following:

IntradocDir/vault/dDocType/account/dID.dExtension

In this path name, *dDocType* is the content type chosen by the user on check in, *dID* is the unique system-generated identification that identifies this revision, and *dExtension* is the extension of the file checked in. In this hierarchical model, the system uses the *dDocType* metadata field to distribute the files within the hierarchy established in the vault directory. Similarly, any web rendition is distributed across the hierarchy within the *IntradocDir/weblayout/groups/* directory. The web rendition is the file served out of a web server, and in the historical file system storage method, could be the native file, the alternate file, or a web-viewable file generated by Inbound Refinery or some other conversion application.

This straightforward determination of file storage location is helpful to component and feature writers, helping them understand where files are located and how to manipulate them.

However, it also has the effect of limiting storage management. Without careful management of the location metadata, directories can become saturated, causing the system to slow down.

12.1.1.2 Metadata Management

The second half of data management is storing metadata associated with an electronic file. With Content Server, metadata management has typically been done using a relational database, primarily involving three database tables. Metadata enables users to catalogue content and provides a means for creating file descriptors to facilitate finding it within the Content Server repository. For users, the retrieval is done by Content Server, and how and where the file is stored can be completely hidden. For component and feature writers, who may need to generate or manipulate files, the metadata provides a robust means of access.

12.1.1.3 File Stores

The traditional file system model historically used by Content Server limits scalability. As data management needs grow, adding extra storage devices to increase storage space is not conducive to easy file sharing through a web-based interface. Complex, nested file structures could slow performance. Suppressing the creation of a duplicate web-viewable file when the native file format could be used could be difficult. As a consequence of dealing with large systems, for example over 100 million content items, Content Server has shifted to using a file store. This offers the advantages of scalability, flexibility, and manageability.

12.1.2 File Store Provider Features

The FileStoreProvider component enables you to define data-driven rules to store and access content managed by Content Server. File Store Provider offers the following features:

- The ability to relocate files easily
- The ability to have the web-viewable file be optional
- The ability to manage and control directory saturation
- The ability to integrate with third-party storage devices
- An API to use, extend, and enhance different storage paradigms

With File Store Provider, checked-in content and associated metadata are examined and assigned a storage rule based on criteria established by a system administrator. Criteria can include metadata, profiles, or other considerations. The storage rule determines how vault and web files are stored by Content Server and how they are accessed by a web server.

12.2 About the File Store Provider Upgrade

The FileStoreProvider component is installed, enabled, and upgraded by default for a Content Server instance with no documents in it. The upgrade includes creation of metadata fields with default values for the file store system (DefaultFileStore). If an existing Content Server instance with documents in it and no File Store Provider is upgraded to a newer version of Content Server, the File Store Provider upgrade is not automatically performed.

If you do not want to upgrade File Store Provider from your current settings, prior to upgrade installation you must add the configuration variable `FsAutoConfigure=false` in the Content Server `config.cfg` file.

▲ Caution:

If you start the Content Server instance to set the variable in the **Additional Configuration Variables** field on the General Configuration page, then Content Server will automatically upgrade File Store Provider.

12.2.1 DefaultFileStore Settings

A Content Server instance containing no documents and with the FileStoreProvider component automatically upgraded uses these DefaultFileStore settings. The settings are single lines of code, not wrapped as shown here.

- Vault Path:

```
$#env.VaultDir$$dDocType$/ $dDocAccount$/ $dispersion$/ $dID$$ExtensionSeparator$
$dExtension$
```

- Dispersion Rule:

```
$dRevClassID[-9:-6:0:b]/ $dRevClassID[-6:-3:0:b]
```

If encoding is not required, specify:

```
$dRevClassID[-9:-6:0]/ $dRevClassID[-6:-3:0]
```

- Web-viewable Path:

```
$#env.WeblayoutDir$groups/ $dSecurityGroup$/ $dDocAccount$/ documents/ $dDocType$/
$dispersion$/ $edisp$/ $dDocName$$RenditionSpecifier$$RevisionLabel$
$ExtensionSeparator$$dWebExtension$
```

- Web URL File Path:

```
$HttpWebRoot$groups/ $dSecurityGroup$/ $dDocAccount$/ documents/ $dDocType$/
$dispersion$/ $edisp$/ $dDocName$$RenditionSpecifier$$RevisionLabel$
$ExtensionSeparator$$dWebExtension$
```

The dispersion field is added in Path information for the storage rule and can be edited. The Web-viewable Path and Web URL File Path fields cannot be edited. The dispersion rule is added in web paths at the `$dispersion$` location.

The dispersion rule allows you to specify `:b` for base 64 encoding of that part of the URL. For example, the following dispersion rule encodes the two parts to be base 64:

```
$dRevClassID[-9:-6:0:b]/ $dRevClassID[-6:-3:0:b]
```

A Content Server instance containing documents and which does not have the FileStoreProvider component upgrade will return an informational message that the Revisions table is not empty, therefore dispersion for the default storage rule is not set for DefaultFileStore.

12.2.2 Empty Storage Rule

If a site has used an earlier version of Content Server without using the file store system, then upgraded and implemented the FileStoreProvider component, or a site has uninstalled the FileStoreProvider component completely and also removed the metadata fields added by File Store Provider, then when a user checks in a document it will not have an associated storage rule (no `xStorageRule` field). When File Store Provider is implemented after these types of situations, users will find that documents checked in before File Store Provider was

implemented will have an empty `xStorageRule` field. To fix this situation, users must perform an Update to the Content Information for those documents. The documents will be updated to the default value of the `xStorageRule` field and will be moved to the location specified by the storage rule. For details on `xStorageRule`, see [Content Server Metadata Fields](#).

12.3 Managing the File Store Provider

A file store for data management is used in Content Server instead of the traditional file system for storing and organizing content. The `FileStoreProvider` component is installed and enabled by default during Content Server deployment. The `FileStoreProvider` component automatically upgrades the default file store (`DefaultFileStore`) to make use of functionality exposed by the component, including modifying the web, vault, and web URL path expressions.

Note:

Partitions are not required to run Content Server, but any attempt to check in content before creating a partition, changing the vault path root, or creating a new, well-formed storage rule will fail. For more information, see [Understanding File Store Provider Storage Principles](#), including the sections on storage rules and path construction.

Note:

Oracle WebLogic Server does not support configuring its web server for the Content Server instance to add a new virtual directory and alias to point to the `weblayout` directory for each partition that is created. Partitions can be used for the vault files, and partitions are supported for web files, but the partition root must exist under the default vault and `weblayout` directories.

Caution:

Resource files should not be edited directly. Proper modification of resource files should be done within the Content Server administration interface or through additional component development. For more information on component development, see [Managing Components](#).

Three resource tables are used to define and handle file paths. The defaults for the [PathMetaData Table](#) and [PathConstruction Table](#) cover most scenarios. The [StorageRules Table](#) stores the values specified when a storage rule is defined. These three tables are provider-specific, and as such are defined in the `provider.hda` file of the `defaultfilestore/` directory. The `defaultfilestore/` directory is located in the `IntradocDir/data/providers/` directory. A fourth table, the [FileSystemFileStoreAlgorithmFilters Table](#), requires a component along with Java code to modify.

This section covers the following topics:

- [Understanding File Store Provider Storage Principles](#)
- [About File Store Provider Modifications to Content Server](#)

- [File Store Provider Resource Tables](#)
- [Working with the File Store Provider](#)

12.3.1 Understanding File Store Provider Storage Principles

When a content item is checked in to Content Server, it consists of metadata, a primary file selected by the user, and potentially an alternate file. The alternate file may also be selected and checked in by the user, and is presumed to be a web-viewable file. In a file system approach to Content Server, the primary file is stored in the `vault` directory at the root of the `DomainHome/` directory and is called the native file. If an alternate file is checked in, it is also stored in the vault, but is copied to the `weblayout` directory or passed to a conversion application, such as Inbound Refinery. If no alternate file is checked in, then the native file is copied from the `vault` directory to the `weblayout` directory, existing in two places. If no alternate file is checked in and Inbound Refinery is installed, a rendition of the native file could be created and stored in `weblayout` directory.

In a file system approach to Content Server, storing content in specified directories defines a path to the content. You can access content from a browser by using a static web URL file path, when you know the content is in a specific location, or using a dynamic Content Server service request, such as `GET_FILE`, when you do not. With File Store Provider, content may or may not be stored in a file system. Consequently, a new approach to defining paths to the content must be taken.

Depending on how you set up File Store Provider, you may or may not have a static web URL. By using a dynamic Content Server service request, you can access content when you do not know the specific location. With File Store Provider, the static web URL is defined as the *web URL file*, and the dynamic access is simply called the *web URL*. Using the File Store Provider interface, you can configure only the static web URL file path. However, you can decide to have the static web URL done as a Content Server service request, essentially making it dynamic.

Note:

- The default caching headers have changed so that all pages served from the Content server have the no-cache headers set and thus caching servers will not cache the pages.
- Cacheable pages may not be an ideal solution in some environments. If the server content pages contain sensitive information, then they should not be cached because they can be retrieved by anyone who has access to the computer.
- Not all pages need to have the headers to avoid caching: Static pages that do not contain sensitive information and static files such as static pictures can be cached to improve performance.
- Cached information does not compromise the security of the application, as the pages that are being cached do not disclose any additional information.

This section covers the following topics:

- [Using Storage Rules on Renditions to Determine Storage Class](#)
- [Understanding Path Construction and URL Parsing](#)

12.3.1.1 Using Storage Rules on Renditions to Determine Storage Class

When content is checked in, all versions of the content managed by Content Server are considered renditions. These renditions include the native file, web-viewable file, and any other files that may have been rendered by Inbound Refinery or third-party conversion applications.

Renditions are grouped together into a storage class, which determines where and how a rendition is accessed. Storage classes are grouped together into a storage rule, which defines the vault, web, and web URL path expressions, through a storage class. Additionally, a storage rule determines if a rendition is not stored, as in a web-less file store, or if it is stored in a different device, such as a database rather than a file system.

The following examples illustrate how storage rules can determine where and how different content items can be stored.

Example 1

A storage rule is defined as **File system only** on the Storage Rule Name dialog and **Is Webless File Store** is not selected. In this scenario, the system makes a copy of the primary files and places them in the weblayout directory.

This traditional file system storage example typically offers the advantage of faster access time to content when compared with database storage. This advantage diminishes if the file system hierarchy is complex or becomes saturated, or as the quantity of content items increases.

Example 2

A storage rule is defined as **File system only** on the Storage Rule Name dialog and **Is Webless File Store** is selected. In this scenario, no copy is made of the primary files and so the native files are the only renditions. Requests for web-viewable files are routed to the native files stored in the vault.

 **Note:**

The web-less option of File Store Provider can specify that no web rendition be created. When this is used in conjunction with Inbound Refinery, a web rendition is always created and stored in either the file system or the database, depending on the storage rule in effect.

This traditional file system storage example, like the previous one, offers the advantage of faster access time to content. It also saves on storage space by not copying a version of the content from the vault directory to the weblayout directory. Instead, it redirects web-viewable access to the content in the vault directory. This is useful if most of the native files checked in are in a web-viewable format, or if Content Server is being used to manage content that is not required to be viewed in a browser.

Example 3

A storage rule is defined as **JDBC Storage** on the Storage Rule Name dialog and no selection is made from the **Renditions** choice list. In this scenario, both the vault and web files are stored in the database.

This database storage example offers the advantage of integrating repository management with database management for consistent backup and monitoring processes, and helps

overcome limitations associated with directory structure and number of files per directory in a file system approach.

! Important:

When necessary, content items stored in a database can be forced onto the file system, for example, during indexing or conversion. The files on the file system are treated as temporary cache and deleted following the parameters specified in the `config.cfg` file located in the `IntradocDir/config/` directory. For more information on the parameters used, see [FileCache Table](#).

Example 4

A storage rule is defined as **JDBC Storage** on the Storage Rule Name dialog and **Web Files** is selected from the **Renditions** choice list. In this scenario, the vault files are stored in the database and the web files are permanently stored on the file system.

This mixed approach of storing native files in a database but web-viewable files on a file system offers the advantages of database storage in the previous example (integrated backup and monitoring, overcoming file system limitations) for the native files, while providing speedy web access to web-viewable renditions. Like the first example, this advantage can be diminished if the file system structure is overly complex, or the quantity of files is extreme.

12.3.1.2 Understanding Path Construction and URL Parsing

The path to content stored in Content Server is defined in the PathExpression column of the [PathConstruction Table](#). Paths are made up of pieces, with each piece separated by a slash (/). Each piece can be made of a static string or a sequence of dynamic parts. A dynamic part is encapsulated by a dollar sign (\$). A part can be calculated using an algorithm, Idoc Script variable, environment variable, or a metadata lookup, and can have the following interpretations:

- It can be a field defined in the PathMetaData table. If it is defined in the PathMetaData table, it can be mapped to an algorithm, for example:

```
$dDocType$
```

- If it has the prefix `#env.`, it is an environment variable, for example:

```
$#env.VaultDir$ or $#env.WeblayoutDir$
```

- It can be an Idoc Script variable, such as `$HttpWebRoot$`. For example, the standard vault location is defined as follows:

```
$PartitionRoot$/vault/$dDocType$/$dDocAccount$/$dID$$ExtensionSeparator$  
$dExtension$
```

When parsed, the path expression turns into five pieces, interpreted according to the rules specified in the PathMetaData table, as follows:

- **\$PartitionRoot\$**: mapped to the partitionSelection algorithm and uses the xPartitionId as a lookup into the PartitionList table to determine the partition root
- **/vault/**: a string, so no calculation or substitution
- **\$dDocType\$**: by the PathMetaData table this is a look up in the file parameters

- **\$dDocAccount\$**: this is mapped to a documentAccount algorithm which takes dDocAccount and parses it into the standard Content Server account presentation with all the appropriate delimiters
- **\$dID\$\$ExtensionSeparator\$\$dExtension\$**: this piece has three parts:
 - **\$dID\$**: similar to dDocType, this is defined in the file parameters and is a required field
 - **\$ExtensionSeparator\$**: determined by an algorithm and by default it returns '.'
 - **\$dExtension\$**: similar to dDocType

In the standard configuration for the web-viewable path, the URL contains variables to add the partition root to the web-viewable path, security, dDocType, and dispersion information, as well as the dDocName, rendition, and extension information. `FsWeblayoutDir` denotes `$#env.WeblayoutDir$` by default.

```
$FsWeblayoutDir$groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/$dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$$ExtensionSeparator$$dWebExtension$
```

In the standard configuration for the web URL file path, the URL contains variables to add the partition root to the web-viewable path, security, dDocType, and dispersion information, as well as the dDocName, rendition, and extension information. `FsHttpWebRoot` denotes `$HttpWebRoot$` by default.

```
$FsHttpWebRoot$groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/$dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$$ExtensionSeparator$$dWebExtension$
```

The `groups` separator indicates to Content Server that the directories that follow are the name of the security group and account to which the content item belongs. Accounts are optional and consequently computed by an algorithm. After the security information is the `documents` separator, which is immediately followed by the `dDocType`. Dispersion is optional. The last part of the URL is the `dDocName`, its rendition and revision information, and its format extension.

Because the URL is expected in this format, Content Server can successfully extract metadata from it. More importantly, it can determine the security information for the content item and derive the access privileges for a particular user.

The parsing guidelines have been expanded to allow for dispersion in the web directory. When `$dRevClass$` is encountered, the system processes the dispersion information, then continues with `dDocName` and `dWebExtension` as before. This means that the system can now successfully parse URLs of the form:

```
../groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/$dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$$ExtensionSeparator$$dWebExtension$
```

12.3.2 About File Store Provider Modifications to Content Server

The `FileStoreProvider` component makes several modifications to the Content Server database, Content Server metadata fields, and other configuration files, allowing for possible configuration options.

This section covers the following topics:

- [Database Options](#)
- [Content Server Metadata Fields](#)

12.3.2.1 Database Options

In some situations, content stored in a database may have to be forced onto a file system. One example would be when Oracle WebCenter Content: Inbound Refinery must have access to a file for conversion. Files forced onto a file system are considered temporary cache. The following configuration values are used to control when the temporarily cached files are to be cleaned up. Note that the system only cleans up files that have an entry in the [FileCache Table](#).

Variable	Description
FsCacheThreshold	Specifies the maximum cache size, in megabytes. The default is 100. When the threshold is met, the Content Server instance starts deleting files that are older than the minimum age, as specified by the FsMinimumFileCacheAge parameter.
FsCleanUpCacheDuringIndexing	Specifies if the cache will be cleaned during the indexing cycle. The default is <code>false</code> .
FsCleanUpCacheIndexingMax	Specifies the number of cache files to delete in each indexing cycle, which limits the load on the cycle. The default is to delete all eligible cache files for the indexing cycle.
FsMaximumFileCacheAge	Specifies the maximum age at which files are cached, expressed in days. The default is 365.
FsMinimumFileCacheAge	Specifies the minimum age at which cached files can be deleted, expressed in days. The default is 1. This parameter is used in conjunction with the FsCacheThreshold parameter to determine when to delete cached files.

12.3.2.2 Content Server Metadata Fields

File Store Provider adds several Content Server metadata fields and makes additional options available for use in configuration files.

12.3.2.2.1 Configuring Metadata Fields

File Store Provider adds three metadata fields to the Content Server instance:

- **xPartitionId:** This metadata field is used in conjunction with the PartitionList table to determine the root location of the content item files. It is recommended that this field be hidden on the user interface, because the partition selection algorithm provides a value.
- **xWebFlag:** This metadata field is used to determine whether a content item has a web-viewable file. Consequently, if the system has content items that have only vault files, then removing this metadata field causes the system to expect the presence of a web-viewable and may cause harm to the system. The metadata field can be specified by the configuration value `WebFlagColumn`.
- **xStorageRule:** This metadata field is used to track the rule that was used to determine how the file is to be stored. The metadata field may be specified by the configuration value `StorageRuleField`.

 **Note:**

These metadata fields are added by File Store Provider on startup and if deleted are added again when the Content Server instance restarts. If the metadata fields must be permanently deleted, set the configuration variable `FsAddExtraMetaFields=false` in the `intradoc.cfg` file to disable the automatic creation of the fields. The `intradoc.cfg` file is located in the `DomainHome/ucm/cs/bin/` directory.

12.3.2.2.2 Setting the Default Storage Directory

A `StorageDir` parameter can be set equal to a root directory, used for all partitions where the `PartitionRoot` column value has not been specified. In this case the storage directory and the partition name is used to create the `PartitionRoot` parameter. The `StorageDir` parameter is set in the `intradoc.cfg` file, located in the `DomainHome/ucm/cs/bin/` directory.

12.3.2.2.3 Standard File Store Variables

In the `provider.hda` file located in the `IntradocDir/data/providers/defaultfilestore/` directory, the following parameters and classes are standard for a file system store:

```
ProviderType=FileStore
ProviderClass=intradoc.filestore.BaseFileStore
IsPrimaryFileStore=true
# Configuration information specific to a file system store provider.
ProviderConfig=intradoc.filestore.filesystem.FileSystemProviderConfig
EventImplementor=intradoc.filestore.filesystem.FileSystemEventImplementor
DescriptorImplementor=intradoc.filestore.filesystem.FileSystemDescriptorImplementor
AccessImplementor=intradoc.filestore.filesystem.FileSystemAccessImplementor
```

12.3.3 File Store Provider Resource Tables

This section covers the following topics:

- [PartitionList Table](#)
- [StorageRules Table](#)
- [PathMetaData Table](#)
- [PathConstruction Table](#)
- [FileSystemFileStoreAlgorithmFilters Table](#)
- [FileStorage Table](#)
- [FileCache Table](#)

12.3.3.1 PartitionList Table

The `PartitionList` table defines the partitions that are available for the `partitionSelection` algorithm. The table is defined in the `fsconfig.hda` file, located in the `DomainHome/ucm/cs/data/filestore/config/` directory, and modified using the `Add/Edit Partition` page in the Content Server interface. The columns of the table are used as follows:

Column	Description
PartitionName	Specifies the name of the partition. This name is referenced in the path expression.
PartitionRoot	An argument passed into the partitionSelection algorithm.
IsActive	Determines if the partition is currently active and accepts new files.
CapacityCheckInterval	Specifies the interval in seconds used in determining the available disk space. This may not work on all platforms.
SlackBytes	Determines if there is sufficient space on a partition to store content. If the available space is lower than the slack bytes, the partition is deactivated and no longer used for contribution.
DuplicationMethods	Specifies how native files are treated when not converted to a web-viewable rendition. copy (default): copies the native file to the web path. link : Resolves the web path to the native file in the vault Copy and Link rely on functionality of the operating system on which the Content Server instance is installed. As such, not all methods are available on all platforms

12.3.3.2 StorageRules Table

The StorageRules table defines the rules used for storing content items. The rule specifies which path expression to use for which storage class, and how content items are to be stored.

The table is defined in the *provider.hda* file, located in the *DomainHome/ucm/cs/data/providers/defaultfilestore/* directory, and it can be modified using the Storage Rule Name dialog in the Content Server interface. The columns of the table are used as follows:

Column	Description
StorageRule	The name of the storage rule. Computed from a dynamic include and stored in the <code>xStorageRule</code> metadata field of a content item.
StorageType	Determines the storage implementation. FileStorage : files are stored on the file system JdbcStorage : files are stored in the database
IsWeblessStore	Used to specify if system allows web-less files. true : By default, newly created content items do not have a web-viewable file. In certain circumstances it is necessary to insist on a web-viewable file. In such situations, an argument in the calling code can be used to specify that a web-viewable file must be created. Information regarding whether there is a web-viewable file is stored in the <code>xWebFlag</code> metadata field. false : By default, newly created content items do have a web-viewable file.
RenditionsOnFileSystem	Used by JdbcStorage to determine if any files are to be stored on the file system instead of the database.

12.3.3.3 PathMetaData Table

The PathMetaData table defines what metadata is used to determine the location of a file. The metadata may come directly from a content item's metadata, or be calculated using an algorithm. The PathMetaData table is defined in the *provider.hda* file of the

`defaultfilestore/ directory`. The `defaultfilestore/ directory` is located in the `DomainHome/ucm/cs/data/providers/ directory`.

The columns of the table are used as described in the following table.

Column	Description
FieldName	Name of the field as it appears in the path expression.
GenerationAlgorithm	Specifies the algorithm used to resolve or compute the value for the field.
RequiredForStorage	Defines for which storage class the metadata is required. #all : Both vault and web-viewable renditions require the metadata web : Just the web-viewable rendition requires the metadata vault : Just the native file rendition requires the metadata The field is optional for all renditions not specified. Consequently, if this column is empty, then the metadata field is optional for all renditions or storage classes. If an algorithm has been specified, this value is empty. The algorithm uses the value specified in the ArgumentFields column to dictate which fields are required.
Arguments	Optional arguments passed into the algorithm specified in the GenerationAlgorithm field.
ArgumentFields	A comma-delimited list of fields required by the arguments defined in the Arguments column, and consequently required by the algorithm specified in the GenerationAlgorithm field.

12.3.3.4 PathConstruction Table

The PathConstruction table maps a file to a path. The PathConstruction table is defined in the `provider.hda` file of the `defaultfilestore/ directory`. The `defaultfilestore/ directory` is located in the `DomainHome/ucm/cs/data/providers/ directory`. For more information, see [Understanding Path Construction and URL Parsing](#).

Caution:

The defaults provided in the PathConstruction table should work for most scenarios. This resource file should not be edited directly. Proper modification should be done through additional component development. For more information on component development, see the chapter about components in *Developing with Oracle WebCenter Content*.

The columns of the PathConstruction table are defined in the following table.

Column	Description
FileStore	<p>Specifies the storage path that is being calculated.</p> <p>web: Path to the web-viewable file.</p> <p>vault: Path to the native file.</p> <p>weblink: Generated by Content Server. Tends to be GET_FILE.</p> <p>weblink.file: Nicely constructed URL used to access the web-viewable rendition in a browser.</p> <p>dispersion: Variable for dispersion of content on the file system.</p> <p>FsWeblayoutDir: Variable for the web-viewable path for the weblayout directory.</p> <p>FsHttpWebRoot: Variable for the web URL file path for the weblayout directory</p>
PathExpression	Defines the path.
AutoCreateLimit	Specifies the depth of the directories that may be created.
StorageRule	Specifies to which storage rule this path construction belongs.

12.3.3.5 FileSystemFileStoreAlgorithmFilters Table

The FileSystemFileStoreAlgorithmFilters table is used to map an algorithm name to an implementation of the FilterImplementor interface. The algorithm can be referenced in the [PathMetaData Table](#) and is used to calculate the desired path field. The class implementing the algorithm must return the required metadata fields it uses for calculation, when the file parameters object is null. Through the ExecutionContext, the doFilter method is passed in information about the field, content item, and file store provider that initiated the call. In particular, for the file system provider, the algorithm will be passed the following information through the ExecutionContext. Bear in mind that other file store providers may choose to pass in more or possibly different information.

```
Properties fieldProperties = (Properties)
    context.getCachedObject("FieldProperties");
Parameters data = (Parameters)
    context.getCachedObject("FileParameters");
Map localData = (Map) context.getCachedObject("LocalProperties");
String algorithm = (String) context.getCachedObject("AlgorithmName");
```

The FileSystemFileStoreAlgorithmFilters table is part of File Store Provider and requires a component along with Java code to modify.

Caution:

The defaults provided in the FileSystemFileStoreAlgorithmFilters table should work for most scenarios. This resource file should not be edited directly. Proper modification should be done with Java code and through additional component development. For more information on component development, see Getting Started with Content Server Components in *Developing with Oracle WebCenter Content*.

12.3.3.6 FileStorage Table

The FileStorage table is added to Content Server when File Store Provider is installed. It is used exclusively by the JdbcStorage storage type, when content is stored in a database. The

FileStorage table contains the renditions of content items and uses the dID of the content item and rendition to uniquely identify what renditions belong to which content item.

12.3.3.7 FileCache Table

The FileCache table is added to Content Server when File Store Provider is installed. It is used exclusively by the JdbcStorage storage type to remember which renditions have been placed on a file system. Renditions stored in a database are placed on a file system when required for a specific event, for example indexing or conversion. These files are often temporary and deleted after a specified interval as part of a scheduled event.

12.3.4 Working with the File Store Provider

When the File Store Provider default file store is upgraded, checked-in content and associated metadata are examined and assigned a storage rule based on criteria established by the system administrator. Criteria can include metadata, profiles, or other considerations. The storage rule determines how vault and web files are stored and accessed by Content Server and how they are accessed by a web server. Files can be stored in a database or placed on one or more file systems or storage media. Partitions can be created to help manage storage location, but are not required.

Caution:

The FileStoreProvider component should not be disabled once it has been used with Content Server.

This section covers these topics:

- [Adding or Editing a Partition](#)
- [Editing the File Store Provider](#)
- [Adding or Editing a Storage Rule](#)

12.3.4.1 Adding or Editing a Partition

You can create partitions to define additional root paths to files managed by Content Server but requiring storage in different locations or on different types of media. You create partitions using the Partition Listing page. When a new partition is created, Content Server modifies the PartitionList resource table in the `fsconfig.hda` file, located in the `IntradocDir/data/filestore/config/` directory.

Note:

Oracle WebLogic Server does not support configuring its web server for the Content Server instance to add a new virtual directory and alias to point to the weblayout directory for each partition that is created. Partitions can be used for the vault files, and partitions are supported for web files.

To add a partition to the Content Server instance:

1. Log in to the Content Server instance as system administrator.
2. Choose **Administration**, then **File Store Administration**.
3. If there are no partitions defined, click **Add Partition**. Otherwise, the Add/Edit Partition page opens.
4. Enter a partition name. The name must be unique.
5. Modify the partition root, duplication methods, and any other pertinent parameters.
6. Ensure that **Is Active** is enabled.
7. Click **Update**.

12.3.4.2 Editing the File Store Provider

You can edit File Store Provider at any time. To edit the provider:

1. Log in to the Content Server instance as system administrator.
2. Choose **Administration**, then **Providers**.
3. In the Providers page, click **Info** in the Action column next to the DefaultFileStore provider.
4. In the File Store Provider Information page, click **Edit**.
5. In the Edit File Store Provider page, make the necessary modifications and click **Update** to submit the changes.

 **Note:**

Do not navigate away from the Edit File Store page before clicking **Update** to submit the change.

6. Restart the Content Server instance.

12.3.4.3 Adding or Editing a Storage Rule

You can add multiple storage rules to the file store.

 **Important:**

Storage rules cannot be deleted. Carefully consider each storage rule before you create it.

 **Caution:**

Changing a storage rule after content has been checked in to the Content Server repository may cause Content Server to lose track of the content.

To add or edit storage rules:

1. Log in to the Content Server instance as a system administrator.

2. Choose **Administration**, then **Providers**.
3. In the Providers page, click **Info** in the Action column next to the DefaultFileStore provider.
4. In the File Store Provider Information page, click **Edit**.
5. In the Edit File Store Provider page, click **Add new rule**, or select the name of the rule to edit from the Storage choice list, and click **Edit rule**.
6. In the Storage Rule Name dialog, make the necessary modifications to the storage rule, and click **OK**.

 **Note:**

If there are records associated with the storage rule being edited, then the following rules cannot be modified: `FsWeblayoutDir` (the weblayout directory) and `FsHttpWebRoot` (the `HttpWebRoot` and URL prefix).

7. In the Edit File Store Provider page, click **Update**.

 **Important:**

If the web root used in the web URL file path defined in the storage rule is something other than the default weblayout directory defined for Content Server, you must add an alias or virtual directory in your web server for the web root used in the storage rule. Otherwise, Content Server does not know where to access the file. For information on adding virtual directories to your web server, see the documentation that came with your web server.

12.4 Sample Implementations of File Store Provider

This section lists the contents of the tables contained in the provider definition file (`provider.hda`) for each of the examples. The `provider.hda` file does not need to be edited manually. Proper modification of the `provider.hda` file should be done within the Content Server interface using the Add/Edit Partition page, or through additional component development. The provided default options for other resource tables, such as [PathMetaData Table](#), [PathConstruction Table](#), and [FileSystemFileStoreAlgorithmFilters Table](#), should have sufficient flexibility for most scenarios.

This section covers these topics:

- [Example PathMetaData Table Options](#)
- [Configuration for Standard File Paths](#)
- [Configuration for a Webless or Optional Web Store](#)
- [Configuration for Database Storage](#)
- [Configuration for OCI Object Storage](#)
- [Configuration for OCI Object Storage Cache](#)
- [Managing Object Storage Migration](#)
- [Altered Path Construction and Algorithms](#)

12.4.1 Example PathMetaData Table Options

In most of the examples, the following [PathMetaData Table](#) configuration definitions are used. The table has been trimmed of some of its columns not pertinent to the examples for clarity.

```
@ResultSet PathMetaData
6
FieldName
GenerationAlgorithm
RequiredForStorage
    <trimmed columns>
dID
#all
dDocName
#all
dDocAccount
documentAccount
dDocType
#all
dExtension
#all
dWebExtension
weblink
dSecurityGroup
#all
dRevisionID
#all
dReleaseState
#all
dStatus
web
xPartitionId
partitionSelection
ExtensionSeparator
extensionSeparator
xWebFlag
RenditionId
#all
RevisionLabel
revisionLabel
RenditionSpecifier
renditionSpecifier
@end
```

12.4.2 Configuration for Standard File Paths

File Store Provider can be configured to place content on a file system in the standard Content Server locations.

12.4.2.1 Defining the Storage Rule

The first step is to define the storage rule. In this case, the storage rule will be of type `FileStorage`, because all content is to be stored on the file system.

Example:

```
@ResultSet StorageRules
4
StorageRule
```

```

StorageType
IsWeblessStore
RenditionsOnFileSystem
default
FileStorage
@end@

```

12.4.2.2 Defining the Path Construction

The second step is to define the path construction for each of the storage classes for the rule. In general, the last part of the path should be standard for all usage examples. If not, then Content Server does not work well with `hcs*` files. However, the root path can be changed without affecting functionality, assuming that changing the web URL file path root is properly acknowledged by the web server as a Content Server web root.

In this configuration, the vault, web, and web URL storage classes need to be defined in the [PathConstruction Table](#). The path expression for the vault has already been discussed in [Understanding Path Construction and URL Parsing](#). `$dispersion$` implements dispersion of content on the file system. The caller can provide this dispersion on the storage rule page.

This setup only looks at the web path expression, which differs from the web URL only in its root. In other words, the web path is an absolute path on the file system, while the web URL is a URL served up by a web server.

Example:

```

@ResultSet PathConstruction
4
FileStore
PathExpression
AutoCreateLimit
IsWritable
StorageRule
vault
$#env.VaultDir$$dDocType$/$dDocAccount$/$dispersion$/$dID$$ExtensionSeparator$
    $dExtension$
6
true
default
weburl
$FsHttpWebRoot$groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/
    $dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$
    $ExtensionSeparator$$dWebExtension$
3
false
default
web
$FsWeblayoutDir$groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/
    $dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$
    $ExtensionSeparator$$dWebExtension$
3
true
default
@end

```

- The web path construction is defined to be:

```

$FsWeblayoutDir$groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/
$dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$
$ExtensionSeparator$$dWebExtension$

```

- This is parsed into its parts as described in the following table:

Path Segment	Description
\$FsWeblayoutDir\$	Variable for the web-viewable path for the weblayout directory.
\$FsHttpWebRoot\$	Alternate Idoc Script variable for web URL.
/groups/	String.
\$dSecurityGroup\$	Used by the PathMetaData table. This is a required field and must consequently be provided by the caller or descriptor creator. It is part of a content item's metadata information.
\$dDocAccount\$	This is mapped to a documentAccount algorithm which takes dDocAccount and parses it into the standard Content Server account presentation with all the appropriate delimiters.
/documents/	String.
\$dDocType\$	Used by the PathMetaData table. This is a required field and must consequently be provided by the caller or descriptor creator. It is part of a content item's metadata information.
\$dispersion\$	Implements dispersion of content on the file system.
ledisp	Indicates that dispersion has ended at the point where this marker is placed. Even if dispersion is empty there will be an ~edisp marker.
\$dDocName\$	Used by the PathMetaData table. This is a required field and must consequently be provided by the caller or descriptor creator. It is part of a content item's metadata information.
\$RenditionSpecifier\$	This is provided by the renditionSpecifier, which is only of interest if the system is creating additional renditions such as thumbnails. Otherwise, this returns an empty string.
\$RevisionLabel\$	The revision label is provided by the revisionLabel algorithm which, depending on the status of the content item, adds a '~dRevLabel' to the path.
\$ExtensionSeparator\$	The extensionSeparator algorithm is used here and by default it returns '.'.
\$dWebExtension\$	The dWebExtension is a required field for the web and web URL storage classes and is passed in through the file parameters.

12.4.3 Configuration for a Webless or Optional Web Store

In this example, the previous example storage rule is configured to have `IsWeblessStore` set to true and consequently the web-viewable file will not be created by default. However, if the document is processed through Inbound Refinery or WebForms or any other component that requires a web-viewable, the web file will be created. The location of the files is as above in the standard configuration. However, because a file might not have a web rendition, the web URL path must be adjusted. Also, note the use of `weburl.file`. This is used to compute the URL when the web-viewable actually exists. The metadata field `xWebFlag` is used to determine how the file is to be served up in the browser.

12.4.3.1 Defining the Storage Rule Example

```
@ResultSet StorageRules
4
StorageRule
StorageType
IsWeblessStore
RenditionsOnFileSystem
default
```

```

FileStorage
true
@end@

```

12.4.3.2 Defining the Path Construction Example

```

@ResultSet PathConstruction
4
FileStore
PathExpression
AutoCreateLimit
IsWritable
vault
$#env.VaultDir$$dDocType$/$dDocAccount$/$dispersion$/$dID$$ExtensionSeparator$
    $dExtension$
6
true
default
weblink
$HttpCgiPath$?IdcService=GET_FILE&dID=$dRevClassID$
    &dDocName=$dDocName$&allowInterrupt=1&noSaveAs=1&fileName=$dOriginalName$
3
false
default
weblink.file
$FsHttpWebRoot$groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/
    $dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$
    $ExtensionSeparator$$dWebExtension$
3
false
default
web
$FsWebLayoutDir$groups/$dSecurityGroup$/$dDocAccount$/documents/$dDocType$/
    $dispersion$/~edisp/$dDocName$$RenditionSpecifier$$RevisionLabel$
    $ExtensionSeparator$$dWebExtension$
3
true
default
@end

```

12.4.4 Configuration for Database Storage

To store files in the database, you need a storage rule that is of type `JdbcStorage`. By default, all content items belonging to this rule have their files stored in the database. However, even though the files are stored in the database, there is the presumption of an underlying file system and the system may need to temporarily cache a file on the file system. In particular, this may happen for indexing or for some conversions.

Note:

A rule can be configured to always store renditions belonging to a given storage class on the file system. This is most useful for systems that store vault files in the database, but web files on the file system.

12.4.5 Configuration for OCI Object Storage

Earlier, WebCenter Content supported two document storage options: local file system or database. Now, a new storage provider component is installed in WebCenter Content that is object storage to store documents and this has removed the block storage limitations.

To store content to OCI object storage:

1. Change storage rule to OCI object storage (as default storage option)
2. Configure Oracle Cloud Infrastructure (OCI)
3. Configure object storage

Change Storage Rule to OCI Object Storage (as default storage option)

The OCI object storage is the new storage option for WebCenter Content. The component is installed by default, but not enabled. WebCenter Content can store and retrieve documents from object storage on cloud.

To enable the OCI object storage as default rule in the system:

1. Log in to the Content Server instance as a system administrator.
2. OCI object storage Component is a system component disabled by default. Choose **Administration**, then **Admin Server**, and then **Component Manager**.
3. On the Component Manager page, click the **advance component manager** link.
4. On the Advanced Component Manager page, select the **Show Systems Components** check box and also, the **OCIObjectStorage** option from the list of **Enabled Components**. Click **Enable** and then restart the Content Server.
5. Choose **Administration**, and then **Desktop Client Apps**.
On the Administration Apps page, download and launch the client. When you launch the client, it shows a link *Open Oracle WebCenter Content Administration.exe*.
6. On the WebCenter Administration page, select **Configuration Manager**.
7. On the Configuration Manager page, select the **StorageRule** name and then edit it.
8. On the Edit Metadata 'StorageRule' page, select the default value as **OCIObjectStorageRule**. You can set the default value as **OCIObjectStorageRule** for the **xStorageRule** metadata field without creating a schema rule.

Note:

You can create a content profile with `xStorageRule` as one of the metadata to be modified and that the storage rule that is to be chosen in the content profile is `OCIObjectStorageRule`. See *Managing Content Profiles*. You can associate storage rules to content based on doc type. For example, `dDocType A` to use storage rule A and `dDocType B` to use storage rule B etc. So, for example, you could have a rule or profile that would populate the storage rule metadata field based off of the document type.

9. Restart the Content Server.

Configure Oracle Cloud Infrastructure (OCI)

To configure an OCI for your project, log in to the OCI console as a system administrator. Create a compartment, bucket, OCID, and tenancy. Also, create an API private or public key pair. For details, see [API signing key](#) and [Understanding Compartments](#).

Configure Object Storage

You need to configure few parameters of object storage in WebCenter Content for a successful connection with Bucket and for a file to reside in cloud.

To configure object storage:

1. Log in to the Content Server instance as a system administrator.
2. Choose **Administration**, then **Object Storage**, and then **Object Storage Configuration**.
3. In the Configure Object Storage page, enter the values for the following fields:

Note:

It is important to note that each Content Server should use its own storage bucket.

These are the minimum configurations that are required to establish the connection between WebCenter Content and Oracle Cloud Infrastructure. When you check-in any document in WebCenter Content, it will be stored in cloud object storage.

12.4.6 Configuration for OCI Object Storage Cache

In some situations, content stored in an OCI bucket may have to be forced onto a file system. One example would be when Oracle WebCenter Content: Inbound Refinery must have access to a file for conversion. Files forced onto a file system are considered temporary cache. The following configuration values are used to control when the temporarily cached files are to be cleaned up. Note that the system only cleans up files that have an entry in the OCIFileCache table.

Variable	Description
OCICacheThreshold	Specifies the maximum cache size, in megabytes. The default is 100. When the threshold is met, the Content Server instance starts deleting files that are older than the minimum age, as specified by the OCIMinimumFileCacheAge parameter.
OCICleanUpCacheDuringIndexing	Specifies if the cache will be cleaned during the indexing cycle. The default is <code>false</code> .
OCIMaximumFileCacheAge	Specifies the maximum age at which files are cached, expressed in days. The default is 30 days.
OCIMinimumFileCacheAge	Specifies the minimum age at which cached files can be deleted, expressed in days. The default is 1 day. This parameter is used in conjunction with the OCICacheThreshold parameter to determine when to delete cached files.

12.4.7 Managing Object Storage Migration

The object storage migration tool migrates the content from the WebCenter Content On-premise system to buckets in an OCI object storage compartment. The migration can be done online or offline. The offline migration is done using media devices being physically transported to the destinations, while an online migration is a direct file transfer into the object storage. During the migration, the copies of a file will be maintained in the WebCenter Content On-premise system as well as in OCI object storage. Once it is verified that the migration is done successfully, then files will be cleaned up from the WebCenter Content On-premise system. This feature will benefit the users who are dealing with billions of files and terabytes of data.

This section contains the following topics:

- [Configuration Parameters](#)
- [Accessing Object Storage Migration Tool](#)
- [Viewing Migration Progress](#)
- [Previewing Migration](#)
- [Retrying Failures](#)
- [Configuring Media Drive Location](#)

12.4.7.1 Configuration Parameters

Since this migration tool is expected to migrate billions of files and terabytes of data, it is designed as a multi-threaded application that can run across multiple nodes.

The number of threads that each node can have is set at 2 by default and is configurable using the `OciMigrationWorkerThreadsPerNode` parameter. This can take a maximum value of 10. If any higher value is provided, 10 will only be considered.

There is a thread running on each node that checks for a new job. When one node starts the migration job, in 15 seconds, the other node is ready for the job. For time duration, you can configure the `OciMigrationCheckInterval` parameter.

And each of these threads by default process 500 documents. Only 500 documents are picked up at one time by a thread and the thread completes the necessary operations on these 500

documents before moving on to the next 500 documents. You can set the value for each thread by configuring the `OciMigrationBatchSizePerWorkerThread` parameter.

The default value of the parameter `OCIMigrationFreeDocumentsWaitInterval` is 120 minutes and it is optional. This setting is specific to documents that are in the processing state. For instance, if the migration is running and the server shuts down, some of the documents currently being worked on by the threads will remain in the processing state and will not be picked up by the threads on startup. These documents that are in the processing state will be released after the configured time of 120 minutes and will be available for the threads to pick up. The `OCIMigrationFreeDocumentsWaitInterval` parameter is set to 120 minutes to allow enough time for documents that are being processed and can be released after the configured time.

12.4.7.2 Accessing Object Storage Migration Tool

The object storage migration tool can be accessed from the Administration menu in the Content Server user interface.

To access the object storage migration tool:

1. Log in to the Content Server instance as a system administrator.
2. Choose **Administration**, then **Object Storage**, and then **OCI Migration Admin Control**. The Migration Job Status tab is displayed by default.
3. On the Migration Job Status tab, view the status of the number of documents that are migrated. To start a new job, click the **Create a new Migration Job** link.
4. On the New Migration Job tab, select **Saved Search** and **Migration Mode** from the drop-down menu. You will get the total number of documents that are searched and will be selected for migration when you select the specific **Saved Search** option. The documents that are already migrated will not be picked up for migration again.
This migration tool works with the My Saved Queries feature of the Content Server. It is created using the Search Builder form. For details, see My Content Server in the *Using Oracle WebCenter Content* guide.

Also, you can determine how many Saved Searches will be displayed in the Content Server by configuring a parameter `MaxSavedSearchResults`. See [MaxSavedSearchResults](#) in the *Configuration Reference for Oracle WebCenter Content* guide.

Note:

Full-text search is not supported by the object storage migration tool.

The two modes of the migration are **Direct Transfer** and **Copy To Drive**. The **Direct Transfer** mode will copy the existing documents directly from the On-premise instance to the buckets present in OCI. The **Copy To Drive** mode will copy the documents to a physical drive. This drive will be shipped physically to the destination to copy the files to the buckets in OCI.

5. Click **Start Migration**.

12.4.7.3 Viewing Migration Progress

Once the migration job is started, the Migration Job Status page is displayed. It displays the start time and end time of the three steps of a job that is Migration, Verification, and Cleaning.

- **Migration** - It is the actual migration or copy of the document from the native storage to OCI or drive. After the migration, if the document is requested from the Content Server, it is fetched from the original storage.
- **Verification** – It is the verification of the signature of the document and checking whether the document has correctly migrated to OCI. After this step, if the document is requested from the Content Server, it is fetched from the OCI storage.
- **Cleaning** – It is the cleanup of the documents from the native storage. After this step, the document will not be present in the original storage. Cleanup is written as a manual process that has to be executed by the administrator who scheduled the migration. Once each of the copies in object storage is verified to match the original in WebCenter Content to ensure that there is no data loss of any kind. After the administrator is satisfied that the migration has been completed successfully, the migration utility also provides a clean-up capability to remove the WebCenter Content copies freeing up local storage space. Therefore, one can control and schedule the clean-up activity as an administrator.

In case of **Direct Transfer** mode, the migration and verification steps are carried out one after the other automatically. In case of **Copy To Drive** mode, verification is a manual process that is to be done only after the drive is physically transported to the destination and the files are copied to the destination bucket.

In addition to the **Verify** and **Cleanup** options, the Migration Status page displays the relevant actions that can be performed on a job are: **Pause**, **Resume**, **Truncate**, and **Abort**. If you want to stop the migration temporarily, you can **Pause** the operation and when you want to restart it, then **Resume** the operation.

When a job is running and 10000 documents are being migrated, but failures are piling up, you can use the **Truncate** operation. The truncate operation will stop the process at the current point and no further documents will be picked up for the operation. The documents for which the threads have already picked up will be honored, but new documents will not be picked up.

In the case of the **Abort** operation, it will stop the process at the current point, but this will also roll back. The documents that have already been migrated to OCI and even verified will be rolled back. This will give you an option to start from fresh, in case you have made some configuration mistake initially. You can start a new job afresh.

The Migration Status page also displays a link to the failures that the job has encountered. The link would redirect you to the Retry Failures page where you can retry them.

12.4.7.4 Previewing Migration

The preview migration is a manual process to preview the migration of a single document. A document goes through all the three steps of migration, verification, and cleanup.

On the Preview Migration tab, enter the **Document ID** and select the **Migration Mode** from the drop-down menu and then click **Get Actions**. It shows the actual migration, verification, and cleanup of a document.

The documents that are migrated using preview will not be available for verification in regular migration.

Alternatively, you can create a Saved Search based on some criteria and the search result will appear accordingly. This search can be used for migration and a job can be started. Once this job ends successfully, the Saved Search conditions or parameters can be changed and hence the number of documents returned in the search will be more. A new migration job with this changed Saved Search can be started.

12.4.7.5 Retrying Failures

The Retry Failures attempts to retry the failures encountered for a particular job. It lists all the failures for a job.

The failures can be at any stage of a job that is migration, verification, or cleanup. You can retry a single failed document or you can retry all the failures. Retry all would attempt to work on all the failures for the job.

If you want to see at which stage a document is failed, enter the job name on the Retry Failures page and then click **Submit**. It will show the list of documents failed with their document IDs, time, reason for the failures, and the stage at which the failure occurred.

12.4.7.6 Configuring Media Drive Location

This is the page where the drive location is configured. You need to configure only if you are using media drive for migrating existing documents into OCI. You can specify the drive location and then click **Update**. To reset the drive location, click **Reset**.

12.4.8 Altered Path Construction and Algorithms

The previous examples have kept the file paths consistent with the standard configuration. For very large implementations, this can result in directory saturation and slow performance. The following examples aid in dispersing files over several storage options.

12.4.8.1 Using Partitioning

File Store Provider makes it easy to use partitions to create a sparser directory structure. By default, the `xPartitionId` metadata field is used and becomes a part of a content item revision's metadata information. It is recommended that this field is disabled on the Content Server interface, instead letting the partition selection algorithm determine the partition to use. The partition selection algorithm looks at all the active partitions, and as a new content enters the system, the partitions are selected in order. Each partition has an entry in the [PartitionList Table](#) and can be declared active. The `PartitionRoot` is calculated from `xPartitionId`, where the value is a look up key into the `PartitionList` table. If no `xPartitionId` is specified, the system finds the next available and active partition and uses this value for the location calculation. The `xPartitionId` is then stored as part of the content item's metadata.

To use the partition selection, define the vault storage class in the `PathConstruction` table as follows:

```
vault
$PartitionRoot$/$dDocType$/$dDocAccount$/$dRevClassID$$ExtensionSeparator$$dExtension$
6
true
```

Partitions can be deactivated using the `Add/Edit Partition` page at any time if a system administrator needs to close a partition to contribution, for example if maintenance is required on the storage device.

12.4.8.2 Adding a Partition to the Weblayout Path

This example shows how to partition both vault and weblayout directories, and also maintain valid web URL file paths.

Add the partition root to the web-viewable path and web URL file path, and edit the variables `$FsWeblayoutDir$` and `$FsHttpWebRoot$` on the Storage Rule Name dialog.

`$FsWeblayoutDir$` represents `$PartitionRoot$/weblayout`. `$FsHttpWebRoot$` represents `$HttpWebRoot$/${xPartitionId}/weblayout/`.

Define `partitionRoot` in the Add/Edit Partition page as follows:

Partition Name	Partition Root
partition1	<code>#{env.WeblayoutDir}/partition1/</code>
partition2	<code>#{env.WeblayoutDir}/partition2/</code>

In order to keep the web URL file path consistent with the web-viewable path in the weblayout directory, the variable `xPartitionId` is used so that `partition1` or `partition2` is correctly replaced when creating the web URL file path.

Ensure that the web-viewable path and the web URL file path evaluate into the same path.

- `$FsWeblayoutDir$` represents `$PartitionRoot$/weblayout/`. For `partition1` this evaluates to `#{env.WeblayoutDir}/partition1/weblayout/`. For `partition2` this evaluates to `#{env.WeblayoutDir}/partition2/weblayout/`.
- `$FsHttpWebRoot$` represents `$HttpWebRoot$/${xPartitionId}/weblayout/`. For `partition1` this evaluates to `$HttpWebRoot$/partition1/weblayout/`. For `partition2` this evaluates to `$HttpWebRoot$/partition2/weblayout/`.

If you set up the partitions (`partition1` and `partition2`) to use the partition root of `#{env.VaultDir}/partition1` and `#{env.VaultDir}/partition2` instead of the `#{env.WeblayoutDir}` and `$HttpWebRoot$` settings, then the weblayout file will end up stored in the vault directory. It then can be used only for partitioning the vault files.

12.4.8.3 Limiting the Number Files in a Directory

Another way of dispersing files is to alter the path so that files get partitioned out by the `dRevClassID` of the content item. In the example below, the directories are limited to 10,000 files plus extra files for additional renditions.

If your path expression

contains `$RevClassID[-12:-10:0]/$dRevClassID[-10:-8:0]/$dRevClassID[-8:-4:0]$` and `$dRevClassID` is 1234567890, the result is 00/12/3456.

Note the `$dRevClassID[-12:-10:0]` in the path expression. This is interpreted as follows:

- Get the characters starting at 12 back from the end of the string until you get the character 10 back from the end of the string.
- Pad the resulting string to length 2, which 12-10, with 0 characters.

12.5 Using Sun Storage Archive Manager

This section introduces the Sun Storage Archive Manager (SAM-QFS) product and explains how to configure Content Server to work with SAM-QFS.

- [About SAM-QFS](#)
- [Considerations for Using SAM-QFS](#)
- [Installing SAM-QFS](#)

- [Configuring Content Server and SAM-QFS with WORM](#)

12.5.1 About SAM-QFS

The Sun Storage Archive Manager (SAM-QFS) is a hierarchical file storage system that runs on the Oracle Solaris operating system. When configured with the WORM (Write Once Read Many) option, it supports archiving file system data so that it can be only read by users. The SAM-QFS environment includes a storage and archive manager along with Sun QFS file system software. SAM-QFS can be used with a NFS mount by the Content Server machine and additional Content Server configuration.

SAM-QFS comprises two products:

- **Quick File System (QFS)** is a kernel-level file system that can be installed on Oracle Solaris and SPARC platforms. This product provides the WORM feature and retention manager feature, which can be used with Content Server.

 **Note:**

Weblayout cannot be stored using WORM.

- **Storage Archive Manager (SAM)** includes several programs that run in user space to archive files initially filed in QFS, retrieve files on demand, and manage the archive by freeing space and so on.
 - The **Archiver** program is proactively notified when files change so that they are archived in an event-driven fashion and not by polling the file system. It also manages the archive and creates backup copies as needed.
 - The **Releaser** program releases the content from primary storage after it validates that all copies have been made by the archiver.
 - The **Stager** program loads data or stages data to primary storage from an archive copy (which can be on an archive disk or an archive tape) so that the data can be retrieved by users from QFS. This activity can be configured to be done on demand or according to policy.
 - The **Recycler** program purges deleted files from secondary storage so that the space can be reclaimed and reused.

Files are stored in the TAR utility format so that the file system metadata is retained along with the actual file. Multiple files can be stored in the same TAR for efficiency.

12.5.2 Considerations for Using SAM-QFS

Consider the following before implementing SAM-QFS:

- SAM-QFS provides WORM (Write Once Read Many) capability, along with the ability to specify a retention period after which the WORM constraints are lifted.
- Files can be automatically archived to tape. SAM-QFS provides an integrated, seamless, backup solution with a transparent restore.
- If recycling of files on archive is scheduled with SAM-QFS, then revisions of documents can be retrieved by maintaining the metadata backup snapshots and mounting them as needed.
- Content items cannot be deleted. A delete action will fail and generate an error message.

- Content checked in using a WORM enabled storage rule will not be able to be edited in a workflow step if that step uses the option of "User can edit (replace) the current revision". When a workflow step uses this option, the vault rendition of the file is replaced, which is not possible with a read-only file system.
- The native file path depends on the storage rule vault path field. If the native file path value contains a metadata field as part of its path, the metadata field cannot be updated, because the update action will try to change the file system path (which is not possible in a read-only system). Trying to change the metadata attribute will fail and generate an error message. The recommended settings for a WORM-enabled storage rule is to not have any metadata field in the native file path if the path might be changed in the future.

12.5.3 Installing SAM-QFS

For information on how to install SAM-QFS on an Oracle Solaris system and enable WORM, see the Sun QFS and Sun Storage Archive Manager (SAM-QFS) wiki at <https://wikis.oracle.com/display/SAMQFS/Home>. The `SUNWsamfswm` package does not come with SAM-QFS 5.2 download version, so please contact the SAM-QFS group for this package.

12.5.4 Configuring Content Server and SAM-QFS with WORM

To work with SAM-QFS, certain configurations must be set. To enable WORM for the default storage rule, the default rule (`DispByContentId`) in the Content Server File Store Provider must be modified. Other storage rules also can be modified to enable WORM, if needed.

12.5.4.1 Configuring the Vault Path

To configure the vault path:

1. In the Content Server instance, choose **Administration**, then **Admin Server**, then **General Configuration**.
2. In the Additional Configuration Variables field, enter the environment variable `IsVaultFileSystemWorm=true`
3. Edit the `DomainHome/ucm/cs/bin/intradoc.cfg` file to set the `VaultDir` parameter to the vault file path for the SAM-QFS location.
4. Starting at the SAM-QFS mount point, apply `chmod -R 4000 directoryName` to the subdirectories *except* for the `vault/~temp` directory. The `vault/~temp` directory must never be WORM enabled.

Work from the top-most level down. The WORM trigger can be applied only if the parent directory has the WORM trigger enabled.

5. Edit the Solaris `/etc/vfstab` file to specify the default retention period.

12.5.4.2 Configuring the File Store Provider to Enable WORM

To configure the File Store Provider to Enable WORM for vault files:

1. In the Content Server instance, choose **Administration**, then **Providers**.
2. From the `DefaultFileStore` row in the list of providers, click **Info** in the Action column.
3. On the File Store Provider Information page, click **Edit**.
4. On the File Store Provider page, in the line for Storage Rules, click **Edit Rule**.
5. On the Storage Rule Name page, ensure that **File system only** is selected.

6. Check **Allow WORM/Retention (SAM-QFS only)**.
7. If a retention period needs to be set, check **Set default retention period for vault files** and enter the number of years and months for retention.

This option has a limitation up to 2038 if either of these two conditions are true: the SAM-QFS file system is 32-bit, or the operating system where Content Server is running is 32-bit. If a greater retention period is needed, use the SAM-QFS `mount` option parameter to set the default retention period instead of checking this Content Server option.

13

Configuring Providers

This chapter describes Oracle WebCenter Content supported providers and explains when and how to use provider connections between WebCenter Content Server and Oracle WebLogic Server or other providers such as Lightweight Directory Access Protocol (LDAP). This chapter includes the following topics:

- [About Content Server Providers](#)
- [Choosing an Appropriate Provider](#)
- [Understanding Content Server Security Providers](#)
- [Managing Providers](#)

13.1 About Content Server Providers

A provider is an Application Programming Interface (API) that establishes a connection between the Content Server instance and outside entities. These entities include:

- Oracle WebLogic Server
- LDAP servers
- databases
- server sockets
- file store system
- Inbound Refinery

By default, the Content Server instance has three system providers:

- **SystemDatabase:** The system database.
- **SystemServerSocket:** A server socket that listens for browser requests.
- **DefaultFileStore:** A file store system.

In addition, you can create the following types of providers:

- **Outgoing:** A connection initiated to an outside entity. You can use this type to communicate between Content Server instances. For information on using SSL with an outgoing provider, see [Understanding Content Server Security Providers](#).
- **Incoming:** A connection initiated from an outside entity like a browser or client application. The provider listens on a specified port to be aware of incoming connections. For information on using SSL with an incoming provider, see [Understanding Content Server Security Providers](#).
- **Database:** An information repository server that provides an API for connecting and communicating with it. This retrieves information and enables information to be changed in the database. Examples of this type are system databases.
- **Preview:** An outgoing provider connection for use with the optional HTML Preview feature.
- **JpsUser:** A connection to an Oracle WebLogic Server instance. This provider uses Java Platform Security (JPS) to perform user authentication, user authorization, and retrieval of

user metadata through an Oracle WebLogic Server instance. This type of provider is supported by the JpsUserProvider component, which is installed (enabled) by default with the Content Server instance.

- **Ldapuser:** A connection initiated to a Lightweight Directory Access Protocol (LDAP) server for managing external user access to the Content Server instance. This type of provider is supported by the ActiveDirectoryLdap component, which is installed (disabled) by default during installation.

 **Note:**

As of 11g Release 1 (11.1.1) Ldapuser functionality is superseded by JpsUser, in particular for nested group support.

- **HTTP:** A connection that allows communication between Content Server instances using the HTTP protocol. This type of provider is supported by the ProxyConnections component, which is installed (enabled) by default during Content Server installation. For information on when and how to use this type of connection, see [Managing Additional Content Server Security Connections](#).

13.2 Choosing an Appropriate Provider

The different types of providers described in the previous section are used under specific circumstances to work with various other Oracle products or utilities. The following subsections describe those conditions and the particular provider types that must be used in each scenario.

- [When to Use an Outgoing Provider](#)
- [When to Use a Database Provider](#)
- [When to Use an Incoming Provider](#)
- [When to Use a Preview Provider](#)
- [When to Use a JpsUser Provider](#)
- [When to Use a Ldapuser Provider](#)

13.2.1 When to Use an Outgoing Provider

Outgoing providers are necessary to use the Content Server Archiver utility and Oracle WebCenter Content: Inbound Refinery. If you want to use SSL or keepalive with an outgoing provider, see details in [Understanding Content Server Security Providers](#).

- **Archiver Utility (Content Server):** The Archiver is a utility within the core Content Server that enables system administrators to copy and remove content and store it for future use. Users can query a set of content from the Content Server instance and export it to an *archive*. Archives can then be imported to other Content Server instances or can be imported back to the same instance with changed metadata fields.

An outgoing provider is required to use the Archiver Transfer feature, which is used to archive content across a firewall or between two systems that do not share a file system. For more information about the Transfer feature, the different types of transfers and the outgoing provider requirements, see [Understanding System Migration and Archiving](#).

- **Inbound Refinery:** The Inbound Refinery server processes content checked in to Content Server and converts it to specified formats. An outgoing connection to the Inbound

Refinery server is necessary for communication with Content Server. See Inbound Refinery in *Managing Oracle WebCenter Content*

13.2.2 When to Use a Database Provider

Database providers are necessary to use external databases. Frequently, it is desirable or necessary to perform database queries on databases that are not the default Content Server database. In this case, customized database providers can be created that make it possible to access any data from any application, regardless of which database management system is handling the data. Using customized database providers to integrate external databases into Content Server, search results can be combined and viewed on a single search page. Additionally, data can be imported from these external database sources.

Administrators can create a database provider with one of two methods:

- Use the Oracle WebLogic Server Administration Console to create an Oracle WebLogic Server data source to the database, then configure a Content Server database provider to use that data source. For information on creating a JDBC data source for a WebLogic domain server, see *Developing Fusion Web Applications with Oracle Application Development Framework*.
- Create a Content Server database provider to connect directly to the database through a JDBC connection, without using an Oracle WebLogic Server data source. This mode is provided for instances with pre-existing connections in their configurations.

13.2.3 When to Use an Incoming Provider

Incoming providers are necessary to use WebDAV support and the Content Server Archiver utility. If you want to use SSL or keepalive with an incoming provider, see details in [Understanding Content Server Security Providers](#).

- **Archiver Utility (Content Server):** The Archiver is a utility within Content Server that enables system administrators to copy and remove content and store it for future use. Users can query a set of content from the Content Server instance and export, import, or replicate to another instance, or change metadata fields. Tasks most frequently performed involve transfer, backup, and reorganization of information within the system.

Generally, when data or content items are moved from one repository to another, the Archiver utility uses a push technology to relocate the files. However, occasionally your system might require that the files be pulled rather than pushed. In this case, an incoming provider must be created.

- **Oracle WebDAV Support:** With Content Server version 7.0 and later, Web-Based Distributed Authoring and Versioning (WebDAV) support is provided by a custom feature, so an incoming provider and servlet engine are not necessary.

See Managing WebDav in *Managing Oracle WebCenter Content*.

13.2.4 When to Use a Preview Provider

Preview providers are necessary to use HTML Preview and Content Categorizer.

- **HTML Preview:** HTML Preview is a feature that provides users with instant feedback on how their content will display on the published website. This feature enables users to modify the original content before it is actually checked in. HTML Preview also helps users ensure that correct metadata has been assigned to the content. During the installation process, a preview provider must be created. For additional overview and installation information about HTML Preview, see *Managing Oracle WebCenter Content*.

- **Content Categorizer:** Content Categorizer suggests metadata values for documents being checked in to Content Server or for existing documents that need to have metadata reapplied. For Content Categorizer to recognize structural properties of a document, the file must be converted to XML.

For more information about Content Categorizer, see *Managing Oracle WebCenter Content*. This guide provides relevant information about any additional products that may be required or are optional.

13.2.5 When to Use a JpsUser Provider

JpsUser is the default provider for the WebCenter Content Server instance to communicate user information and credentials managed through the Oracle WebLogic Server Administration Console. For Oracle WebCenter Content and Content Server instances, it is recommended that you use the JpsUser provider.

Note:

As of Release 11gR1, direct LDAP provider functionality is superseded by the JpsUser provider for a Content Server instance, in particular for cases such as nested group support.

Note:

If a site is upgrading from an 10g or earlier release of WebCenter Content software and is using Active Directory, LDAP, or Active Directory with LDAP, information about those providers is available in the Release 10gR3 document *Managing Security and User Access*. It is strongly recommended that sites upgrade to use JpsUser provider.

The system-defined JpsUser provider connects to the Content Server instance and supports the Oracle WebLogic Server authentication mechanism (Basic, Form, Single Sign-On, WNA, and so forth). Java Platform Security (JPS) provides a uniform interface for authenticating and authorizing users from Oracle WebCenter applications regardless of the back-end user storage (XML, LDAP, database, Active Directory, and so on). JPS API calls are used to perform user authentication, user authorization, and retrieval of user metadata.

The JpsUserProvider component is installed and enabled as a system component when the Content Server instance is installed against an Oracle WebLogic Server instance. JpsUserProvider also is available as a standard Content Server component.

Caution:

It is unlikely that a site would ever add another JpsUser provider in addition to the system-defined JpsUser provider. Adding another such provider could cause problems for the WebCenter Content Server installation.

You can edit the JpsUser provider configuration using the Providers page in the Content Server instance. The connection configuration also can be edited through the `jps-config.xml` file to use identity and credential stores.

If you want to authenticate against a JPS store, JpsUser provider can be used to share the same security storage as another application on an Oracle WebLogic Server instance. For example, you could use JpsUser provider to share security storage with Image and Processing Manager software installed on an Oracle WebLogic Server instance.

 **Note:**

As of release 11R1 (11.1.1.6.0) Oracle WebCenter Content supports use of the Oracle Virtual Directory library (LibOVD) feature, which enables a site to use multiple providers for login and group membership information through JpsUserProvider. For example, it would be possible to use both Oracle Internet Directory (OID) and Active Directory as sources of user and role information. For information on multi-LDAP configuration in Oracle WebLogic Server, see *Oracle Fusion Middleware Application Security Guide*.

13.2.5.1 Retrieving Direct and Indirect Group Membership for Users

JpsUser provider includes the UseNestedGroups configuration option to specify whether Content Server retrieves users' direct and indirect group membership in the authentication provider, or just users' direct group membership.

If UseNestedGroups is set to FALSE, only users' direct group membership is retrieved from the authentication provider.

If UseNestedGroups is set to TRUE, both direct and indirect group membership is retrieved from the authentication provider. This is the default behavior for the JpsUser provider.

The configuration setting is located in the file `IntradocDir/data/providers/jpsuserprovider/provider.hda`.

13.2.5.2 Custom Field Mapping from LDAP Server

If you map custom fields from your LDAP service to WebCenter Content through the JpsUser provider, the default behavior is to take no action if the custom field is empty. For example, if you had a custom field with the value `123456789` and then removed the value, Oracle WebCenter Content will ignore the missing attribute and continue to reflect `123456789` on the basis that custom fields are unlikely to be empty.

To clear a custom field in WebCenter Content, you must change the default behavior by enabling and setting the variable `ClearMissingAttributes=true` in the `provider.hda` file for JpsUser. The default location for this file is `Domain_Home/ucm/cs/data/providers/jpsuserprovider/provider.hda`. Add the variable before the `@end` line in the file. For example:

```
SourcePath=jpsuser
ProviderClass=idc.provider.jps.JpsUserProvider
ClearMissingAttributes=true
@end
```

See Configuration Variables in *Configuration Reference for Oracle WebCenter Content*.

13.2.5.3 Single Character Mapping for Accounts

WebCenter Content supports the use of single character mapping to specify an account hierarchy retrieved from a flat LDAP structure, such as a % (percent sign) character as a separator to be mapped to a / (forward slash) character. The mapping takes place after all other filtering and name collapsing is performed.

Three settings control this behavior. They can be specified in the `Domain_Home/ucm/cs/data/providers/jpsuserprovider/provider.hda` file or in the `DomainHome/ucm/cs/config/config.cfg` file

- **DoAccountCharMap:** (Boolean) Enables or disables the option. Can be set to `1` or `true`. The default is `false`.
- **AccountCharMapSource:** Specifies the single character in the user store group (account). The default is `%`.
- **AccountCharMapTarget:** Specifies the single character in the Oracle WebCenter Content account name. The default is `/`.

For example:

```
DoAccountCharMap=true
AccountCharMapSource=%
AccountCharMapTarget=/
```

13.2.5.4 Credential Map for JpsUser Provider

You can define a Credential Map for the JpsUser provider by enabling and setting the variable `ProviderCredentialsMap=name_of_map` in the file `Domain_Home/ucm/cs/data/providers/jpsuserprovider/provider.hda`. See [Configuration Variables in Configuration Reference for Oracle WebCenter Content](#). For more information on credentials mapping, see [Credential Mapping](#).

13.2.6 When to Use a Ldapuser Provider

Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs over TCP/IP. It provides high-level functionality to manage resources within a network and works with an application to manage security and user authentication. The LDAP directory service model is based on a collection of attributes and is used to access information stored in an information directory. As such, LDAP is used to validate a set of user name and password credentials against an authentication source. This process will grant privileges to a user to give them access to web resources.

An LDAP server provides a single source for user-related information that can be accessed from applications such as Content Server and other Oracle product modules.

 **Note:**

As of Release 11gR1, Ldapuser provider functionality is superseded by JpsUserProvider for Content Server. Use of the Content Server LDAP provider is **not** recommended for user and security management for Content Server. For more information, see [When to Use a JpsUser Provider](#).

If you decide to use a LDAP server (other than Active Directory, which can be integrated directly with the Content Server instance), you must create a Ldapuser provider to set up communication between the Content Server instance and the LDAP server. When properly configured, the Ldapuser provider authorizes external users through the mapping properties that are linked to role assignments and account permissions (defined on the LDAP Provider page).

For information on LDAP servers that Oracle Fusion Middleware supports, see the certification information on the Oracle Technology Network:

<http://www.oracle.com/technetwork/middleware/webcenter/content/documentation/documentation-155348.html>

Although not required, you are encouraged to have Consulting Services assist you with creating a LDAP security model and deploying the LDAP integration. Contact your sales representative for more information.

LDAP integration can be useful with the following content management products and architectures:

- Content Tracker: Content Tracker is a system that is built from a collection of software features that, when combined, enable users to use a standard browser to track content usage through an integrated set of analytical tools. The data provided by the Content Server instance is derived from logged data that includes web server log data, Content Server data, and user information. Content Tracker accesses this data, performs analysis on it, and produces descriptive reports. Integrating an LDAP directory server with Content Tracker is optional. However, if LDAP is used, a LDAP provider must be created.

For more information about the related data repositories, report generation, producing queries and installation procedures, see Introduction to Oracle WebCenter Content Features in *Managing Oracle WebCenter Content*.

13.3 Understanding Content Server Security Providers

Aside from security configuration integration between Content Server and other Oracle applications, the Content Server's own SecurityProviders component can be used to add security by extending the functionality of basic incoming and outgoing socket providers with two types of providers:

- Secure Socket Layer (SSL) provider
- Keepalive provider

Appropriate use of security providers, along with keys and certificates, can improve the security for network and Internet communication with the Content Server instance. Benefits of using the SecurityProviders component include the following:

- SSL enhances security for web communication by providing communication encryption and authentication.
- Security providers enable use of certificates for socket or server authentication.
- Keepalive and connection pooling logic help avoid SSL expense overhead by reducing the amount of SSL socket creation and teardown.

The SecurityProviders component is installed (enabled) by default with the Content Server instance.

References

To use the SecurityProviders component it is necessary to be familiar with socket providers, security and authentication, SSL, keepalive, and other aspects of security for network communication. The following sources of information can be useful in working with the SecurityProviders component:

- *Java Secure Socket Extension (JSSE) Reference Guide for the Java 2 SDK, Standard Edition*
This online document is available from Oracle. It contains an extensive Related Documents section that includes web links to reference books, security standards, government security policies and regulations, and a list of books on cryptography and SSL.
- *keytool Key and Certification Management Tool*
This online document is available from Oracle.
- *RSA's Public Key Cryptography Standards*
- *RSA's Cryptography FAQ*
- *SSL Certificate FAQ*

Terminology

The following table shows definitions for some of the security terms used in this section. For detailed information refer to the list of information references or to security and authentication standards sources.

Term	Description
Certificate	A digital signature that verifies the identity and public key for an entity (a person or organization). A certificate can be issued by a Certification Authority or by an individual entity.
Certificate Authority (CA)	An entity that issues certificates for other entities, and is recognized as a well-known and trusted source for certificates, such as VeriSign and Thawte.
Keystore	A file or database of information for keys, used for authentication processing.
Private key	Information packaged as a key that is known only to the entity that issues it. Private keys are used in generating signatures.
Public key	Information packaged as a key that is publicly associated with an entity. Public keys are used in verifying signatures.
SSL	Secure Socket Layer, a protocol for secure network communication using a combination of public and secret key technology.
Truststore	A file or database of keys that the trust manager has determined can be trusted.

13.3.1 Planning to Use Security Providers

It is recommended that you determine how you want to use security providers before implementing SSL socket providers or keepalive socket providers for Content Server. Examine the keepalive and SSL connection types and determine whether additional configuration is required to use the security providers you select, such as a need to create keystores or a truststore.

The following sections provide more information about the SSL and keepalive provider types, including the Java classes used to control the behavior of the provider types, and additional configuration that may be necessary.

- [Keepalive Connections](#)
- [SSL Connections](#)
- [Additional Security Configuration](#)

13.3.1.1 Keepalive Connections

The keepalive feature enables persistent connections and the pooling of socket connections for service requests. The setup for keepalive connections is most useful in situations where connection setup and teardown can take a considerable amount of time, and you want to minimize the time spent on that activity. The SecurityProviders component provides two keepalive socket providers: incoming and outgoing.

The following Java classes are used to set up the keepalive incoming socket provider:

Java Class	Description
Provider Class	idc.provider.ExtendedSocketIncomingProvider
Connection Class	idc.provider.KeepaliveSocketIncomingConnection
Server Thread Class	idc.server.KeepaliveIdcServerThread

The following Java classes are used to set up the keepalive outgoing socket provider:

Java Class	Description
Provider Class	idc.provider.KeepaliveSocketOutgoingProvider
Connection Class	idc.provider.KeepaliveSocketOutgoingConnection
Request Class	idc.server.KeepaliveServerRequest

13.3.1.2 SSL Connections

The SSL provider setup enables the use of SSL connections in a keepalive environment. This setup is recommended over a simple SSL provider setup because it helps minimize the cost of SSL socket setup and teardown. The SecurityProviders component provides two SSL socket providers with keepalive: incoming and outgoing.

The following Java classes are used to set up the SSL keepalive incoming socket provider:

Java Class	Description
Provider Class	idc.provider.ssl.SSLSocketIncomingProvider
Connection Class	idc.provider.KeepaliveSocketIncomingConnection
Server Thread Class	idc.server.KeepaliveIdcServerThread

The following Java classes are used to set up the keepalive SSL outgoing socket provider:

Java Class	Description
Provider Class	idc.provider.KeepaliveSocketOutgoingProvider
Connection Class	idc.provider.ssl.SSLSocketOutgoingConnection

Java Class	Description
Request Class	idc.provider.KeepaliveServerRequest

13.3.1.3 Additional Security Configuration

Depending on which type of security provider you choose, there can be additional required configuration.

- **Keepalive and SSL outgoing providers:** The Add Provider page includes a `NumConnections` field, which specifies the number of connections to pool.
- **SSL incoming providers:** The Add Provider page includes two additional options:
 - **Request Client Auth option:** If clients are able, they should authenticate themselves when they make a connection.
 - **Require Client Auth option:** Clients must authenticate themselves in order to make a connection.

SSL providers may also require setup of a keystore or keystores, and a truststore, for both the client and server, depending on the value of the Request Client Auth option, the value of the Require Client Auth option, and what type of Certification Authority signed the certificates handled by these options. For information on keystores and truststore, see [Keystores and Truststore](#).

13.3.2 Keystores and Truststore

SSL providers may require use of keystores and may require a truststore. Keystores are files that hold public and secret key information for use in SSL. A truststore contains certificates that have been determined to be trusted. If a certificate used on the server and client is signed by a well-known Certification Authority (CA) such as VeriSign or Thawte, then a truststore is not necessary, because the default JVM truststore contains the certificates of these CAs. Truststores are needed when certificates used by the SSL providers are self-signed or signed by a private CA. If SSL providers require keystores, and a truststore, then they must be created and managed.

The following sections provide overview information about keystores and truststore.

- [When to Use Keystores and a Truststore](#)
- [Specifying Keystore and Truststore Information](#)
- [Generating a Keystore](#)
- [Creating a Truststore](#)

For more information on keystores and truststores see the sources of information listed in [Understanding Content Server Security Providers](#).

13.3.2.1 When to Use Keystores and a Truststore

The following examples present different situations and uses for keystores and a truststore.

- The server requires a keystore containing a signed SSL certificate in order to create SSL sockets.
- The server requests or requires client authentication, which may require a truststore. If the client's certificate is not signed by a well-known CA, then the server will need a truststore containing that CA's certificate.

- The server requests or requires client authentication, which may require that the client have a keystore in which it stores the certificate the client presents for authentication.
- The server uses a certificate that hasn't been signed by a well-known CA, therefore the client will require a truststore that contains the server's certificate.

13.3.2.2 Specifying Keystore and Truststore Information

In order to use keystore and truststore information, the SSL incoming and outgoing providers require that a file named `sslconfig.hda` be set up in the `providers/` directory (next to the `provider.hda` file). The `sslconfig.hda` file contains configuration information you specify for your keystore and truststore. It has a format similar to the following example. For security reasons, there is no web interface to assist in editing this file; all edits must be done manually using a text editor. Make certain no trailing spaces are included at the end of each line of this or any `.hda` file.

```
@Properties LocalDataTruststoreFile=/servers/idc/data/providers/ssloutgoing1/
truststoreKeystoreFile=/servers/idc/data/providers/ssloutgoing1/keystore@end
```

Configuration Name	Value Description
TruststoreFile	The full path to the truststore file.
KeystoreFile	The full path to the keystore file.

13.3.2.3 Generating a Keystore

This section describes the basic process for generating a keystore. You must determine the specific requirements and names for keys and keystores you want to create for your SSL providers. You can store keystore files wherever you want, because the `sslconfig.hda` file contains full paths for its `KeystoreFile` config settings. However, it is recommended that keystore files are stored in the `IntradocDir/data/providers/provider_name` directory (next to the `provider.hda` and `sslconfig.hda` files) or in the `IntradocDir/config/` directory. Aliases and passwords are set using the provider page in the Content Server instance.

For detailed information on how to use the `keytool` utility to generate a keystore, see the document titled *keytool Key and Certification Management Tool*, available online from Oracle.

Note:

The Java `keytool` utility has a feature that prevent direct interaction with private keys. This feature means that a certificate that is generated using `keytool` is "stuck" in the keystore; there is no way to retrieve the private key portion of the certificate. Inversely, there is no way for `keytool` to import a pre-existing certificate into a Java keystore.

The Portecle Java keystore allows the import and export of private keys from Java keystores. For information refer to portecle.sourceforge.net.

To use `keytool` you must have the utility in your path when you enter the command.

1. Create a key in a keystore. The following command-line example shows how to create a key entry with the name `alias` in a keystore with the name `keystore`. This command prompts for a keystore password, for information that will be used to generate the key, and for a password for the key itself. If the password on the key is different from the password

on the keystore, then the values `KeystoreAlias` and `KeystoreAliasPassword` are required to retrieve the key.

```
keytool -genkey -v -alias alias -keystore keystore
```

2. Generate a certificate signing request. The following command-line example shows how to generate a certificate signing request for the key entry named *alias* in the keystore named *keystore*, which is then stored in the file named *csr_file*. This file can be sent to a CA to be signed.

```
keytool -certreq -v -alias alias -keystore keystore -file csr_file
```

3. Import the CA's certificate into the keystore. The keytool checks the chain of trust on the user's certificate upon import. If the certificate was signed by a CA that is not well-known and the keytool knows nothing about the CA, the certificate is rejected. Therefore any certificate from a CA that is not well-known must first be imported into the keystore to permit the user's certificate to successfully be imported in the next step. The following command line example shows how to import a certificate in a file named *cert_file* into the keystore named *keystore*:

```
keytool -import -v -alias ca_alias -keystore keystore -file cert_file
```

4. Import the signed certificate back into the keystore. Once the certificate signing request has been received by a CA and the signed certificate is sent back from the CA, the certificate can be read into the keystore entry identified by *alias*. The following command line example shows how to import the signed certificate.

```
keytool -import -v -alias alias -keystore keystore_name -file csr_file
```

5. Check that everything is in the keystore.

```
keytool -list -v -keystore keystore_name
```

13.3.2.4 Creating a Truststore

This section describes the basic process for generating a truststore. A truststore is necessary when a SSL provider uses keys that have not been signed by a well-known Certification Authority. A truststore contains only public certificates that have been verified by the person managing the truststore (the trust manager) for the Content Server instance. You must determine the specific requirements and name for the truststore you want to create. You can store a truststore file wherever you want, because the `sslconfig.hda` file contains a full path for a `TruststoreFile` config setting. However, it is recommended that a truststore file is stored in the `IntradocDir/data/providers/provider_name` directory (next to the `provider.hda` and `sslconfig.hda` files) or in the `IntradocDir/config/` directory.

For detailed information on how to use the keytool utility to generate a truststore refer to the document titled `keytool Key and Certification Management Tool`, available online at <http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html>. To use the keytool utility you must have the utility in your path when you enter the command.

The following command line example shows how to create a truststore:

```
keytool -import -v -alias alias -keystore keystore -file cert_files
```

Variable	Description
<i>alias</i>	Alias name for the key.
<i>keystore</i>	Name of the keystore.
<i>cert_file</i>	Path to the Certification Authority's certificate.

13.4 Managing Providers

This section covers the following topics:

- [Adding an Outgoing Provider](#)
- [Adding a Database Provider](#)
- [Adding an Incoming Provider](#)
- [Adding a Preview Provider](#)
- [Adding an Incoming Security Provider](#)
- [Adding an Outgoing Security Provider](#)
- [Adding a JpsUser Provider](#)
- [Adding a HTTP Outgoing Provider](#)
- [Editing Provider Configuration](#)
- [Deleting a Provider](#)

13.4.1 Adding an Outgoing Provider

To add an outgoing provider:

1. Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.
2. In the **Create a New Provider** table on the Providers page, click **Add** in the Action column for the **outgoing** provider type.
3. Enter configuration values on the Outgoing Socket Provider page:

Required Fields

- Provider Name
- Provider Description
- Server Host Name
- Server Port
- Provider Class (predefined)

Optional Fields

- Connection Class (predefined)
- Configuration Class
- Relative Web Root
- HTTP Server Address
- Instance Name
- Required Roles
- Account Filter

Optional Check Boxes

- Proxied
- Notify Target

- Users
 - Released Documents
4. Click **Add**. The Providers page opens with the new provider added to the Providers table.
 5. Restart the Content Server instance.

 **Note:**

Enterprise Search users must restart all open WebCenter Content Server instances when finished adding providers.

13.4.2 Adding a Database Provider

Database provider configuration is specified when WebCenter Content and the Content Server instance are installed in an Oracle WebLogic Server domain.

 **Note:**

If you want to configure database connections for standalone mode, see [Configuring a System Database Provider for Standalone Mode](#), [Configuring a JDBC Database Driver for Standalone Mode](#), and [Configuring an External Database Provider for Standalone Mode](#).

To add a database provider:

1. Using a web browser, access your Content Server home page and select **Administration**, then **Providers**.
2. In the **Create a New Provider** section of the Providers page, click **Add** in the Action column for the **database** provider type.
3. Enter configuration values on the Database Provider page:

Required Fields

- Provider Name
- Provider Description
- Provider Class (predefined)
- Database Type
- JDBC Driver
- JDBC Connection String
- Test Query

Optional Fields

- Connection Class (predefined)
- Configuration Class
- Data Source
- Database Directory

- Database Name
- JDBC User
- JDBC Password
- Number of Connections (default provided)
- Extra Storage Keys (default provided)
- Additional Settings

Optional Check Boxes

- Use Data Source
4. Click **Add**. The Providers page opens with the new provider added to the Providers table.
 5. Restart the Content Server instance.

13.4.3 Adding an Incoming Provider

Consulting Services are required to use providers to connect to server sockets.

To add an incoming provider:

1. Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.
2. In the Create a New Provider section on the Providers page, click **Add** in the Action column for the **incoming** provider type.
3. Enter configuration values on the Incoming Provider page:

Required Fields

- Provider Name
- Provider Description
- Server Port
- Provider Class (predefined)

Optional Fields

- Connection Class (predefined)
 - Configuration Class
4. Click **Add**. The Providers page opens with the new provider added to the Providers table.
 5. Restart the Content Server instance.

13.4.4 Adding a Preview Provider

For instructions on adding the Preview provider, see the information provided with the HTML Preview feature zip file. The HTML Preview feature zip file and guide are available for download from the Oracle Technology Network website.

13.4.5 Adding an Incoming Security Provider

To add an incoming security provider:

1. Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.

- In the **Create a New provider** table on the Providers page, click **Add** in the Action column for the **keepaliveincoming** or the **sslincoming** provider type.
- Enter configuration values on the keepaliveincoming Provider page or the sslincoming Provider page:
Required Fields
 - Provider Name
 - Provider Description
 - Provider Class (predefined)
 - Server Port**Optional Fields**
 - Connection Class (predefined)
 - Configuration Class
 - Server Thread Class (predefined)**Optional Check Boxes (sslincoming provider only)**
 - Request Client Authentication
 - Require Client Authentication
- Click **Add**. The Providers page opens with the new provider added to the Providers table.
- Restart the Content Server instance.

13.4.6 Adding an Outgoing Security Provider

To add an outgoing security provider:

- Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.
- In the **Create a New provider** table on the Providers page, click **Add** in the Action column for the **keepaliveoutgoing** or **ssloutgoing** provider type.
- Enter configuration values on the keepaliveoutgoing Provider page or the ssloutgoing Provider page:
Required Fields
 - Provider Name
 - Provider Description
 - Provider Class (predefined)
 - Server Host Name (predefined)
 - Server Port
 - Instance Name
 - Relative Web Root**Optional Fields**
 - Connection Class (predefined)
 - Configuration Class
 - Request Class (predefined)

- Number of Connections (predefined)
- HTTP Server Address
- Required Roles
- Account Filter

Optional Check Boxes

- Proxied
 - Notify Target
 - Users
 - Released Documents
4. Click **Add**. The Providers page opens with the new provider added to the Providers table.
 5. Restart the Content Server instance.

13.4.7 Adding a JpsUser Provider

A default JpsUser provider, which integrates with Oracle JPS (for an Oracle WebLogic Server instance), is provided with installation of the WebCenter Content system.

 **Caution:**

It is unlikely that a site would ever add another JpsUser provider in addition to the system-defined JpsUser provider. Adding another such provider could cause problems for the Content Server installation.

For information on configuration options in addition to those specified on the JpsUser Provider page, see [Retrieving Direct and Indirect Group Membership for Users](#).

To add a JpsUser provider:

1. Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.
2. In the **Create a New Provider** table on the Providers page, click **Add** in the Action column for the **jpsuser** provider type.
3. Enter configuration values on the JPS User Provider page:

Required fields

- Provider Name
- Provider Description
- Provider Class (predefined)
- Source Path

Optional fields

- Connection Class
- Configuration Class
- JPS Context
- Default Network Roles

4. To specify an attribute map:
 - a. Select an information field from the JPS Attributes list.
 - b. Select a Content Server user information field from the User Attribute list.
 - c. Click **Add**. The attribute map is added to the text box.
 - d. If necessary, edit the attributes directly in the Attribute Map text box.
5. If necessary, change or add Default Network Roles.
6. Click **Add**. The Providers page opens with the new provider added to the Providers table.
7. Restart the Content Server instance.
8. Restart the web server.

13.4.8 Adding a HTTP Outgoing Provider

To add a HTTP outgoing provider:

1. Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.
2. In the **Create a New Provider** table on the Providers page, click **Add** in the Action column for the **httpoutgoing** provider type.
3. Enter configuration values on the Outgoing Http Provider page:

Required fields

- Provider Name
- Provider Description
- Provider Class (predefined)
- CGI URL
- Instance Name
- Relative Web Root

Optional fields

- Connection Class (predefined)
 - Configuration Class
 - Connection Password Name
 - Connection Password
 - Client IP Filter
4. Click **Add**. The Providers page opens with the new provider added to the Providers table.
 5. Restart the Content Server instance.

13.4.9 Editing Provider Configuration

To edit the configuration for an existing provider (except for default system providers):

1. Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.
2. In the **Providers** table on the Providers page, click **Info** in the Action column for the provider to edit.

3. In the Provider Information page, click **Edit**.
4. In the Add/Edit Provider page, make the required changes.
5. Click **Update** to save the changes and return to the Providers page.
6. Restart the Content Server instance.

13.4.10 Deleting a Provider

To delete an existing provider (except for default system providers):

1. Using a web browser, access your Content Server home page and choose **Administration**, then **Providers**.
2. In the **Providers** table on the Providers page, click the **Info** link in the Action column for the provider you want to delete.
3. In the Provider Information page, click **Delete**.
4. Click **OK** on the confirmation window. The provider is removed from the Providers table.

 **Important:**

Ensure that you intend to delete the provider and not just edit the information. When you delete a provider, the provider name and all of its related information is permanently removed from the Providers table.

14

Mapping URLs

This chapter provides information about using the `WebUrlMapPlugin` component to map shortened URLs to other URLs in support of the Oracle WebCenter Content Server use of the Oracle WebLogic Server web server to filter pages through a web browser. This chapter includes the following topics:

- [WebUrlMapPlugin Component](#)
- [Script Construction](#)
- [Supported Variables for Referencing](#)
- [Add/Edit URL Mapping Entries](#)
- [Mapping Examples](#)

14.1 WebUrlMapPlugin Component

WebCenter Content uses an Oracle WebLogic Server, which has a built-in web server, to filter pages through a web browser. User requests are authenticated with the Oracle WebLogic Server user store, or other configured user store, and communicated with the Content Server instance.

The `WebUrlMapPlugin` component enables you to map shortened URLs to other URLs using a substitution script for the mapping, which also enables you to map long URLs to abbreviated versions. The `WebUrlMapPlugin` component is installed (enabled) by default with the Content Server instance.

14.2 Script Construction

The shortened URLs that you can create generally use the following format:

```
http://myhostexample.com/prefix/suffix
```

The actual mapping process is based on the part of the URL that follows the host name portion. To resolve the shortened URL, the Content Server instance compares the prefix to those in the list of defined `WebUrlMapPlugin` entries. If a match exists, the Content Server instance uses the map script that corresponds to the matching prefix to display the applicable document or Content Server page. For more information about the suffix, see [Supported Variables for Referencing](#).

To construct a URL mapping entry using the `WebUrlMaps` page, you must establish a prefix and define the corresponding map.

Prefix

The prefix portion of the mapping entry is any abbreviation you want to use to identify URLs of a certain form. For example, if you want your short URL to return the dynamic conversions of documents, you can use `idc` as your prefix (for example, the abbreviated form of dynamic converter).

When you create your prefix, do not enter a slash (/) character at the beginning of it because the Content Server instance removes the first slash from the incoming URL before the prefix test is performed.

▲ Caution:

Include a slash (/) at the end of your URL map prefix. Otherwise, your mappings can apply to many more URLs and interfere with standard Content Server operations.

Map

The map portion of the mapping entry is the Idoc Script code that the Content Server instance uses to resolve the shortened URL. You can use substitution tags (`<!--$variable-->`) in the map portion. Examples include:

```
<!--$cgipath-->
<!--$internetuser-->
<!--$suffix-->
```

These substitution tags are variables that refer to the applicable parameters of a URL.

Simple 'if' constructions are also supported. For example, the following script segment performs a test to determine whether a value exists and is not empty:

```
<!--$if myconfigvar-->something<!--$endif-->
```

14.3 Supported Variables for Referencing

The map portion of the URL mapping entry uses the following standard variables for referencing:

- The CGI path
This is the current CGI path of the Oracle WebLogic Server web server filter's configured Content Server instance. The web server filter is configured to provide both communication and security for this Content Server instance. A typical example is `/idcm1/idcplg`.
- The 'suffix' parameter
The value of the suffix variable (`<!--$suffix-->`) is derived from the part of the URL that follows the preliminary mapping 'prefix' and before the question mark (?). Any slashes (/) at the beginning of the suffix are removed before being substituted into this variable. For example, in the following URL, 'dc' is the mapping prefix followed by the suffix.

```
http://myhostexample.com/dc/mydocumentname
```

After removing the slash, `mydocumentname` is used as the value for the suffix variable that is used as a substitution tag in the map portion of the mapping entry. Also, the suffix variable does not include any CGI parameters. Therefore, in the following URL, `mydocumentname` is still used as the suffix variable's value.

```
http://myhostexample.com/dc/mydocumentname?a=1
```

To enforce the slash separation between the prefix and suffix, add the slash at the end of your prefix abbreviation.

- Any plugin variable

For example, you could use the construct `<!--$internetuser-->` to substitute for the user ID of the currently logged-in user.

- Any CGI parameter

14.4 Add/Edit URL Mapping Entries

To add or edit URL mapping entries:

1. On the Content Server home page, choose **Administration**, then **WebUrlMapPlugin**.
2. In the WebUrlMaps page, enter the appropriate values in the **Prefix** and **Map** fields to edit the existing mapping entries, or define new entries, or both.
3. Click **Update**. The page refreshes and the **Prefix** and **Map** field values are saved. If all of the displayed fields are populated, two additional **Prefix** and **Map** field pairs are displayed after the page is redisplayed.

! Important:

The WebUrlMapPlugin feature is designed to support hundreds of mapping entries. However, be aware that thousands of mapping entries will impact performance of the web server.

14.5 Mapping Examples

The following examples demonstrate mapping scripts and techniques.

- [Info Update Form](#)
- [Dynamic Conversion](#)
- [CGI parameters](#)

14.5.1 Info Update Form

You can define a web URL mapping script that enables you to create a shortened URL to generate the Info Update Form for existing content items. You can write the mapping script to allow users to enter any identification variable for a particular document. For example, all URLs with the following format:

```
http://myhostexample.com/u/mydoc_parameter
```

can be mapped to the URL:

```
http://myhostexample.com/idcm1//idcplg?IdcService=GET_UPDATE_FORM&dDocName=mydocumentname
```

To map URLs, define the following web URL map entry using the WebUrlMaps page:

- **Prefix:**
u/
- **Map:**
`<!--$cgipath-->?IdcService=GET_UPDATE_FORM<!--$suffix-->&myparam=<!--$myparam-->`

14.5.2 Dynamic Conversion

Dynamic Converter must be installed for this URL mapping example to work. See Dynamic Converter in *Managing Oracle WebCenter Content*.

You can define a web URL mapping script that enables you to create shortened URLs to various dynamic conversions of documents. For example, all URLs with the following format:

```
http://myexamplename.com/dc/mydocumentname
```

can be mapped to the URL:

```
http://myhostexample.com/idcm1/idcplg?  
IdcService=GET_DYNAMIC_CONVERSION&dDocName=mydocumentname&RevisionSelectionMethod=LatestR  
eleased
```

To map URLs, define the following web URL map entry using the WebUrlMaps page:

- **Prefix:**
dc/
- **Map:**
<!--\$cgipath-->?IdcService=GET_DYNAMIC_CONVERSION&dDocName=<!--\$suffix--
>&RevisionSelectionMethod=LatestReleased

14.5.3 CGI parameters

You can also directly reference CGI parameters. For example, URLs with the following format:

```
http://myhostexample.com/dcp/mydocumentname?myparam=myvalue
```

can be mapped to the URL:

```
http://myhostexample.com/idcm1/idcplg?  
IdcService=GET_DYNAMIC_CONVERSION&dDocName=mydocumentname&RevisionSelectionMethod=LatestReleased&myparam=  
myvalue
```

To map URLs, define the following web URL map entry using the WebUrlMaps page:

- **Prefix:**
dcp/
- **Map:**
<!--\$cgipath-->?IdcService=GET_DYNAMIC_CONVERSION&dDocName=<!--\$suffix--
>&RevisionSelectionMethod=LatestReleased&myparam=<!--\$myparam-->

Part V

Administering Security

This part provides information about administering security for Oracle WebCenter Content. It includes details for integrating the system with other Oracle security software; configuring and managing user types, logins, aliases, and accounts; administering ACLs; and managing security for Imaging and Records features.

This part contains the following chapters:

- [Understanding Security and User Access](#)
- [Configuring Fusion Middleware Security for Content Server](#)
- [Managing User Types, Logins, and Aliases](#)
- [Managing Security Groups, Roles, and Permissions](#)
- [Managing Accounts](#)
- [Managing Access Control List Security](#)
- [Managing Additional Content Server Security Connections](#)
- [Customizing Content Server Communication](#)

Understanding Security and User Access

This chapter provides introductory information on Oracle WebCenter Content security as it is integrated with other Oracle products, and its own internal security features and supplemental security options.

This chapter includes the following topics:

- [Overview of Content Server Security](#)
- [Security within Content Server](#)
- [Additional Security Options](#)
- [Advanced Security Options](#)

15.1 Overview of Content Server Security

A Content Server instance is deployed on a WebCenter Content domain, which is deployed on an Oracle WebLogic Server domain in Oracle Fusion Middleware. Security is supported at multiple levels including the Content Server instance, the WebCenter Content domain, the Oracle WebLogic Server domain, and Oracle Platform Security Services (OPSS).

Access to content in the Content Server repository requires a Content Server administrator to manage content, users, and groups, as well as roles, permissions, and accounts. An Oracle WebLogic Server administrator functions as the Content Server administrator. An Oracle WebLogic Server administrator must log in to the Content Server instance and set up the primary Content Server administrator account and password, if no such user was configured during deployment. After the Content Server administrator is configured, management tasks can be performed on the Content Server instance. See *Installing the Oracle WebCenter Content Software* in *Installing and Configuring Oracle WebCenter Content*.

Most user management tasks must be performed using the Oracle WebLogic Server Administration Console instead of the User Admin app on the Content Server instance. By default, WebCenter Content uses the Oracle WebLogic Server user store to manage user names and passwords, and the credential store is leveraged to grant users access to the Content Server instance. For an enterprise-level system, Oracle Platform Security Services (OPSS) can be used instead of the default Oracle WebLogic Server user store to authenticate and authorize users. For more information on integrating WebCenter Content security with Oracle WebLogic Server and OPSS, see [Configuring Fusion Middleware Security for Content Server](#).

Content Server offers several levels of security for repository content: *security groups* (which are required) and *accounts* (which are optional). Each content item is assigned to a security group, and if accounts are enabled then content items can also be assigned to an account. Users are assigned a certain level of permission (Read, Write, Delete, or Admin) for each security group and account, which enables them to work with a content item only to the extent that they have permissions to the item's security group and account. For more information on users, groups, and accounts internal to Content Server, see [Managing User Types, Logins, and Aliases](#), [Managing Security Groups, Roles, and Permissions](#), and [Managing Accounts](#).

Access control lists (ACLs) can be configured for a Content Server instance to provide extended control of content access to users on an enterprise-level system. An access control

list is a list of users, groups, or Enterprise roles with permission to access or interact with a content item. For more information, see [Managing Access Control List Security](#) .

15.2 Security within Content Server

The administrator sets up initial user and content security within Content Server by using the User Admin application to define user roles, permissions to groups, and accounts. Then the administrator uses the Oracle WebLogic Server Administration Console to create users and assign each user to one or more of the Content Server roles, which in turn are assigned specific permissions to security groups. If accounts are enabled in Content Server, the administrator can assign users specific permissions to certain accounts, which then limits the permissions the users might otherwise have through their assigned roles.

For information on users, see [Managing User Types, Logins, and Aliases](#) . For information on security groups, roles, and permissions, see [Managing Security Groups, Roles, and Permissions](#) . For information on accounts, see [Managing Accounts](#) .

The following components also can be used to provide additional internal Content Server security:

- Security can be customized for user access by using the ExtranetLook component, which is installed (disabled) with Content Server. For more information, see [Login/Logout Customization](#) .

Note:

The ExtranetLook component is not applicable when the Oracle WebLogic Server domain is used as the web server for the Content Server instance. Modification of the security implementation is controlled through direct customization of the Oracle WebLogic Server domain and administrative configuration.

- Security can be customized for user access and search results by using the NeedToKnow component. This component enables you to further configure user access restrictions, modify the display of search results, alter search behavior, and set up *hit list* roles. To use this component, you must install and enable it.

Be aware that Internet Explorer 7 supplies the following message to users logging in with basic authentication without a secure connection:

```
Warning: This server is requesting that your username and password be sent in an insecure manner
```

The behavior (sending user name and password in text) is not new for basic authentication and does not cause problems.

15.3 Additional Security Options

WebCenter Content can combine additional authentication methods. For example, you can define some users with the Oracle WebLogic Server Administration Console, allow some users to log in using their Microsoft domain identity, and grant other users access to the Content Server instance based on their external Lightweight Directory Access Protocol (LDAP) credentials. However, authentication is configured through Oracle WebLogic Server, so the combination of methods is limited. Users can authenticate against multiple authentication stores, but because of the Oracle Platform Security Services (OPSS) and Oracle WebLogic

Server integration, only one of the configured user stores can be used to extract authorization (group) information.

 **Note:**

As of 11g Release 1 (11.1.1.6.0) Oracle WebCenter Content supports use of the Oracle Virtual Directory library (libOVD) feature, which enables a site to use multiple providers for login and group membership information. For example, it would be possible to use both Oracle Internet Directory (OID) and Active Directory as sources of user and role information. For information on multi-LDAP configuration in Oracle WebLogic Server, see *Configuring Single and Multiple LDAPS* in *Oracle Fusion Middleware Application Security Guide*.

The following options can be used to provide additional security:

- Security can be customized to support encrypted socket communication and authentication by using the SecurityProviders component, which is installed (enabled) by default with WebCenter Content. This component enables a Secure Sockets Layer (SSL) provider, which can be configured to use certificates for socket or server authentication.

If you use SSL and HTTPS to connect to WebCenter Content, and are unable to connect through WebDAV, try connecting to the Content Server instance through the browser using the same URL you used in your WebDAV connection string. This lets you see if there is a problem with the certificate, which is used to encrypt communications. If you get a dialog box stating a problem with the certificate, resolve the issue and then try to connect through WebDAV again.

- For users to access the Content Server instance using different web server front ends, when one server front end is HTTPS and the other is HTTP, you can customize the Content Server configuration using the BrowserUrlPath component. This component is installed (disabled) by default with WebCenter Content and supports a web server front end using HTTPS and a load balancer that forwards itself as the HTTP Host header. If you only use one access method (only HTTPS, or only HTTP), or you are not using a load balancer that blocks the "Host" parameter from the browser, then this component is unnecessary. For more information, see [Browser URL Customization](#).
- Extended security attributes can be assigned to external users or to users for a specific application. The extended attributes are merged into pre-existing user attributes and enable additional flexibility in managing users. For more information, see [Extended User Attributes](#).

In all environments, a comprehensive understanding of your organization's security needs and a thorough planning phase is crucial to a successful security integration.

15.4 Advanced Security Options

The advanced security options allow you to handle all the security configurations recommended for WebCenter Content. You can specify the advanced security options either by using APIs or the user interface.

 **Note:**

If a user provides an invalid field name in the QueryText when the advanced security options are enabled, an error message is displayed.

Configuring Advanced Security by Using APIs

Use the following APIs to enable the advanced security options:

- `ASC_GET_SECURITY_CONFIGURATIONS`: Provides details about the existing security configurations in WebCenter Content.
- `ASC_UPDATE_SECURITY_CONFIGURATIONS`: Enables you to update the security configurations as well as the field or column names when a new table is added or deleted, by passing the respective input parameters.

For more information on the APIs and parameters, see Core Content Server Services in *Services Reference for Oracle WebCenter Content*.

Configuring Advanced Security by Using the User Interface

You can specify the advanced security options in the Oracle Advanced Security Configurations page. However, this page is not available by default. You can enable or disable this page based on your requirement. For more information, see [Enabling Oracle Advanced Security Configurations Page](#).

15.4.1 Enabling Oracle Advanced Security Configurations Page

By enabling the Oracle Advanced Security Configurations page, you can specify the security options for Core QueryText and FrameworkFolders QueryText.

To enable the Oracle Advanced Security Configurations Page:

1. Using a text editor, open the `config.cfg` file located in the `IntradocDir/config/directory`.
2. Add the following parameter:
 - `IsAdvanceSecurityConfigUIEnabled=True`
3. Save the `config.cfg` file.
4. Restart the Content Server instance.

The Oracle Advanced Security Configurations option is available in the **Administration** menu.

 **Note:**

You can also enable the Oracle Advanced Security Configurations page by selecting **Administration**, then **Admin Server**, and then **General Configuration**. In the Additional Configuration Variables area, you can add the parameter `IsAdvanceSecurityConfigUIEnabled=True`. However, you must restart the content server to see the Oracle Advanced Security Configurations option in the **Administration** menu.

This section covers the following topics:

- [Specifying Advanced Security Options for Core QueryText](#)
- [Specifying Advanced Security Options for FrameworkFolders QueryText](#)

15.4.1.1 Specifying Advanced Security Options for Core QueryText

Specifying the advanced security options for Core QueryText executes the search function by matching the entered search criteria and returning the results accordingly.

To specify the advanced security options for Core QueryText:

1. Select **Administration**, then **Oracle Advanced Security Configurations**.

The Oracle Advanced Security Configurations page appears.

2. Select the **Core QueryText Security Config** check box to edit and update this section.

If you do not select the **Core QueryText Security Config** check box, the changes made to this section are not saved.

3. Select the **Enable QueryText security validation** check box to enable the custom query validations.

If you do not select the **Enable QueryText security validation** check box, the Core QueryText validation is disabled.

4. Enter one or more table names in the **Custom table names** field to include these tables in the search criteria.

5. Enter one or more field names in the **Custom field names** field to include these fields in the search criteria.

 **Note:**

The values entered in the fields **Custom table names** and **Custom field names** should be separated by a semicolon (;).

6. Click **Update** to save the entered details.

15.4.1.2 Specifying Advanced Security Options for FrameworkFolders QueryText

Specifying the advanced security options for FrameworkFolders QueryText executes the entered search criteria within the framework folders and returns the results accordingly.

To specify the advanced security options for FrameworkFolders QueryText:

1. Select **Administration**, then **Oracle Advanced Security Configurations**.

The oracle Advanced Security Configurations page appears.

2. Select the **FrameworkFolders QueryText Security Config** check box to edit and update this section.

If you do not select the **FrameworkFolders QueryText Security Config** check box, the changes made to this section are not saved.

3. Select the **Enable QueryText security validation** check box to enable the custom query validations.

If you do not select the **Enable QueryText security validation** check box, the FrameworkFolders QueryText validation is disabled.

4. Enter one or more table names in the **Custom table names** field to include these tables in the search criteria.
5. Enter one or more field names in the **Custom field names** field to include these fields in the search criteria.

 **Note:**

The values entered in the fields **Custom table names** and **Custom field names** should be separated by a semicolon (;).

6. Click **Update** to save the entered details.

16

Configuring Fusion Middleware Security for Content Server

This chapter provides security configuration information and procedures for integrating Oracle Fusion Middleware, Oracle WebLogic Server, and Oracle authentication and authorization software with Oracle WebCenter Content and Oracle WebCenter Content Server. This chapter includes the following topics:

- [LDAP Authentication Providers](#)
- [Configuring Oracle WebCenter Content to Use SSL](#)
- [Configuring WebCenter Content for Single Sign-On](#)
- [Configuring Oracle Infrastructure Web Services](#)
- [Configuring WebCenter Content for Oracle Identity Cloud Service \(IDCS\)](#)
- [Configuring SAML-Based Single Sign-On](#)

For more information about Oracle Fusion Middleware and Oracle WebLogic Server security, see the documentation listed in [Table 16-1](#).

16.1 LDAP Authentication Providers

Oracle WebCenter Content runs on Oracle WebLogic Server. The Oracle WebLogic Server domain includes an embedded Lightweight Directory Access Protocol (LDAP) server that acts as the default security provider data store for the Default Authentication, Authorization, Credential Mapping, and Role Mapping providers. WebCenter Content provides the default JpsUserProvider to communicate with Oracle WebLogic Server. See *Managing the Embedded LDAP Server* in *Administering Security for Oracle WebLogic Server*, and *Configure the Embedded LDAP Server* in *Oracle WebLogic Server Administration Console Online Help*.

In almost all cases, an Oracle WebCenter Content production system identity store must be reassociated with an external LDAP authentication provider rather than use the embedded LDAP server. Once the new LDAP authentication provider is configured, then you migrate users from the embedded LDAP provider to the new LDAP provider. The external LDAP authentication provider, such as Oracle Internet Directory (OID), must be listed before all other authentication providers including the default authentication provider. See *Reassociating the Identity Store with an External LDAP Authentication Provider* in *Installing and Configuring Oracle WebCenter Content*.

Note:

As of 11g Release 1 (11.1.1.6.0) Oracle WebCenter Content supports use of the Oracle Virtual Directory library (libOVD) feature, which enables a site to use multiple providers for login and group membership information. For example, it would be possible to use two Oracle Internet Directory (OID) providers as sources of user and role information. See *Configuring Single and Multiple LDAPs* in *Securing Applications with Oracle Platform Security Services*.

Table 16-1 lists some of the LDAP providers that can be configured for user authentication.

Table 16-1 LDAP Authenticator Types

LDAP Servers	Authenticator Providers
Microsoft AD	ActiveDirectoryAuthenticator
SunOne LDAP	IPlanetAuthenticator
Oracle Directory Server Enterprise Edition (ODSEE)	IPlanetAuthenticator
Oracle Unified Directory (OUD)	IPlanetAuthenticator
Oracle Internet Directory	OracleInternetDirectoryAuthenticator
Oracle Virtual Directory	OracleVirtualDirectoryAuthenticator
EDIRECTORY	NovellAuthenticator
OpenLDAP	OpenLDAPAuthenticator
EmbeddedLDAP	DefaultAuthenticator

If you want to configure WebCenter Content to use an external LDAP server and have dynamic groups (as well as static groups) on your Directory whose privileges you want recognized by WebCenter Content, additional configuration is necessary. User creation, authentication, and authorization is managed using Oracle Platform Services Security (OPSS), which uses a different mechanism to gather Directory Server information when compared to the native Oracle WebLogic Server providers for an external LDAP server. See Oracle WebCenter and Dynamic Groups from an External LDAP Server blog.

16.2 Configuring Oracle WebCenter Content to Use SSL

You can configure Oracle Fusion Middleware to secure communications with WebCenter Content using SSL, which is an industry standard for securing communications. Oracle Fusion Middleware supports SSL version 3, as well as TLS version 1.

This section covers the following topics:

- [Configuring WebCenter Content for Two-Way SSL Communication](#)
- [Invoking References in One-Way SSL Environments in Oracle JDeveloper](#)
- [Configuring WebCenter Content, Oracle HTTP Server for SSL Communication](#)
- [Switching from Non-SSL to SSL Configurations for WebCenter Content](#)
- [Using a Custom Trust Store for One-Way SSL](#)
- [Enabling an Asynchronous Process to Invoke an Asynchronous Process](#)
- [Configuring RIDC SSL for Valid Certificate Path](#)

For additional information, see *Configuring SSL in Administering Security for Oracle WebLogic Server*. For information on Web Tier configuration, see *SSL Configuration in Oracle Fusion Middleware in Administering Oracle Fusion Middleware*.

16.2.1 Configuring WebCenter Content for Two-Way SSL Communication

WebCenter Content uses the Oracle WebLogic Server secure socket layer (SSL) stacks for two-way SSL configurations.

- For the inbound Web service bindings, WebCenter Content uses the Oracle WebLogic Server infrastructure and, therefore, the Oracle WebLogic Server libraries for SSL.
- For the outbound Web service bindings, WebCenter Content uses JRF HttpClient and, therefore, the Oracle Sun JDK libraries for SSL.

Due to this difference, start Oracle WebLogic Server with the following JVM option:

1. Open the following file:
 - On UNIX operating systems, open `$MIDDLEWARE_HOME/user_projects/domains/domain_name/bin/setDomainEnv.sh`.
 - On Window operating systems, open `MIDDLEWARE_HOME\user_projects\domains\domain_name\bin\setDomainEnv.bat`.
2. Add the following lines in the `JAVA_OPTIONS` section, if the server is enabled for one-way SSL (server authorization only):

```
-Djavax.net.ssl.trustStore=your_truststore_location
```

For two-way SSL, the keystore information (location and password) is not required.

To enable two-way SSL for WebCenter Content to invoke another application:



Note:

Both the server and client are assumed to have been configured for SSL with mutual authentication.

1. On the client side, provide the keystore location.
 - a. From the **SOA Infrastructure** menu, choose **SOA Administration**, then **Common Properties**.
 - b. At the bottom of the page, click **More SOA Infra Advanced Configuration Properties**.
 - c. Click **KeystoreLocation**.
 - d. In the **Value** column, enter the keystore location.
 - e. Click **Apply**.
 - f. Click **Return**.

2. On the client side, provide the keystore location in `DOMAIN_HOME\config\soa-infra\configuration\soa-infra-config.xml`.

```
<keystoreLocation>absolute_path_to_the_keystore_location_and_the_file_name
</keystoreLocation>
```

3. During design time in Oracle JDeveloper, update the reference section in the `composite.xml` file with the `oracle.soa.two.way.ssl.enabled` property.

```
<reference name="Service1"
  ui:wSDLLocation=". . .">
  <interface.wSDL interface=". . ."/>
  <binding.ws port=". . .">
    <property name="oracle.soa.two.way.ssl.enabled">true</property>
  </binding.ws>
</reference>
```

4. In Oracle Enterprise Manager Fusion Middleware Control Console, select **WebLogic Domain**, then *domain_name*.
5. Right-click *domain_name* and select **Security**, then **Credentials**.
6. Click **Create Map**.
7. In the **Map Name** field, enter a name (for example, SOA), and click **OK**.
8. Click **Create Key**.
9. Enter the following details:

Field	Description
Select Map	Select the map created in Step 7 (for this example, SOA).
Key	Enter the key name (<i>KeystorePassword</i> is the default).
Type	Select Password .
User Name	Enter the keystore user name (<i>KeystorePassword</i> is the default).
Password	Enter the password that you created for the keystore.

 **Note:**

When you set up SSL on an Oracle WebLogic Server domain, a key alias is required. You must enter *mykey* as the alias value. This value is required.

10. Set the keystore location in Oracle Enterprise Manager Fusion Middleware Control Console. See Step 1 for instructions.
11. Modify the `composite.xml` syntax to use `https` and `sslport` to invoke Oracle WebCenter Content. For example, change the syntax shown in bold:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- Generated by Oracle SOA Modeler version 1.0 at [4/1/09 11:01 PM]. -->
<composite name="InvokeEchoBPELSync"
revision="1.0"
label="2009-04-01_23-01-53_994"
mode="active"
state="on"
xmlns="http://xmlns.example.com/sca/1.0"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:orawsp="http://schemas.example.com/ws/2006/01/policy"
xmlns:ui="http://xmlns.example.com/soa/designer/">
<import
namespace="http://xmlns.example.com/CustomApps/InvokeEchoBPELSync/BPELProcess1"
location="BPELProcess1.wsdl" importType="wsdl"/>
<import namespace="http://xmlns.example.com/CustomApps/EchoBPELSync/
BPELProcess1" location="http://hostname:port/soa-infra/services/default/EchoBPEL
Sync/BPELProcess1.wsdl"
importType="wsdl"/>
```

to use `https` and `sslport`:

```
location="https://hostname:sslport/soa-infra/services/default/EchoBPELSync
/BPELProcess1.wsdl"
```

16.2.2 Invoking References in One-Way SSL Environments in Oracle JDeveloper

When invoking a Web service as an external reference from WebCenter Content in one-way SSL environments, ensure that the certificate name (CN) and the host name of the server exactly match. This ensures a correct SSL handshake.

For example, if a Web service is named `adfbcl` and the certificate has a server name of `host`, the following results in a SSL handshake exception.

```
<import namespace="/adfbcl/common/"
location="https://host.example.com:8002/CustomApps-adfbcl-context-root/AppModuleService?WSDL"
importType="wsdl"/>
<import namespace="/adfbcl/common/" location="Service1.wsdl"
importType="wsdl"/>
```

If you switch the order of `import`, the SSL handshake passes.

```
<import namespace="/adfbcl/common/" location="Service1.wsdl"
importType="wsdl"/>
<import namespace="/adfbcl/common/"
location="https://host.example.com:8002/CustomApps-adfbcl-context-root/AppModuleService?WSDL"
importType="wsdl"/>
```

Note the following restrictions around this issue:

- There are no options for ignoring host name verification in Oracle JDeveloper as exist with the Oracle WebLogic Server Administration Console. This is because the SSL kit used by Oracle JDeveloper is different. Only the trust store can be configured from the command line. All other certificate arguments are not passed.
- In the WSDL file, `https://hostname` must match with that in the certificate, as described above. You cannot perform the same procedures as you can with a browser. For example, if the host name is `host.example.com` in the certificate's CN, then you can use `host`, `host.example.com`, or the IP address from a browser. In Oracle JDeveloper, always use the same name as in the certificate (that is, `host.example.com`).

16.2.3 Configuring WebCenter Content, Oracle HTTP Server for SSL Communication

Follow these procedures to configure SSL communication between WebCenter Content and Oracle HTTP Server.

See *Configuring SSL for the Web Tier* in *Administering Oracle Fusion Middleware*.

To configure Oracle HTTP Server for SSL communication:

1. Append `ssl.conf` with the `<Location /cs>` location directive, where `port` is the port number of the target managed server.

```
<Location /cs>
    WebLogicPort 8002
    SetHandler weblogic-handler
    ErrorPage http://host.example.com:port/error.html
</Location>
```

2. Start the Oracle WebLogic Server as described in [Configuring WebCenter Content for Two-Way SSL Communication](#).

To configure certificates for Oracle Client, Oracle HTTP Server, and Oracle WebLogic Server:

1. Export the user certificate from the Oracle HTTP Server wallet.

```
orapki wallet export -wallet . -cert cert.txt -dn 'CN=\"Self-Signed Certificate for  
ohsl \",OU=OAS,O=ORACLE,L=REDWOODSHORES,ST=CA,C=US'
```

2. Import the above certificate into the Oracle WebLogic Server truststore as a trusted certificate.

```
keytool -file cert.txt -importcert -trustcacerts -keystore DemoTrust.jks
```

3. Export the certificate from the Oracle WebLogic Server truststore.

```
keytool -keystore DemoTrust.jks -exportcert -alias wlscertgencab -rfc -file  
certgencab.crt
```

4. Import the above certificate to the Oracle HTTP Server wallet as a trusted certificate.

```
orapki wallet add -wallet . -trusted_cert -cert certgencab.crt -auto_login_only
```

5. Restart Oracle HTTP Server.

6. Restart the Oracle WebLogic Server as described in [Configuring WebCenter Content for Two-Way SSL Communication](#).

16.2.4 Switching from Non-SSL to SSL Configurations for WebCenter Content

Switching from non-SSL to SSL configurations for WebCenter Content requires the **Frontend Host** and **Frontend HTTPS Port** fields to be set in the Oracle WebLogic Server Administration Console. Not doing so results in exception errors when you attempt to create to-do tasks.

1. Log in to the `wls_console`.
2. In the **Environment** section, select **Servers**.
3. Select the name of the managed server (for example, `UCM_server1`).
4. Select **Protocols**, then select **HTTP**.
5. In the **Frontend Host** field, enter the host name on which the WebCenter Content domain is located.
6. In the **Frontend HTTPS Port** field, enter the SSL listener port.
7. Click **Save**.

16.2.5 Using a Custom Trust Store for One-Way SSL

To invoke WebCenter Content over HTTPS when using a custom trust store created with a tool such as `keytool` or `orapki`, perform the following actions in Oracle JDeveloper:

1. To fetch a WSDL file in the reference section, set the trust store information in **Tools**, then **Preferences**, then **Http Analyzer**, then **HTTPS Setup**, then **Client Trusted Certificate Keystore**.
2. During deployment to a SSL-enabled server, use the JSSE property at the command line:

```
jdev -J-Djavax.net.ssl.trustStore=your_trusted_location
```

16.2.6 Enabling an Asynchronous Process to Invoke an Asynchronous Process

To enable an asynchronous process deployed to a SSL-enabled, managed server to invoke another asynchronous process over HTTP, start by assuming you create the following environment:

- Asynchronous BPEL process A that invokes asynchronous BPEL process B
- Asynchronous BPEL process A is deployed to a one-way SSL enabled, managed server
- All WSDL reference and bindings use plain HTTP

At run time, the WSDL is looked for over HTTPS, and the callback message from asynchronous BPEL process B fails.

To resolve this issue, the `callbackServerURL` property must be passed at the reference binding level in the `composite.xml` file. This explicitly indicates the value of the callback URL for the given reference invocation. If the client composite is running in a SSL-managed server, then the callback defaults to SSL.

```
<reference name="Service1" ui:wSDLLocation="http://localhost:8000/soa-infra/services/default/
  AsyncSecondBPELMTOM/BPELProcess1.wsdl">
  <interface.wsdl interface="http://xmlns.example.com/Async/AsyncSecondBPELMTOM/BPELProcess1#
    wsdl.interface (BPELProcess1)" callbackInterface="http://xmlns.example.com/Async/
    AsyncSecondBPELMTOM/BPELProcess1#wsdl.interface (BPELProcess1Callback)"/>
  <binding.ws port="http://xmlns.example.com/Async/AsyncSecondBPELMTOM/BPELProcess1#
    wsdl.endpoint (bpelprocess1_client_ep/BPELProcess1_pt)"
    location="http://localhost:8000/soa-infra/services/default/AsyncSecondBPELMTOM
    /bpelprocess1_client_ep?WSDL">
    <wsp:PolicyReference URI="oracle/wss_username_token_client_policy"
      orawsp:category="security" orawsp:status="enabled"/>
    <wsp:PolicyReference URI="oracle/wsaddr_policy" orawsp:category="addressing"
      orawsp:status="enabled"/>
    <property name="callbackServerURL">http://localhost:8000/</property>
  </binding.ws>
  <callback>
    <binding.ws port="http://xmlns.example.com/Async/AsyncSecondBPELMTOM/BPELProcess1#
      wsdl.endpoint (bpelprocess1_client_ep/BPELProcess1Callback_pt)">
      <wsp:PolicyReference URI="oracle/wss_username_token_service_policy"
        orawsp:category="security" orawsp:status="enabled"/>
    </binding.ws>
  </callback>
</reference>
```

16.2.7 Configuring RIDC SSL for Valid Certificate Path

To use Remote Intradoc Client (RIDC) and self-signed certificates, you must import the certificate into your local JVM certificate store so the certificate will be trusted.

1. Retrieve the key from the Content Server instance. For example:

```
openssl s_client -connect host.example.com:7045 2>/dev/null

CONNECTED(00000003)
---
Certificate chain
 0 s:/C=US/ST=MyState/L=MyTown/O=MyOrganization/OU=FOR TESTING ONLY/CN=hostname
  i:/C=US/ST=MyState/L=MyTown/O=MyOrganization/OU=FOR TESTING ONLY/CN=CertGenCAB
```

```

---
Server certificate
-----BEGIN CERTIFICATE-----
MIIB6zCCAZUCEItVMwHDFXAnYG//RoVbXQgwdQYJKoZIhvcNAQEEBQAweTELMakG
A1UEBhmCVVMxEDAObgNVBAgTB015U3RhdGUxZDZANBgNVBAcTBk15VG93bjEXMBUG
A1UEChMOTXlPcmdhbm16YXRpb24xGTAXBgNVBAsTEEZPUIBURVNUSU5HIE90TFkx
EzARBgNVBAMTCkNlcnRHZW5DQUIwHhcNMDkwMzI5MjM0NDM0WhcNMjQwMzZmMjM0
NDM0WjB5MQswCQYDVQGEwJVUzEQMA4GA1UECBYHTXlTdGF0ZTEPMA0GA1UEBxYG
TXlUb3duMRcwFQYDVQKFg5NeU9yZ2FuaXphdGlvbWZEMBCGA1UECXYQRk9SIFRF
U1RJTkcwT05MWTETMBEGA1UEAxYKZGFkdm1jMDAyMjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQCmxv+h8kzOc2xyjMCDPM6By5LY0Vlp4vzWFKmPgEYtp6Wd87sG+YDB
PeFOz210XXGMx6F/14/yFlpCplmazWkDagMBAAEwDQYJKoZIhvcNAQEEBQADQQBn
uF/s6EqCT38Aw7h/406uPhNh6LUF7XH7QzmRv3J1sCqxRnA/fk3JCXE1shv1Pk8G
hwe4G1zxpr/JZu6+jLrW
-----END CERTIFICATE-----
subject=/C=US/ST=MyState/L=MyTown/O=MyOrganization/OU=FOR TESTING
ONLY/CN=host
issuer=/C=US/ST=MyState/L=MyTown/O=MyOrganization/OU=FOR TESTING
ONLY/CN=CertGenCAB
---
No client certificate CA names sent
---
SSL handshake has read 625 bytes and written 236 bytes
---
New, TLSv1/SSLv3, Cipher is RC4-MD5
Server public key is 512 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher   : RC4-MD5
    Session-ID: 23E20BCAA4BC780CE20DE198CE2DFEE4
    Session-ID-ctx:
    Master-Key:
4C6F8E9B9566C2BAF49A4FD91BE90DC51F1E43A238B03EE9B700741AC7F4B41C72D2990648DE103
BB73B3074888E1D91
    Key-Arg : None
    Start Time: 1238539378
    Timeout : 300 (sec)
    Verify return code: 21 (unable to verify the first certificate)
---

```

2. Copy and paste the Server Certificate including the surrounding -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines. Save the certificate into a new file. For example:

```
/tmp/host.pem:
```

```

-----BEGIN CERTIFICATE-----
MIIB6zCCAZUCEItVMwHDFXAnYG//RoVbXQgwdQYJKoZIhvcNAQEEBQAweTELMakG
A1UEBhmCVVMxEDAObgNVBAgTB015U3RhdGUxZDZANBgNVBAcTBk15VG93bjEXMBUG
A1UEChMOTXlPcmdhbm16YXRpb24xGTAXBgNVBAsTEEZPUIBURVNUSU5HIE90TFkx
EzARBgNVBAMTCkNlcnRHZW5DQUIwHhcNMDkwMzI5MjM0NDM0WhcNMjQwMzZmMjM0
NDM0WjB5MQswCQYDVQGEwJVUzEQMA4GA1UECBYHTXlTdGF0ZTEPMA0GA1UEBxYG
TXlUb3duMRcwFQYDVQKFg5NeU9yZ2FuaXphdGlvbWZEMBCGA1UECXYQRk9SIFRF
U1RJTkcwT05MWTETMBEGA1UEAxYKZGFkdm1jMDAyMjBcMA0GCSqGSIb3DQEBAQUA
A0sAMEgCQQCmxv+h8kzOc2xyjMCDPM6By5LY0Vlp4vzWFKmPgEYtp6Wd87sG+YDB
PeFOz210XXGMx6F/14/yFlpCplmazWkDagMBAAEwDQYJKoZIhvcNAQEEBQADQQBn
uF/s6EqCT38Aw7h/406uPhNh6LUF7XH7QzmRv3J1sCqxRnA/fk3JCXE1shv1Pk8G
hwe4G1zxpr/JZu6+jLrW
-----END CERTIFICATE-----

```

3. Import the certificate into the local JVM certificate store. You will need the keystore password. For example (the password is `changeit`):

```
sudo /opt/java/jdk1.6.0_12/bin/keytool -import -alias host -keystore
/opt/java/jdk1.6.0_12/jre/lib/security/cacerts -trustcacerts -file
/tmp/host.pem

Enter keystore password: changeit
Owner: CN=host, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown,
ST=MyState, C=US
Issuer: CN=CertGenCAB, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown,
ST=MyState, C=US
Serial number: -74aaccfe3cea8fd89f9000b97aa4a2f8
Valid from: Sun Mar 29 16:44:34 PDT 2009 until: Sat Mar 30 16:44:34 PDT 2024
Certificate fingerprints:
    MD5:  94:F9:D2:45:7F:0D:E3:87:CF:2B:32:7C:BF:97:FF:50
    SHA1: A8:A5:89:8B:48:9B:98:34:70:56:11:01:5C:14:32:AC:CB:18:FF:1F
    Signature algorithm name: MD5withRSA
    Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

16.3 Configuring WebCenter Content for Single Sign-On

You can configure one of these single sign-on (SSO) solutions for Oracle WebCenter Content:

- Oracle Access Manager 11g
- Oracle Access Manager 10g
- Oracle Single Sign-On (OSSO)
- Windows Native Authentication (WNA)

Oracle Access Manager (OAM) is the recommended single sign-on (SSO) solution for Oracle Fusion Middleware enterprise-class installations including WebCenter Content. OAM is part of Oracle's suite of enterprise-class products for identity management and security.

If your enterprise-class installation uses Microsoft desktop logins that authenticate with a Microsoft domain controller with user accounts in Active Directory, then configuring Windows Native Authentication (WNA) single sign-on may be an option. For more information about WNA, see [Configuring WebCenter Content and Single Sign-On for Windows Native Authentication](#).

For an overview of Oracle WebLogic Server authentication providers, see *Configuring Authentication Providers in Administering Security for Oracle WebLogic Server*.

Note:

WebDAV (`/dav`) is protected by basic authentication per WebDAV protocol and is not protected by SSO, which typically requires form-based login. If you want to use a custom SSO solution for WebDAV, then a custom component is necessary.

Configuration information is provided in the following sections:

- [Configuring Oracle Access Manager 14c with WebCenter Content](#)
- [Configuring Oracle Access Manager 12c with WebCenter Content](#)

- [Configuring Oracle Access Manager 11g with WebCenter Content](#)
- [Configuring Oracle Access Manager 10g with WebCenter Content](#)
- [Configuring Oracle Single Sign-On for WebCenter Content](#)
- [Configuring the First Authentication Provider](#)
- [Configuring the WebCenter Content URL for Single Sign-On](#)
- [Configuring WebCenter Content and Single Sign-On for Windows Native Authentication](#)

16.3.1 Configuring Oracle Access Manager 14c with WebCenter Content

This section describes how to integrate WebCenter Content with Oracle Access Manager (OAM) 14c. Configuration information is provided for Oracle WebCenter Content: Content Server (CS), Oracle WebCenter Content: Inbound Refinery (IBR), and Oracle WebCenter Content: Site Studio (SS).

1. Configure OAM 14c, Oracle HTTP Server (OHS), and WebGate as described in *Administrator's Guide for Oracle Access Management for All Platforms*.
 - a. Append entries to the `mod_wl_ohs.conf` file to add WebCenter Content Uniform Resource Identifiers (URIs) to forward. Use the appropriate location entries from the following example. Each entry in the example maps the incoming path to the appropriate Oracle WebLogic Server on which the corresponding application resides.

In the following list of entries, *hostname* represents the name of the computer hosting the Content Server, and *portnumber* represents the port number of the Oracle WebLogic Server on which the corresponding applications resides. Replace *hostname* and *portnumber* with your system's host name and port name.

Note:

The URIs you forward depend on the WebCenter Content functionality that you have installed. Use the appropriate location entry for your functionality. For example: `/cs`, `/adfAuthentication`, `/_ocsh`, `/ibr`.

For Site Studio, the URI to forward is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to append a location entry for `/mysite`.

Caution:

The Content Server location `/cs` can be customized, so the `/cs` designation can't guarantee that HTTP requests will include the correct location. If `/cs` has been changed, then forward the location the administrator has configured.

```
# Content Server
<Location /cs>
    SetHandler weblogic-handler
    WebLogicHost <hostname>
    WebLogicPort <portnumber>
</Location>
```

```
# Content Server authentication
<Location /adfAuthentication>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# WebCenter online help
<Location /_ocsh>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# IBR
<Location /ibr>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# SS
<Location /customer-configured-site-studio>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>
```

- b. Use the OAM 14c remote registration tool (`oamreg`) to register an OAM Agent, specifying Oracle WebCenter Content URIs to protect and to make public.

See *Administrator's Guide for Oracle Access Management for All Platforms*.

 **Note:**

The URIs you protect and make public depend on the WebCenter Content functionality that you have installed: Content Server (CS), Inbound Refinery (IBR), Site Studio (SS).

For Site Studio, the URI to protect is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to specify the URI `/mysite`.

Functionality	Type	URI
CS	Protect	<code>/adfAuthentication</code>
CS	Public	<code>/cs</code>
CS	Public	<code>/_ocsh</code>
IBR	Protect	<code>/ibr/adfAuthentication</code>
IBR	Public	<code>/ibr</code>
SS	Protect	<code>/customer_configured_site_studio</code>

- c. Add the URL `/oamssso/logout.html` to the logout URL setting for the AccessGate so the single sign-on logout works properly. See *Configuring Centralized Logout* for

Sessions Involving OAM WebGates in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

2. Configure the WebCenter Content domain by ensuring you perform these tasks.
 - a. Configure the OAM Identity Asserter. The control flag for the OAM Identity Asserter must be set to `REQUIRED`, and both `OAM_REMOTE_USER` and `ObSSOCookie` must be selected as Active Types.
 - b. Configure the Authentication provider. This is necessary to specify the external LDAP server for the user store, such as Oracle Internet Directory (OID) or Oracle Virtual Directory (OVD), to match the LDAP server used by OAM. For example, if OAM is using OID, then an OID Authentication provider must be added to the WebCenter Content domain.

 **Note:**

When you configure the Oracle WebLogic Server for WebCenter Content to use an authentication provider other than the default one, ensure that it is the first authentication provider listed in the security realm configuration; otherwise, WebCenter Content will fail to load any user privileges. You can re-order the authentication providers so the new authentication provider is listed before the `DefaultAuthenticator` provider. Also ensure that the `DefaultAuthenticator` control flag is set to `SUFFICIENT`. For more information, see [Configuring the First Authentication Provider](#).

- c. Configure the OPSS (OAM) Single Sign-On provider.
3. After installing and configuring OAM 14c, check that you can access all of the configured applications, and that the login is giving you access to all of your configured applications without prompting you to sign in again. Also test global logout where available and make sure you are logged out of all other related applications.

16.3.2 Configuring Oracle Access Manager 12c with WebCenter Content

This section describes how to integrate WebCenter Content with Oracle Access Manager (OAM) 12c. Configuration information is provided for Oracle WebCenter Content: Content Server (CS), Oracle WebCenter Content: Inbound Refinery (IBR), and Oracle WebCenter Content: Site Studio (SS).

1. Configure OAM 12c, Oracle HTTP Server (OHS), and WebGate as described in *Administrator's Guide for Oracle Access Management for All Platforms*.
 - a. Append entries to the `mod_wl_ohs.conf` file to add WebCenter Content Uniform Resource Identifiers (URIs) to forward. Use the appropriate location entries from the following example. Each entry in the example maps the incoming path to the appropriate Oracle WebLogic Server on which the corresponding application resides.

In the following list of entries, *hostname* represents the name of the computer hosting the Content Server, and *portnumber* represents the port number of the Oracle WebLogic Server on which the corresponding applications resides. Replace *hostname* and *portnumber* with your system's host name and port name.

 **Note:**

The URIs you forward depend on the WebCenter Content functionality that you have installed. Use the appropriate location entry for your functionality. For example: `/cs`, `/adfAuthentication`, `/_ocsh`, `/ibr`.

For Site Studio, the URI to forward is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to append a location entry for `/mysite`.

 **Caution:**

The Content Server location `/cs` can be customized, so the `/cs` designation can't guarantee that HTTP requests will include the correct location. If `/cs` has been changed, then forward the location the administrator has configured.

```
# Content Server
<Location /cs>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# Content Server authentication
<Location /adfAuthentication>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# WebCenter online help
<Location /_ocsh>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# IBR
<Location /ibr>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# SS
<Location /customer-configured-site-studio>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>
```

- b. Use the OAM 12c remote registration tool (`oamreg`) to register an OAM Agent, specifying Oracle WebCenter Content URIs to protect and to make public.

See *Administrator's Guide for Oracle Access Management for All Platforms*.

 **Note:**

The URIs you protect and make public depend on the WebCenter Content functionality that you have installed: Content Server (CS), Inbound Refinery (IBR), Site Studio (SS).

For Site Studio, the URI to protect is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to specify the URI `/mysite`.

Functionality	Type	URI
CS	Protect	<code>/adfAuthentication</code>
CS	Public	<code>/cs</code>
CS	Public	<code>/_ocsh</code>
IBR	Protect	<code>/ibr/adfAuthentication</code>
IBR	Public	<code>/ibr</code>
SS	Protect	<code>/customer_configured_site_studio</code>

- c. Add the URL `/oamssso/logout.html` to the logout URL setting for the AccessGate so the single sign-on logout works properly. See *Configuring Centralized Logout for Sessions Involving OAM WebGates in Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
2. Configure the WebCenter Content domain by ensuring you perform these tasks.
 - a. Configure the OAM Identity Asserter. The control flag for the OAM Identity Asserter must be set to `REQUIRED`, and both `OAM_REMOTE_USER` and `ObSSOCookie` must be selected as Active Types.
 - b. Configure the Authentication provider. This is necessary to specify the external LDAP server for the user store, such as Oracle Internet Directory (OID) or Oracle Virtual Directory (OVD), to match the LDAP server used by OAM. For example, if OAM is using OID, then an OID Authentication provider must be added to the WebCenter Content domain.

 **Note:**

When you configure the Oracle WebLogic Server for WebCenter Content to use an authentication provider other than the default one, ensure that it is the first authentication provider listed in the security realm configuration; otherwise, WebCenter Content will fail to load any user privileges. You can re-order the authentication providers so the new authentication provider is listed before the `DefaultAuthenticator` provider. Also ensure that the `DefaultAuthenticator` control flag is set to `SUFFICIENT`. For more information, see [Configuring the First Authentication Provider](#).

- c. Configure the OPSS (OAM) Single Sign-On provider.

3. After installing and configuring OAM 12c, check that you can access all of the configured applications, and that the login is giving you access to all of your configured applications without prompting you to sign in again. Also test global logout where available and make sure you are logged out of all other related applications.

16.3.3 Configuring Oracle Access Manager 11g with WebCenter Content

This section describes how to integrate WebCenter Content with Oracle Access Manager (OAM) 11g. Configuration information is provided for Oracle WebCenter Content: Content Server (CS), Oracle WebCenter Content: Inbound Refinery (IBR), and Oracle WebCenter Content: Site Studio (SS).

Before you can configure OAM 11g, install the software using the instructions provided in *Installing and Configuring Oracle Identity Management in Oracle Fusion Middleware Installation Guide for Oracle Identity Management*, 11g Release 1 (11.1.1.9.0).

1. Configure OAM 11g, Oracle HTTP Server (OHS), and WebGate as described in *Administrator's Guide for Oracle Access Management for All Platforms*.
 - a. Append entries to the `mod_wl_ohs.conf` file to add WebCenter Content Uniform Resource Identifiers (URIs) to forward. Use the appropriate location entries from the following example. Each entry in the example maps the incoming path to the appropriate Oracle WebLogic Server on which the corresponding application resides.

In the following list of entries, *hostname* represents the name of the computer hosting the Content Server, and *portnumber* represents the port number of the Oracle WebLogic Server on which the corresponding applications resides. Replace *hostname* and *portnumber* with your system's host name and port name.

Note:

The URIs you forward depend on the WebCenter Content functionality that you have installed. Use the appropriate location entry for your functionality. For example: `/cs`, `/adfAuthentication`, `/_ocsh`, `/ibr`.

For Site Studio, the URI to forward is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to append a location entry for `/mysite`.

Caution:

The Content Server location `/cs` can be customized, so the `/cs` designation can't guarantee that HTTP requests will include the correct location. If `/cs` has been changed, then forward the location the administrator has configured.

```
# Content Server
<Location /cs>
    SetHandler weblogic-handler
    WebLogicHost <hostname>
    WebLogicPort <portnumber>
</Location>
```

```
# Content Server authentication
<Location /adfAuthentication>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# WebCenter online help
<Location /_ocsh>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# IBR
<Location /ibr>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# SS
<Location /customer-configured-site-studio>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>
```

- b. Use the OAM 11g remote registration tool (`oamreg`) to register an OAM Agent, specifying Oracle WebCenter Content URIs to protect and to make public. See *Administrator's Guide for Oracle Access Management for All Platforms*.

 **Note:**

The URIs you protect and make public depend on the WebCenter Content functionality that you have installed: Content Server (CS), Inbound Refinery (IBR), Site Studio (SS).

For Site Studio, the URI to protect is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to specify the URI `/mysite`.

Functionality	Type	URI
CS	Protect	<code>/adfAuthentication</code>
CS	Public	<code>/cs</code>
CS	Public	<code>/_ocsh</code>
IBR	Protect	<code>/ibr/adfAuthentication</code>
IBR	Public	<code>/ibr</code>
SS	Protect	<code>/customer_configured_site_studio</code>

- c. Add the URL `/oamssso/logout.html` to the logout URL setting for the AccessGate so the single sign-on logout works properly. See [Configuring Centralized Logout for OAM](#)

[11g](#) in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*, 11g Release 1 (11.1.1).

2. Configure the WebCenter Content domain by ensuring you perform these tasks.
 - a. Configure the OAM Identity Asserter. The control flag for the OAM Identity Asserter must be set to `REQUIRED`, and both `OAM_REMOTE_USER` and `ObSSOCookie` must be selected as Active Types.
 - b. Configure the Authentication provider. This is necessary to specify the external LDAP server for the user store, such as Oracle Internet Directory (OID) or Oracle Virtual Directory (OVD), to match the LDAP server used by OAM. For example, if OAM is using OID, then an OID Authentication provider must be added to the WebCenter Content domain.

 **Note:**

When the Oracle WebLogic Server domain for WebCenter Content is configured to use a different authentication provider than the `DefaultAuthenticator` provider, the new authentication provider must be the first authentication provider listed in the security realm configuration, or WebCenter Content will fail to load any user privileges. Make sure to re-order the authentication providers so the new authentication provider is listed before the `DefaultAuthenticator` provider. Also ensure that the `DefaultAuthenticator` control flag is set to `SUFFICIENT`. For more information, see [Configuring the First Authentication Provider](#).

- c. Configure the OPSS (OAM) Single Sign-On provider.
3. After installing and configuring OAM 11g, check that you can access all of the configured applications, and that the login is giving you access to all of your configured applications without prompting you to sign in again. Also test global logout where available and make sure you are logged out of all other related applications.

16.3.4 Configuring Oracle Access Manager 10g with WebCenter Content

This section describes how to integrate WebCenter Content with Oracle Access Manager (OAM) 10g. Configuration information is provided for Oracle WebCenter Content Server (CS), Oracle WebCenter Content: Inbound Refinery (IBR), and Oracle WebCenter Content: Site Studio (SS).

Before you can configure OAM, install the software. See information on OAM integration in *Enterprise Deployment Guide for Oracle WebCenter Content*.

1. Configure OAM 10g, Oracle HTTP Server (OHS), and WebGate.
 - a. Append entries to the `mod_wl.conf` file to add WebCenter Content Uniform Resource Identifiers (URIs) to forward. Use the appropriate location entries from the following example. The entries in the following `Location` list map the incoming paths to the appropriate Oracle WebLogic Server on which the corresponding applications reside.

In the following list of entries, *hostname* represents the name of the computer hosting the Content Server, and *portnumber* represents the port number of the Oracle WebLogic Server on which the corresponding applications resides. Replace *hostname* and *portnumber* with your system's host name and port name.

 **Note:**

The URIs you forward depend on the WebCenter Content functionality that you have installed. Use the appropriate location entry for your functionality. For example: `/cs`, `/adfAuthentication`, `/_ocsh`, `/ibr`.

For Site Studio, the URI to forward is defined by the customer. For example, if the site is accessed as `/mysite`, then you need to append a location entry for `/mysite`.

 **Caution:**

The Content Server location `/cs` can be customized, so the `/cs` designation can't guarantee that HTTP requests will include the correct location. If `/cs` has been changed, then forward the location the administrator has configured.

```
# Content Server
<Location /cs>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# Content Server authentication
<Location /adfAuthentication>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# WebCenter online help
<Location /_ocsh>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# IBR
<Location /ibr>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portnumber>
</Location>

# SS
<Location /customer-configured-for-site-studio>
  SetHandler weblogic-handler
  WebLogicHost <hostname>
  WebLogicPort <portname>
</Location>
```

- b. Use the OAM 10g configuration tool (OAMCfgTool) to specify WebCenter Content URIs to protect.

The OAM Configuration tool is a command-line utility you can use to launch a series of scripts to request information and set up the required profiles and policies in OAM.

 **Note:**

The URIs you protect depend on the WebCenter Content functionality that you have installed: Oracle WebCenter Content (CS), Inbound Refinery (IBR), Site Studio (SS).

For Site Studio, the URI to protect is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to specify the URI `/mysite`.

Functionality	URI
CS	<code>/adfAuthentication</code>
IBR	<code>/ibr/adfAuthentication</code>
SS	<code>/customer_configured_site_studio</code>

 **Note:**

If the URL for WebCenter Content does not link correctly after completing the OAM configuration, you might need to change the server host and server port values. For more information, see [Configuring the WebCenter Content URL for Single Sign-On](#).

- c. Configure the WebGate to handle the `end_url` in order to complete the setup for OAM global logout. Without this additional configuration, you are logged out, but not redirected to the end URL because `end_url` is not processed.
- d. Add the URL `/oamssso/logout.html` to the logout URL setting for the AccessGate so the single sign-on logout works properly. See [Configuring Centralized Logout for OAM 11g](#) in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*, 11g Release 1 (11.1.1).

 **Note:**

Deploying WebCenter Content version 11gR1 in an environment using OAM version 10g requires additional configuration to process logout requests properly.

- 2. Configure the WebCenter Content domain by performing the following tasks.
 - a. Configure the OAM Identity Asserter. The control flag for the OAM Identity Asserter must be set to `REQUIRED`.
 - b. Configure the Authentication provider. This is necessary to specify the external LDAP server for the user store, such as Oracle Internet Directory (OID) or Oracle Virtual Directory (OVD), to match the LDAP server used by OAM. For example, if OAM is using OID, then an OID Authentication provider must be added to the Oracle WebCenter Content domain.

 **Note:**

When the Oracle WebLogic Server domain for WebCenter Content is configured to use a different authentication provider than the `DefaultAuthenticator` provider, the new authentication provider must be the first authentication provider listed in the security realm configuration, or WebCenter Content will fail to load any user privileges. Make sure to re-order the authentication providers so the new authentication provider is listed before the `DefaultAuthenticator` provider. Also ensure that the `DefaultAuthenticator` control flag is set to `SUFFICIENT`. For more information, see [Configuring the First Authentication Provider](#).

- c. Configure the OPSS (OAM) Single Sign-On provider.
3. After installing and configuring OAM 10g, check that you can access all of the configured applications, and that the login is giving you access to all of your configured applications without prompting you to sign in again. Also test global logout where available and make sure you are logged out of all other related applications.

16.3.5 Configuring Oracle Single Sign-On for WebCenter Content

Oracle Single Sign-On (OSSO) is part of the 14c Oracle Application Server suite. OSSO is an enterprise-level single sign-on solution that works with the application server in conjunction with Oracle Internet Directory and Oracle HTTP Server (OHS) 14c.

If OSSO is already in place as the enterprise solution for your existing Oracle deployment, Oracle Fusion Middleware continues to support the existing OSSO as a solution. However, Oracle recommends that you consider upgrading to OAM 14c Single Sign-On solution.

This section provides information for integrating WebCenter Content with OSSO. Configuration information is provided for Oracle WebCenter Content Server (CS), Oracle WebCenter Content: Inbound Refinery (IBR), and Oracle WebCenter Content: Site Studio (SS).

Before you can configure OSSO, ensure that the software is installed. OSSO and Oracle Delegated Administration Service are not part of the 11g release. Customers must download the 10.1.4.* versions of these products, which are compatible with 11g Oracle Internet Directory and Oracle Directory Integration Platform, to form what was known in 10g as the Application Server Infrastructure. For deployment instructions on these 10g products, read "Installing and Configuring JAZN-SSO/DAS" in the *Oracle Application Server Enterprise Deployment Guide* (B28184-02) for Oracle Identity Management release 10.1.4.0.1. This manual is available on Oracle Technology Network at:

http://download.oracle.com/docs/cd/B28196_01/core.1014/b28184/toc.htm

1. Configure OSSO.
 - a. Append WebCenter Content Uniform Resource Identifier (URI) entries to the `mod_wl_ohs.conf` file. Use the appropriate location entries from the following example. Each entry in the example maps the incoming path to the appropriate Oracle WebLogic Server on which the corresponding application resides.

In the following list of entries, *hostname* represents the name of the computer hosting the Content Server, and *portnumber* represents the port number of the Oracle WebLogic Server on which the corresponding applications resides. Replace *hostname* and *portnumber* with your system's host name and port name.

 **Note:**

The URIs you forward depend on the WebCenter Content functionality that you have installed. Use the appropriate location entry for your functionality. For example: `/cs`, `/adfAuthentication`, `/_ocsh`, `/ibr`.

For Site Studio, the URI to forward is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to append a location entry for `/mysite`.

 **Caution:**

The Content Server location `/cs` can be customized, so the `/cs` designation can't guarantee that HTTP requests will include the correct location. If `/cs` has been changed, then forward the location the administrator has configured.

```
# Content Server
<Location /cs>
    SetHandler weblogic-handler
    WebLogicHost <hostname>
    WebLogicPort <portnumber>
</Location>

# Content Server authentication
<Location /adfAuthentication>
    SetHandler weblogic-handler
    WebLogicHost <hostname>
    WebLogicPort <portnumber>
</Location>

# WebCenter online help
<Location /_ocsh>
    SetHandler weblogic-handler
    WebLogicHost <hostname>
    WebLogicPort <portnumber>
</Location>

# IBR
<Location /ibr>
    SetHandler weblogic-handler
    WebLogicHost <hostname>
    WebLogicPort <portnumber>
</Location>

# SS
<Location /customer-configured-site-studio>
    SetHandler weblogic-handler
    WebLogicHost <hostname>
    WebLogicPort <portnumber>
</Location>
```

- b. Modify the `mod_osso.conf` file (at `ORACLE_HOME/ohs/conf/`) to include WebCenter Content Uniform Resource Identifiers (URIs) to protect.

 **Note:**

The URIs you protect depend on the WebCenter Content functionality that you have installed: Content Server (CS), Inbound Refinery (IBR), and Site Studio (SS).

For Site Studio, the URI to protect is configured by the customer. For example, if the site is accessed as `/mysite`, then you need to specify the URI `/mysite`.

Functionality	URI
CS	<code>/adfAuthentication</code>
IBR	<code>/ibr/adfAuthentication</code>
SS	<code>/customer_configured_site_studio</code>

2. Configure the WebCenter Content domain by ensuring you perform these tasks.
 - a. Add and configure the OSSO Identity Asserter for the Oracle WebLogic Server for WebCenter Content. Oracle recommends the following Authentication Providers: OSSO Identity Asserter, OID Authenticator, Default Authenticator.

The OID Authenticator provider is for the Oracle Internet Directory server, which is used in production-level systems. The Default Authenticator provider is for the Oracle WebLogic Server embedded LDAP server.

Ensure that `OSSOIdentityAsserter` is set as the primary provider authenticator for the domain, so that user profiles can be retrieved from the associated Oracle Internet Directory server. If necessary, reorder the providers so they appear in the following order, with control flags set as listed:

OSSOIdentityAsserter (REQUIRED)

OIDAuthenticator (SUFFICIENT)

DefaultAuthenticator (SUFFICIENT)

 **Note:**

When the Oracle WebLogic Server domain for WebCenter Content is configured to use a different authentication provider than the `DefaultAuthenticator` provider, the new authentication provider must be the first authentication provider listed in the security realm configuration, or WebCenter Content will fail to load any user privileges. Make sure to re-order the authentication providers so the new authentication provider is listed before the `DefaultAuthenticator` provider. Also ensure that the `DefaultAuthenticator` control flag is set to `SUFFICIENT`. For more information, see [Configuring the First Authentication Provider](#).

- b. Configure the Authentication provider. This is necessary to specify the external LDAP server for the user store, such as Oracle Internet Directory (OID) or Oracle Virtual Directory (OVD), to match the LDAP server used by OAM. For example, if OSSO is using OID, then an OID Authentication provider must be added to the WebCenter Content domain.

 **Note:**

If the URL for WebCenter Content does not link correctly after completing the OSSO configuration, you might need to change the server host and server port values. For more information, see [Configuring the WebCenter Content URL for Single Sign-On](#).

16.3.6 Configuring the First Authentication Provider

When the Oracle WebLogic Server domain for WebCenter Content is configured to use an authentication provider other than its default authentication provider for user authentication (such as Oracle Internet Directory or another LDAP provider), the primary provider must be the *first* authentication provider listed in the security realm configuration, or login authentication will fail.

If the primary provider is not listed first (for example, it is listed below the Oracle WebLogic Server provider, `DefaultAuthenticator`), then WebCenter Content will fail to successfully load users' Group membership and therefore fail to load any user privileges. You can use the Oracle WebLogic Server Administration Console to change the order in which the configured authentication providers are called. See *Configuring Authentication Providers* in *Administering Security for Oracle WebLogic Server*.

 **Note:**

When you use Oracle Internet Directory, all WebCenter Content administrator and other users must be defined in Oracle Internet Directory.

 **Note:**

Content Server assigns a Content Server administrator role to administrative users defined in the internal Oracle WebLogic Server user store. This is true regardless of whether Oracle Internet Directory is used or not used. However, if you use Oracle Internet Directory and the Oracle Internet Directory Authentication provider is *not* listed first, then any request by the Content Server instance to retrieve the roles of the Oracle WebLogic Server defined administrative users will fail.

 **Note:**

As of 11g Release 1 (11.1.1.6.0) Oracle WebCenter Content supports use of the Oracle Virtual Directory library (libOVD) feature, which enables a site to use multiple providers for login and group membership information. For example, it would be possible to use both Oracle Internet Directory (OID) and Active Directory as sources of user and role information. For more information about multi-LDAP configuration in Oracle WebLogic Server, see *Configuring the Service for Multiple LDAP using Fusion Middleware Control* in *Oracle Fusion Middleware Application Security Guide*.

16.3.7 Configuring the WebCenter Content URL for Single Sign-On

When you configure an Oracle application for use with Single Sign-On (SSO) and have set up Oracle Access Manager (OAM) or Oracle Single Sign-On (OSSO), the WebCenter Content `GET_ENVIRONMENT` service provides the server name, server port, and relative webroot to the application service call (for example, the WebCenter Content Doclib service). However, the values provided by `GET_ENVIRONMENT` might not be correct for your SSO configuration.

If you want to redirect the application service to use the OHS server host and server port (because both OAM and OSSO solutions require front-end applications with OHS), you must modify the Content Server host and server port configuration values.

You can use either of the following two methods to modify the Content Server host and server port values:

- Use the Oracle WebLogic Server Administration Console.
- Use the WebCenter Content standalone System Properties application.
 1. Go to the WebCenter Content domain directory.
 2. Change the directory to **ucm/cs/bin**
 3. Run the standalone application: **./SystemProperties**
 4. In the System Properties window, select the Internet tab.
 5. Update the HTTP Server address to the OHS (or Load Balancer) server host and server port values.
 6. Exit the System Properties window.
 7. Restart the Oracle WebLogic Server domain.

16.3.8 Configuring WebCenter Content and Single Sign-On for Windows Native Authentication

Setting up WebCenter Content and single sign-on (SSO) with Microsoft clients for Windows Native Authentication (WNA) requires configuring the Microsoft Active Directory, the client, and the Oracle WebLogic Server domain. Details including system requirements for SSO with Microsoft clients are provided in *Configuring Single Sign-On with Microsoft Clients in Administering Security for Oracle WebLogic Server*.

As part of configuring SSO with Microsoft clients, you must specify a LDAP authentication provider to access the external Microsoft Active Directory. Oracle WebLogic Server offers the Active Directory Authentication provider. See *Configuring LDAP Authentication Providers in Administering Security for Oracle WebLogic Server*.

 **Note:**

When the Oracle WebLogic Server domain for WebCenter Content is configured to use a different authentication provider than the DefaultAuthenticator provider, the new authentication provider must be the first authentication provider listed in the security realm configuration, or WebCenter Content will fail to load any user privileges. Make sure to re-order the authentication providers so the new authentication provider is listed before the DefaultAuthenticator provider. Also ensure that the `DefaultAuthenticator` control flag is set to `SUFFICIENT`. For more information, see [Configuring the First Authentication Provider](#).

As part of configuring SSO with Microsoft clients, you must configure the Negotiate Identity Assertion provider in Oracle WebLogic Server security realm. The identity assertion provider decodes Simple and Protected Negotiate (SPNEGO) tokens to obtain Kerberos tokens, validates the Kerberos tokens, and maps Kerberos tokens to WebLogic users. Use the Oracle WebLogic Server Administration Console to add a new provider in the appropriate security realm in the domain structure, assign it a name, then select **NegotiateIdentityAsserter** for its Type. Activate the changes and restart the Oracle WebLogic Server. Now your server can use the Kerberos ticket it receives from the browser.

You must redeploy each WebCenter Content application (Content Server, Inbound Refinery, Records) that will be used in the Windows Native Authentication (Kerberos) environment, using an associated deployment plan. A deployment plan is a XML document. Oracle provides a plan for each of the three WebCenter Content applications: [Example 16-1](#) and [Example 16-2](#). You also can implement a deployment plan using the Oracle WebLogic Scripting Tool.

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Deployments** in the Domain Structure navigation tree.
3. In the **Control** tab, click **Next** until you see the WebCenter Content deployment you want to change:
 - Oracle WebCenter Content Server
 - Oracle WebCenter Content: Inbound Refinery
 - Oracle WebCenter Content: Records
4. Select the check box to the left of the deployment to be changed.
5. Click **Update**.
6. Under the Deployment plan path, select **Change Path**.
7. Navigate to and select the appropriate plan file:
 - `cs-deployment-plan.xml` (for Content Server)
 - `ibr-deployment-plan.xml` (for Inbound Refinery)
8. Verify that **Redeploy this application using the following deployment files** is selected.
9. Click **Next**.
10. Click **Finish**.
11. To verify that SSO with Microsoft clients is configured properly, point a browser to the Microsoft Web application or Web service you want to use. If you are logged in to a Windows domain and have Kerberos credentials acquired from the Active Directory server in the domain, you should be able to access the Web application or Web service without providing a user name or password.

Example 16-1 cs-deployment-plan.xml

Use the provided `cs-deployment-plan.xml` file, or create a `.xml` file and name it **cs-deployment-plan.xml**.

```
<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan
  xmlns="http://xmlns.oracle.com/weblogic/deployment-plan"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.oracle.com/weblogic/deployment-plan http://xmlns.oracle.com/
weblogic/deployment-plan/1.0/deployment-plan.xsd"
  global-variables="false">
  <application-name>cs.ear</application-name>
  <variable-definition>
    <variable>
      <name>http-only</name>
      <value>false</value>
    </variable>
  </variable-definition>
  <module-override>
    <module-name>cs.war</module-name>
    <module-type>war</module-type>
    <module-descriptor external="false">
      <root-element>weblogic-web-app</root-element>
      <uri>WEB-INF/weblogic.xml</uri>
      <variable-assignment>
        <name>http-only</name>
        <xpath>/weblogic-web-app/session-descriptor/cookie-http-only</xpath>
      </variable-assignment>
    </module-descriptor>
  </module-override>
</deployment-plan>
```

Example 16-2 ibr-deployment-plan.xml

Use the provided `ibr-deployment-plan.xml` file, or create a `.xml` file and name it **ibr-deployment-plan.xml**.

```
<?xml version='1.0' encoding='UTF-8'?>
<deployment-plan xmlns="http://xmlns.oracle.com/weblogic/deployment-plan" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance" xsi:schemaLocation="http://xmlns.oracle.com/weblogic/deployment-plan http://
xmlns.oracle.com/weblogic/deployment-plan/1.0/deployment-plan.xsd" global-variables="false">
  <application-name>ibr.ear</application-name>
  <variable-definition>
    <variable>
      <name>http-only</name>
      <value>false</value>
    </variable>
  </variable-definition>
  <module-override>
    <module-name>ibr.war</module-name>
    <module-type>war</module-type>
    <module-descriptor external="false">
      <root-element>weblogic-web-app</root-element>
      <uri>WEB-INF/weblogic.xml</uri>
      <variable-assignment>
        <name>http-only</name>
        <xpath>/weblogic-web-app/session-descriptor/cookie-http-only</xpath>
      </variable-assignment>
    </module-descriptor>
  </module-override>
</deployment-plan>
```

16.4 Configuring Oracle Infrastructure Web Services

Oracle Infrastructure Web services provide the ability to create and attach policy sets to subjects on a global scope (domain, server, application, or SOA composite). Oracle Infrastructure Web services are implemented according to the Web services for Java EE 1.2 specification, which defines the standard Java EE runtime architecture for implementing Web services in Java. The specification also describes a standard Java EE Web service packaging format, deployment model, and runtime services, all of which are implemented by Oracle Infrastructure Web services.

16.5 Configuring WebCenter Content for Oracle Identity Cloud Service (IDCS)

Configure Single Sign-On with IDCS for WebCenter applications such as WebCenter Content Server, Enterprise Capture (console and client), WebCenter Desktop Client, WebCenter Content: Imaging, and WebCenter Content ADFUI.

Configuration information is provided in the following sections:

- [Updating SSL.hostnameVerifier Property](#)
- [Configuring IDCS Security Provider](#)
- [Configuring WebCenter Content for User Logout](#)

16.5.1 Updating SSL.hostnameVerifier Property

To update `SSL.hostnameVerifier` property, do the following:

 **Note:**

This is necessary for the IDCS provider to access IDCS.

1. Stop all the servers in the domain including Admin server and all managed Weblogic servers.
2. Update the `SSL.hostnameVerifier` property:
 - a. Create or modify the file `<DOMAIN_HOME>/<domain_name>/bin/setUserOverrides.sh`. Add the `SSL.hostnameVerifier` property for the IDCS Authenticator:

```
set EXTRA_JAVA_PROPERTIES=%EXTRA_JAVA_PROPERTIES%-  
Dweblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWi  
ldcardHostnameVerifier
```

- b. Alternatively, edit the file `<DOMAIN_HOME>/<domain name>/bin/setDomainEnv.sh`:

```
set EXTRA_JAVA_PROPERTIES=%EXTRA_JAVA_PROPERTIES% -  
Dweblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWi  
ldcardHostnameVerifier
```

3. Start the Admin server.

16.5.2 Configuring IDCS Security Provider

To obtain an OAuth client for IDCS Security Provider:

1. Log in to the IDCS admin console.
2. Create a trusted application. In the Add Confidential Application wizard:
 - a. Enter the client name and the description (optional).
 - b. Select the **Configure this application as a client now** option. To configure this application, expand the **Client Configuration** in the Configuration tab.
 - c. In the **Client Credentials** field, select the **Allowed Grant Types** check box.
 - d. In the Grant the client access to Identity Cloud Service Admin APIs section, click **Add** to add the application roles. You can add the *Identity Domain Administrator* role.
 - e. Keep the default settings for the pages and click **Finish**.
 - f. Record the Client ID and Client Secret.
This is needed when you will create the IDCS provider.
 - g. Activate the application.

16.5.2.1 Configuring Oracle Identity Cloud Integrator Provider

To configure Identity Cloud Integrator Provider:

1. Log in to the Weblogic Server Administration console.
2. Select **Security Realm** in the Domain Structure pane.
3. On the Summary of Security Realms page, select the name of the realm (for example, myrealm). Click **myrealm**.
The Settings for myrealm page appears.
4. On the Settings for Realm Name page, select **Providers** and then **Authentication**. To create a new Authentication Provider, in the Authentication Provider's table, click **New**.
5. In the Create a New Authentication Provider page, enter the name of the authentication provider, for example, *IDCSIntegrator* and select the **OracleIdentityCloudIntegrator** type of authentication provider from the drop-down list and click **OK**.
6. In the Authentication Provider's table, click the newly created Oracle Identity Cloud Integrator, *IDCSIntegrator* link.
7. In the Settings for IDCSIntegrator page, for the **Control Flag** field, select the **Sufficient** option from the drop-down list.
8. Go to the Provider Specific page to configure the additional attributes for the security provider. Enter the values for the following fields: **Host**, **Port**, select **SSLEnabled**, **Tenant**, **Client Id**, and **Client Secret**. Click **Save**.

 **Note:**

If IDCS URL is `idcs-abcde.identity.example.com`, then IDCS host would be `identity.example.com` and tenant name would be `idcs-abcde`.

9. Select **Security Realm**, then **myrealm**, and then **Providers**. In the Authentication Provider's table, click **Reorder**.
10. In the Reorder Authentication Providers page, move *IDCSIntegrator* on the top and click **OK**.
11. In the Authentication Provider's table, click the **DefaultAuthenticator** link. In the Settings for DefaultAuthenticator page, for the **Control Flag** field, select the **Sufficient** option from the drop-down list. Click **Save**.
12. All changes will be activated. Restart the Admin domain.

16.5.2.2 Setting Up Trust between IDCS and Weblogic

To set up trust between IDCS and Weblogic:

1. Import certificate in KSS store.
 - a. Run this from the Admin Server node.
 - b. Get IDCS certificate:

```
echo -n | openssl s_client -showcerts -servername <IDCS_HOST> -connect
<IDCS_HOST>:443|sed -ne '/-BEGIN CERTIFICATE-/,/-END
CERTIFICATE-/p' > /tmp/idcs_cert_chain.crt
```

Optionally, IDCS Certificates can be downloaded directly from any browser.

- c. Import certificate. Run <MW_HOME>/oracle_common/common/bin/wlst.sh file.

```
connect ("weblogic", "Welcome_1", "t3://<WEBLOGIC_HOST>:7001")
svc=getOpssService (name='KeyStoreService')
```

```
svc.importKeyStoreCertificate (appStripe='system', name='trust', password='
', alias='idcs_cert_chain', type='TrustedCertificate', filepath='/tmp/
idcs_cert_chain.crt', keypassword='')
syncKeyStores (appStripe='system', keystoreFormat='KSS')
```

- d. exit()
2. Restart the Admin server.

Note:

After creating the IDCS provider and importing the certificate, unlike the users in the *DefaultAuthenticator* and LDAP servers, the IDCS users will not be present in the User's list. To view the list of users, click **myrealm**, then **Users and Groups**, and then **Users**.

16.5.2.3 Creating Admin User in IDCS for WebCenter Content

It is important to create the Admin user in IDCS because once the managed servers are configured for SAML, the domain admin user (typically weblogic user) will not be able to log into the managed servers.

To create WLS Admin user in IDCS for WebCenter Content JaxWS connection:

1. Go to the Groups tab and create *Administrators* and *sysmanager* roles in IDCS.
2. Go to the Users tab and create a wls admin user, for example, *weblogic* and assign it to *Administrators* and *sysmanager* groups.
3. Restart all the managed servers.

This step is not required if WebCenter Content connection type is *socket* as socket type WebCenter Content connection uses *sysadmin* user, which is WebCenter Content internal user.

 **Note:**

This step is not required if WebCenter Content connection type is *socket* as socket type of UCM connection uses *sysadmin* user which is the WebCenter Content internal user.

4. Start all the managed Weblogic servers in domain.

16.5.2.4 Managing Group Memberships, Roles, and Accounts

Oracle Identity Cloud Service can be used for user log-in authentication and an external LDAP server (such as OID or Active Directory) can be used to get user group memberships.

For every user, the same user name will be required in both IDCS and the LDAP server. Oracle Identity Cloud Service can be used to provide the WCC user role and account group memberships.

This will require modifying OPSS and libOVD to access IDCS. The following steps are required if using IDCS for user authorization. Do not run these steps if you are using IDCS only for user authentication. Ensure that all the servers are stopped (including admin) before proceeding with the following steps:

- Run the following script:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh
```

 **Note:**

It's not required to connect to the port of the Admin server.

- Read the domain:

```
readDomain(<DOMAIN_HOME>)
```

- Add the template:

```
addTemplate("<MIDDLEWARE_HOME>/oracle_common/common/templates/wls/  
oracle.opss_scim_template.jar")
```

 **Note:**

This step may throw a warning, which can be ignored. The `addTemplate` is deprecated. Use `selectTemplate` followed by `loadTemplates` in place of `addTemplate`.

- Update the domain:

```
updateDomain()
```

- Close the domain:

```
closeDomain()
```

- Start the servers (Admin and managed).

16.5.3 Configuring WebCenter Content for User Logout

If the **Logout** link is selected, you will be re-authenticated by SAML. To be able to select the **Logout** link:

1. Log in to WebCenter Content as an administrator. Select **Administration**, then **Admin Server**, and then **General Configuration**.
2. In the Additional Configuration Variables pane, add the following parameter:

```
set EXTRA_JAVA_PROPERTIES=%EXTRA_JAVA_PROPERTIES%-
Dweblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWildc
ardHostnameVerifier
```

3. Click **Save**.
4. Restart the WebCenter Content Managed server(s).

16.5.3.1 Configuring Logout for WebCenter Content and WebCenter Content: Imaging

Complete the following steps for WebCenter Content and WebCenter Content: Imaging Logout to work:

1. Deselect **Enable Single Logout** under **SSO Configuration** for WebCenter Content: Imaging and WebCenter Content applications in IDCS admin console.
2. The cookie path should be set to / for WebCenter Content: Imaging in the `imaging.ear` file and it should be redeployed.
3. Set `IpmCustomLogoutURL` property for WebCenter Content: Imaging via MBean (under `oracle.imaging`) in EM to this value: `http://<IPM Host>:<IPM Port>/imaging/adfAuthentication?logout=true&end_url=https://<IDC Tenant id>.identity.oraclecloud.com/sso/v1/user/logout`
4. For WebCenter Content, specify the logout URL in the WebCenter Content configuration. Either update the `config.cfg` file or you can do it from the WebCenter Content Admin configuration page. Make the following entry and restart WebCenter Content: `LogoutServerUrl=http://<UCM Hostname>:<UCM Port>/adfAuthentication?`

```
logout=true&end_url=https://<IDC Tenant id>.identity.oraclecloud.com/sso/v1/  
user/logout
```

16.5.3.2 Configuring Logout for Enterprise Capture

Complete the following steps for Enterprise Capture Logout to work:

Go to Enterprise Manager Console, open MBean browser and change the Capture's MBean attribute `logoutRedirectURL` to `https://<IDCS Tenantid>.identity.oraclecloud.com/sso/v1/user/logout`. Save the changes. This change is effective immediately. To unset this attribute's value, put any empty string.

1. The cookie path of `/dc-client` and `/dc-console` should be set to `/` in the `capture.ear` file and it should be redeployed.
2. Go to the Enterprise Manager console, open the MBean browser and change the Capture's MBean attribute `logoutRedirectURL` to `https://<IDCS Tenantid>.identity.oraclecloud.com/sso/v1/user/logout`. Save the changes. This change is effective immediately. To unset this attribute's value, add an empty string.

16.5.3.3 Configuring Logout for ADFUI

For WebCenter Content ADFUI Logout feature to work, do the following:

1. Go to Enterprise Manager Console, open the System MBean browser.
2. Expand the Application Defined MBeans and `oracle.adf.share.config` and change the `WccAdfConfiguration` MBean attribute `customLogoutUrl` to <https://<IDCS Tenantid>.identity.oraclecloud.com/sso/v1/user/logout>.
3. Save the changes to the parent MBean by invoking the save operation.
4. This change is effective after restarting the UI server.

To unset the attribute's value, add any empty string.

16.6 Configuring SAML-Based Single Sign-On

Security Assertion Markup Language (SAML) enables cross-platform user authentication between web-based applications or web services in a WebLogic Server domain and web browsers or other HTTP clients. When users log in to a website of the application that is part of a single sign-on network, they automatically gain access to all the applications in that network without having to log in separately in to each application.

This section covers the following topics:

- [SAML Components](#)
- [SAML Single Sign-On Prerequisites](#)
- [Configuring SAML 1.1 Source Services](#)
- [Configuring SAML 1.1 Destination Services](#)
- [Configuring SAML 2.0 \(IDCS\) Single Sign-On](#)

16.6.1 SAML Components

A SAML-based single-sign on setup includes the following components:

- **SAML Credential Mapping:** The SAML Credential Mapping provider allows WebLogic Server to act as a source site for using SAML for single sign-on. This provider generates valid SAML 1.1 assertions for authenticated subjects based on the configuration of the target site or resource.
- **Inter Site Transfer Service (ITS):** An addressable component that generates identity assertions and transfers the user to the destination site.
- **Assertion Retrieval Service (ARS):** An addressable component that returns the SAML assertion corresponding to the artifact. You can allocate the assertion ID at the time of generating the assertion.
- **SAML Identify Asserter:** The SAML Identity Assertion provider allows the WebLogic Server to act as a destination site for using SAML for single sign-on. This provider processes valid SAML 1.1 assertions for authenticated subjects obtained from the source site or resource.
- **Assertion Consumer Service (ACS):** An addressable component that receives assertions and/or artifacts generated by ITS and uses them to authenticate users at the destination site.
- **SAML Relying Party:** A SAML Relying Party is an entity that relies on the information in a SAML assertion produced by the SAML source site. You can configure SAML assertions for each Relying Party or use the defaults established by the Federation Services source site configuration for producing assertions.
- **SAML Asserting Party:** A SAML Asserting Party is a trusted SAML Authority, which asserts security information in the form of SAML assertions.

16.6.2 SAML Single Sign-On Prerequisites

Before configuring SAML 1.1 source and destination services, you must do the following:

- **Create a domain with WebCenter Content and Portal servers:** Applicable for SAML configurations with Content Server as a source and Portal as a destination.
- **Create a domain with WebCenter Content and ADF UI servers:** Applicable for SAML configurations with Content Server as a source and Application Development Framework (ADF) as a destination.
- **Create a domain with WebCenter Content and Imaging servers:** Applicable for SAML configurations with Content Server as a source and Imaging as a destination.

The prerequisites for SAML-based SSO are described in the following topics:

- [Enabling SSL for Source Services](#)
- [Enabling SSL for Destination Services](#)
- [Creating and Exporting Certificates](#)
- [Hiding Login Area for WebCenter Portal Landing Page](#)

 **Note:**

The instructions assume that you have already installed WebCenter Content and associated components.

These port numbers are used for source, destination, and SSL as examples:

Source-SSL Ports:

CS: 16200, SSL: 16201

Destination-SSI Ports:

Portal: 8888, SSL: 8788

Imaging: 16000, SSL: 16001

ADF UI: 16225, SSL: 16226



Note:

You can configure the port numbers based on your requirement.

16.6.2.1 Enabling SSL for Source Services

To enable SSL for source services:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Environment** in the Domain Structure pane.
The Summary of Environment page appears.
3. Click **Servers**.
The Summary of Servers page appears.
4. Click **UCM_server1**.
The Settings for UCM_server1 page appears.
5. In the **Configurations > General** tab, provide the following details:
 - Select the **SSL Listen Port Enabled** check box.
 - In the **SSL Listen Port** field, Enter 16201.

16.6.2.2 Enabling SSL for Destination Services

To enable SSL for destination services, such as Portal, ADF UI, and Imaging servers:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Environment** in the Domain Structure pane.
The Summary of Environment page appears.
3. Click **Servers**.
The Summary of Servers page appears.
4. Click one of the following servers based on the destination service that you want to configure.
 - WC_Portal to configure Portal as the destination service.
 - WCCADF_server1 to configure ADF UI as the destination service.
 - IPM_server1 to configure Imaging as the destination service.
5. In the **Configurations > General** tab, select the **SSL Listen Port Enabled** check box.
6. In the **SSL Listen Port** field, enter one of the following values based on the destination service that you want to configure:
 - 8788 to configure Portal as the destination service.

- 16226 to configure ADF UI as the destination service.
- 16001 to configure Imaging as the destination service.

16.6.2.3 Creating and Exporting Certificates

To create and export certificates:

1. Open `oracle_common/common/bin` and launch `./wlst.sh`.
2. Connect to Admin Server of the source using the following `wlst` command:
 - `connect ('adminServerUsername', 'password', 'hostboxName:adminport/console')`.
3. List and export the certificates using following `wlst` commands:
 - `svc = getOpssService(name='KeyStoreService')`
 - `svc.listKeyStoreAliases(appStripe="system",name="demoidentity",password='DemoIdentityKeyStorePassPhrase',type="*")`
 - `svc.exportKeyStoreCertificate(appStripe='system',name='demoidentity',password='DemoIdentityKeyStorePassPhrase',alias='DemoIdentity',type='Certificate',filepath='/scratch/priyaaro/demoidentity.der')`
4. Remove the value *FORM* from the `<auth-method>` element of the `web.xml` file and retain the value *CLIENT-CERT* from all the destination servers.

The `web.xml` file paths for the destination servers are:

- **Portal:** `Oracle_Home/wcportal/archives/applications/webcenter.ear/spaces.war/WEB-INF/web.xml`
- **ADF UI:** `Oracle_Home/wccontent/wccadf/WccAdf.ear/WccAdf.war/WEB-INF/web.xml`
- **Imaging:** `ORACLE_HOME/wccontent/ipm/lib/imaging.ear/imaging-ui.war/WEB-INF/web.xml`

Note:

After modifying the `web.xml` file, you must redeploy the destination application.

16.6.2.4 Hiding Login Area for WebCenter Portal Landing Page

To hide the login area in the WebCenter Portal landing page:

1. Open `$(MIDDLEWARE_HOME)/user_projects/domains/domain_name/bin/setDomainEnv.sh` and update the following property:
 - `EXTRA_JAVA_PROPERTIES="-Doracle.webcenter.spaces.osso=true ${EXTRA_JAVA_PROPERTIES}"`
 - `export EXTRA_JAVA_PROPERTIES`
2. Restart the Portal Server.

16.6.3 Configuring SAML 1.1 Source Services

You can configure a Content Server instance to function as a SAML source site that provides an Intersite Transfer Service (ITS). A source site generates assertions that are conveyed to a destination site using one of the single sign-on profiles.

The section covers the following topics:

- [Creating Credential Mapping Providers](#)
- [Configuring Credential Mapping Providers](#)
- [Creating Relying Parties](#)
- [Configuring Relying Parties](#)
- [Defining Federation Services for Source](#)

16.6.3.1 Creating Credential Mapping Providers

To create the credential mapping providers:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Security Realms** in the Domain Structure pane.
The Summary of Security Realms page appears.
3. Click **myrealm**.
The Settings for myrealm page appears.
4. Click **Providers**, then **Credential Mapping**, and then **New**.
5. In the **Name** field, enter a name for the credential mapping provider. For example, `SAMLCredentialMapper`.
6. In the **Type** field, select **SAMLCredentialmapperV2**.
7. Click **OK**.

The credential mapper that you created is available in the Credential Mapping Providers section.

16.6.3.2 Configuring Credential Mapping Providers

To configure the provider-specific information:

1. Click the credential mapping provider created previously, for example `SAMLCredentialMapper`.
To create a credential mapping provider, see [Creating Credential Mapping Providers](#).
2. Click **Provider Specific**.
3. In the **Issuer URL** field, enter `http://www.oracle.com/webcenter`.
4. In the **Name Qualifier** field, enter `webcenter.com`.
5. In the **Default Time to Live** field, enter `120`.
6. In the **Default Time to Live Offset** field, enter `0`.
7. In the **Web Service Assertion Signing Key Alias** field, enter `Demoidentity`.

8. In the **Web Service Assertion Signing Key Pass Phrase** field, enter *DemolentityPassPhrase*.
9. In the **Confirm Credential** field, confirm the signing key pass phrase value by entering *DemolentityPassPhrase*.
10. Restart the WebCenter Content server.

16.6.3.3 Creating Relying Parties

To create a relying party:

1. Click the credential mapping provider created previously, for example *SAMLCredentialMapper*.

To create a credential mapping provider, see [Creating Credential Mapping Providers](#).

2. Click **Management**, then **Relying Parties**, and then **New**.
3. In the **Profile** field, select **Browser/POST**.
4. In the **Description** field, enter *relyingparty*.
5. Click **OK**.

A relying party with the partner ID *rp_00001* is created.

 **Note:**

The partner ID increments by 1 for every new relying party that you create. For example, *rp_00002*.

16.6.3.4 Configuring Relying Parties

To specify relying party information for destination services such as Portal, ADF UI, and Imaging servers:

1. Click the relying partner ID created previously, for example, *rp_00001*.

To create a relying party, see [Creating Relying Parties](#).

2. Select the **Enabled** check box.
3. In the **Target URL** field, enter one of the following values based on the destination service that you want to configure:
 - *http://hostboxname:8888/webcenter* to configure Portal as the destination service.
 - *http://hostboxname:16225/wcc* to configure ADF UI as the destination service.
 - *http://hostboxname:16007/imaging* to configure Imaging as the destination service.

 **Note:**

The preceding port numbers are used to configure the destination servers.

4. In the **Assertion Consumer URL** field, enter one of the following values based on the destination service you want to configure:
 - *https://hostboxname:8788/webcenter/samlacs/acs* to configure Portal as the destination service.

- *https://hostboxname:16226/wcc/samlacs/acs* to configure ADF UI as the destination service.
 - *https://hostboxname:16001/imaging/samlacs/acs* to configure Imaging as the destination service.
5. In the **Assertion Consumer Parameters** field, enter *APID=ap_00001*.
 6. In the **Assertion Time to Live** field, enter *0*.
 7. In the **Assertion Time To Live Offset** field, enter *0*.
 8. Select the **Sign Assertions** check box.
The **Include Keyinfo** check box is selected by default. Leave the check box as is.
 9. Click **Save**.

16.6.3.5 Defining Federation Services for Source

To define the federation services for source:

1. Click **Environment** in the Domain Structure pane.
The Summary of Environment page appears.
2. Click **Servers**.
The Summary of Servers page appears.
3. Click **UCM_server1**.
The Settings for UCM_server1 page appears.
4. Select the **Source Site Enabled** check box.
5. In the **Source Site URI** field, enter *http://hostboxname:16200*.
6. In the **Signing Key Alias** field, enter *Demoidentity*.
7. In the **Signing Key Passphrase** field, enter *DemoidentityPassPhrase*.
8. In the **Confirm Signing Key Passphrase** field, confirm the value by entering *DemoidentityPassPhrase*.
9. In the **Intersite Transfer URIs** field, enter the following:
/samlits_ba/its
/samlits_ba/its/post
/samlits_ba/its/artifact
/samlits_cc/its
/samlits_cc/its/post
/samlits_cc/its/artifact
10. Select the **ITS Requires SSL** check box.
11. In the **Assertion Retrieval URIs** field, enter */samlars/ars*.
12. Select the **ARS Requires SSL** check box.
13. Click **Save**.

16.6.4 Configuring SAML 1.1 Destination Services

To configure the SAML destination services, you must first configure a SAML Identity Asserter in the server's Security Realm. You can configure a WebLogic Server instance to function as a SAML destination site. A destination site receives SAML assertions and uses them to authenticate local subjects.

This section covers the following topics:

- [Creating Identity Asserters](#)
- [Adding Source Certificates](#)
- [Creating Asserting Parties](#)
- [Configuring Asserting Parties](#)
- [Defining Federation Services for Destination](#)

16.6.4.1 Creating Identity Asserters

To create identity asserters for destination services such as Portal, ADF UI, and Imaging:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Security Realms** in the Domain Structure pane.
The Summary of Security Realms page appears.
3. Click **myrealm**.
The Settings for myrealm page appears.
4. Click **Providers**, then **Authentication**, and then **New**.
The Create a New Authentication Provider page appears.
5. In the **Name** field, enter a name for the identity assenter. For example, `SAMLIdentityAsseter`.
6. In the **Type** field, select **SAMLIdentityAsserterV2**.
7. Click **Save**.
8. Restart one of the following servers based on the destination service that you want to configure:
 - Admin Server if you are configuring Portal as the destination service.
 - ADF UI server if you are configuring ADF UI as the destination service.
 - IPM server if you are configuring Imaging as the destination service.

16.6.4.2 Adding Source Certificates

To add a source certificate for the destination service:

1. Click the identity assenter created previously, for example, `SAMLIdentityAsseter`.
To create an identity assenter, see [Creating Identity Asserters](#).
2. Click **Management**, then **Certificates**, and then **New**.
3. In the **Alias** field, enter `demoidentity`.
4. In the **Path** field, enter the path where you have exported the source certificate.

5. Click **OK**.

16.6.4.3 Creating Asserting Parties

To create an asserting party:

1. Click the identity asserter created previously, for example, `SAMLIdentityAsseter`.
To create an identity asserter, see [Creating Identity Asserters](#).
2. Click **Management**, then **Asserting Parties**, and then **New**.
3. In the **Profile** field, select the value **Browser/POST**.
4. In the **Description** field, enter `assertingparty`.
5. Click **OK**.

An asserting party with the partner ID `ap_00001` is created.

16.6.4.4 Configuring Asserting Parties

To specify the asserting party information for destination services such as Portal, ADF UI, and Imaging servers:

1. Click the asserting partner ID created previously, for example, `ap_00001`.
To create an asserting party, see [Creating Asserting Parties](#).
2. Select the **Enabled** check box.
3. In the **Target URL** field, enter one of the following values based on the destination service that you want to configure:
 - `http://hostboxname:16200` to configure Portal as the destination service.
 - `http://hostboxname:16200` to configure ADF UI as the destination service.
 - `http://hostboxname:16200` to configure Imaging as the destination service.
4. In the **POST Signing Certificate Alias** field, enter `demoidentity`.
5. In the **Source Site Redirect URIs** field, enter one of the following values based on the destination service that you want to configure.
 - `/webcenter/adfAuthentication` to configure Portal as the destination service.
 - `/wcc/adfAuthentication` to configure ADF UI as the destination service.
 - `/imaging/faces/Pages/Welcome.jspx` to configure Imaging as the destination service.
6. In the **Source Site ITS URL** field, enter `https://hostboxname:16201/samlits_ba/its`.
7. In the **Source Site ITS Parameters** field, enter `RPID=rp_00001`.
8. In the **Issuer URI** field, enter `http://www.oracle.com/webcenter`.
9. In the **Assertion Signing Certificate** field, enter `demoidentity`.
10. Select the **Signature Required** check box.
11. Click **Save**.

16.6.4.5 Defining Federation Services for Destination

To define the federation services for a destination such as Portal, ADF UI, and Imaging:

1. Click **Environment** in the Domain Structure pane.

The Summary of Environment page appears.

2. Click **Servers**.

The Summary of Servers page appears.

3. Click one of the following servers based on the destination service that you want to configure.

- **WC_Portal** to configure Portal as the destination service.
- **WCCADF_server1** to configure ADF UI as the destination service.
- **IPM_server1** to configure Imaging as the destination service.

4. Click **Federation Services** and then **SAML 1.1 Destination Site**.

5. Select the **Destination Site Enabled** check box.

6. In the **Assertion Consumer URIs** field, enter one of the following values based on the destination service that you want to configure.

- `/webcenter/samlacs/acs` to configure Portal as the destination service.
- `/wcc/samlacs/acs` to configure ADF UI as the destination service.
- `/imaging/samlacs/acs` to configure Imaging as the destination service.

7. Select the **ARS Requires SSL** check box.

8. In the **SSL Client Identity Alias** field, enter *Demoidentity*.

9. In the **SSL Client Identity Pass Phrase** field, enter *DemoidentityPassPhrase*.

10. In the **Confirm SSL Client Identity Pass Phrase** field, confirm the SSL client identity pass phrase by entering *DemoidentityPassPhrase*.

11. Select the **POST Recipient Check Enabled** and the **POST One-Use Check Enabled** check boxes.

12. In the **Used Assertions Cache Properties** field, enter *APID=ap_00001*.

13. Click **Save**.

 **Note:**

After configuring the destination services, log in to the source as a weblogic user and open the required destination URL. Notice that you can access the destination URL without having to log in again.

16.6.5 Configuring SAML 2.0 (IDCS) Single Sign-On

This section covers the steps for configuring SAML 2.0 SSO with IDCS for WebCenter applications including:

- WebCenter Content Server (see [Configuring WebCenter Content for Oracle Identity Cloud Service \(IDCS\)](#))
- WebCenter Desktop Client
- Enterprise Capture (console and client)
- WebCenter Content ADFUI
- WebCenter Content: Imaging

The following topics are covered:

- [Configuring SAML 2.0 Asserter](#)
- [Configuring Weblogic Managed Servers as SAML 2.0 SSO Service Providers](#)
- [Completing SAML 2.0 Identity Asserter Configuration](#)
- [Creating SAML Applications in IDCS](#)
- [Assigning Groups to SAML Applications](#)
- [Modifying Cookie Path](#)
- [Configuring Oracle HTTP Server](#)
- [Configuring Desktop Client](#)

16.6.5.1 Configuring SAML 2.0 Asserter

To configure SAML 2.0 Asserter:

1. Log in to the Weblogic Server Administration Console.
2. Click **Security Realm** in the Domain Structure pane.
3. On the Summary of Security Realms page, select the name of the realm (for example, myrealm). Click **myrealm**.

The Settings for myrealm page appears.

4. Click **Providers** and then **Authentication**. To create a new Authentication Provider, in the Authentication Provider's table, click **New**.
5. In the Create a New Authentication Provider page, enter the name of the new asserter, for example, *SAML2Asserter* and select the **SAML2IdentityAsserter** type of authentication provider from the drop-down list and then click **OK**.
6. In the Authentication Provider's table, click the newly created Identity Asserter Provider **SAML2Asserter** link.
7. Select **Security Realm**, then **myrealm**, and then **Providers**. In the Authentication Provider's table, click **Reorder**.
8. In the Authentication Providers page, move *SAML2Asserter* on the top (above the already configured IDCS authentication provider) and click **OK**.
9. Restart the Admin and the managed servers.

16.6.5.2 Configuring Weblogic Managed Servers as SAML 2.0 SSO Service Providers

To configure the Weblogic Managed Servers as SAML 2.0 SSO Service Providers:

1. Log in to the Weblogic Server Administration Console.
2. Click **Environment** in the Domain Structure pane.

The Summary of Environment page appears.

3. Click **Servers**.

The Summary of Servers page appears.

4. Go to the managed server (for Content Server), click **Federation Services** and then **SAML 2.0 Service Provider**. In the Service Provider page:

- a. Select the **Enabled** check box.
- b. In the **Preferred Binding** field, select the value **POST** from the drop-down list.
- c. In the **Default URL** field, enter `http://<HOST/IP>:<PORT>/cs` or `https://<HOST/IP>:<SSL_PORT>/cs`.
- d. Click **Save**.
- e. Repeat the above steps for other managed servers, Capture and Content UI. The **Default URL** for Capture is `http://<HOST/IP>:<PORT>/dc-console` or `https://<HOST/IP>:<SSL_PORT>/dc-console`. The **Default URL** for Content UI is `http://<HOST/IP>:<PORT>/wcc` or `https://<HOST/IP>:<SSL_PORT>/wcc`.

 **Note:**

If OHS is in place, enter the following default URLs:

- i. **Content Server:** `http://<HOST/IP>/cs` or `https://<OHS_HOST/IP>:<SSL_PORT>/cs`
- ii. **Capture:** `http://<HOST/IP>/dc-console` or `https://<OHS_HOST/IP>:<SSL_PORT>/dc-console`
- iii. **Content UI:** `http://<HOST/IP>/wcc` or `https://<OHS_HOST/IP>:<SSL_PORT>/wcc`

5. Go to the managed server (for Content Server), click **Federation Services** and then **SAML 2.0 Service Provider**.
 - a. Select the **Replicated Cache Enabled** check box.
 - b. In the **Published Site URL** field, enter `http://<HOST/IP>:<PORT>/saml2`.
 - c. In the **Entity ID** field, enter the value **ucm**. It can be any name, such as **ucm**, but it must be unique. Note the ID as it will be used while configuring SAML in IDCS.
 - d. Click **Save**. Restart the managed server.
 - e. Publish SP metadata to file, `<DOMAIN_HOME>/<Entity_ID>_sp_metadata.xml`. Unlike other SAML IDPs, IDCS doesn't require this to be imported; however, it can be useful for reference purpose.

Repeat the above steps for other managed servers, Capture and Content UI, with **Entity ID** as **capture**, **wcc** respectively. Publish the respective metadata:

- Published Site URL [Capture]: `http://<HOST/IP>:<PORT>/saml20`
- Published Site URL [Content UI]: `http://<HOST/IP>:<PORT>/saml2`

 **Note:**

If OHS is in place, enter the following for the Published Site URLs:

- a. **Content Server:** `http://<HOST/IP>/saml2`
- b. **Capture:** `http://<HOST/IP>/saml2_capture`
- c. **Content UI:** `http://<HOST/IP>/saml2_wcc`

After configuration, publish the respective metadata files.

16.6.5.3 Completing SAML 2.0 Identity Asserter Configuration

To complete SAML 2.0 Identity Asserter Configuration:

1. Download the IDCS metadata file from https://<IDCS_HOST>/fed/v1/metadata. This is the IdP (IDCS in this case) metadata which needs to be imported in SP (weblogic server in our case). Copy the file to the Admin server.
2. Click **Security Realm** in the Domain Structure pane.
3. On the Summary of Security Realms page, select the name of the realm (for example, myrealm). Click **myrealm**.

The Settings for myrealm page appears.

4. On the Settings for Realm Name page, select **Providers > Authentication**. In the Authentication Providers table, select the SAML 2.0 Identity Assertion provider, for example, **SAML2Asserter**.

The Settings for SAML2Asserter page appears.

5. On the Settings for SAML2Asserter page, select **Management**.
6. In the table under Identity Provider Partners, click **New > Add New Web Single Sign-On Identity Provider Partner**.
7. On the Create a SAML 2.0 Web Single Sign-on Identity Provider Partner page:
 - a. Specify the name of the Identity Provider partner.
 - b. In the field **Path**, specify the location of the IDCS metadata file.
 - c. Click **OK**.

8. On the Settings for SAML 2.0 Identity Asserter page, in the Identity Provider Partners table, select the name of your newly-created web single sign-on Identity Provider partner.

9. In the General page, select the **Enabled** check box.

10. Provide the Redirect URIs specific to the servers:

- For Content server, /adfAuthentication.
- For Capture Console, /dc-console/adfAuthentication.
- For Capture Client, /dc-client/*.
- For Content UI, /wcc/adfAuthentication.

11. Click **Save**.

12. Select **Security Realm > myrealm > Providers**. In the Authentication Provider's table, click **Reorder**.

13. In the Reorder Authentication Providers page, move *SAML2Asserter* on the top of the list of Authenticators and click **OK**.

14. Restart the Admin and the managed servers.

16.6.5.4 Creating SAML Applications in IDCS

To create SAML applications in IDCS:

1. Log in to the IDCS admin console.

2. In the IDCS admin console, on the Applications icon, click **Add an Application**. The list of applications will be displayed. Select the **SAML Application**.
3. In the Add SAML Application Details's page, enter the name of the application and its URL. For example, `http://<HOST/IP>:<PORT>/cs` or `https://<HOST/IP>:<SSL_PORT>/cs`. The application name must be unique, for example, *UCMSAML*.
4. In the Add SAML Application SSO Configuration's page, do the following:
 - In the **Entity ID** field, enter the value **ucm**. This is the same **Entity ID** as set in the managed server Service Provider.
 - In the **Assertion Consumer URL** field, enter `http://<HOST/IP>:<PORT>/saml2/sp/acs/post` or `https://<HOST/IP>:<SSL_PORT>/saml2/sp/acs/post` (copy the Location from `md:AssertionConsumerService` attribute of SP metadata xml file, for example, `ucm_sp_metadata.xml`).
 - For the **NameID Format** field, select the **Unspecified** option from the drop-down list.
 - For the **NameID Value** field, select the **User Name** option from the drop-down list.
5. Click **Finish** to create a SAML application.
6. Create two more SAML applications for Capture Server and Content UI.
7. Provide above values from the respective metadata files and activate both the applications.

 **Note:**

If OHS is in place, use the below values for the Application URLs and Assertion Consumer Service [ACS] URLs:

Application	Assertion Consumer Service URLs	Application URL
Content Server	<code>http://<HOST>/saml2/sp/acs/post</code>	<code>http://<HOST>/cs</code>
Capture	<code>http://<HOST>/saml2_capture/sp/acs/post</code>	<code>http://<HOST>/dc-console</code>
Content UI	<code>http://<HOST>/saml2_wcc/sp/acs/post</code>	<code>http://<HOST>/wcc</code>

16.6.5.5 Assigning Groups to SAML Applications

For users to be authenticated through the IDCS SAML, users must be added to the SAML application. If users are members of an IDCS group, that group can be added to the application and those users will be authenticated. If IDCS will be used for user WCC authorization, the groups that will be used for corresponding WCC roles that can be added to the application (as WCC users will already be members of those groups).

To assign groups to SAML applications:

1. Create a group in IDCS, for example, *WebcenterGroup* and assign it to SAML applications.
2. Go to the SAML Application. Click **Groups > Assign**. Assign *WebcenterGroup* group.

 **Note:**

Users who are part of the group will only be able to use the WebCenter applications.

3. Assign the group to all SAML applications that are already created.
4. Add IDCS users to the *WebcenterGroup* group.

16.6.5.6 Modifying Cookie Path

For SAML 2.0, cookie path must be set to `/`. Follow these steps to update cookie path to `/` for `capture.ear` and `WccAdf.ear`:

 **Note:**

Before you make changes, take a backup copy of the `ear` file.

1. Go to `<MW_HOME>/wccapture/capture/lib`.
2. Unzip the `capture.ear` file: `jar xvf capture.ear`
3. After extracting the `capture.ear` file, you should get two `war` files along with other contents:
 - a. For Capture console, `dc-admin.war`
 - b. For Capture client, `dc-wa.war`
4. Unzip `dc-admin.war` and `dc-wa.war` files in separate directories
5. Open `/WEB-INF/weblogic.xml` file after the extraction of `war` files and then modify the `cookie-path` element under `session-descriptor` element to the following value: `<cookie-path>/</cookie-path>`
6. Remove the old `dc-admin.war` and `dc-wa.war` files and recreate them.

```
jar -cvf dc-admin.war *
jar -cvf dc-wa.war *
```

7. Remove the old `capture.ear` file and recreate it.


```
jar -cvf capture.ear *
```
8. Replace the old `capture.ear` file with the new one.
9. Restart the Admin and the managed servers.
10. Similarly, update the cookie path for `WccAdf.ear` located at `<MW_HOME>/wcccontent/wccadf/lib/WccAdf.ear`.
11. In addition to modifying the cookie path, remove the following line only for WCC ADFUI: `<cookie-name>WCCSID</cookie-name>`.

 **Note:**

The above approach is suitable for development and staging environments. If a Bundle Patch is applied, the ear files may get overwritten, requiring that the modification be made again.

16.6.5.6.1 Creating a Deployment Plan to Override the Cookie-Path

For production deployments, follow these steps:

1. Create a `plan.xml` file in `DOMAIN_HOME`. The `config-root` element in `plan.xml` should point to `DOMAIN_HOME` directory, for example, `<config-root> MW_HOME/user_projects/domains/base_domain/</config-root>`.
2. Redeploy using `weblogic.Deployer`:

```
java -cp <MW_HOME>/wlserver/server/lib/weblogic.jar:. weblogic.Deployer
  -username weblogic -password <password> -adminurl t3://<admin
  hostname>:7001 -plan <path of plan.xml> -deploy
  <MW_HOME>/wccapture/capture/lib/capture.ear -targets <comma
  separated cluster
  targets>
```

16.6.5.7 Configuring Oracle HTTP Server

For each OHS location, you must have a unique URI so that there can be only one `<Location /saml2>`. If there are multiple managed servers configured for SAML, then each managed server requires its own unique location.

After OHS installation and configuration is done, the `mod_wl_ohs` file have the routing rules. Additionally, ensure the below port mappings are there:

1. `/saml2` mapped to port for Content server.
2. `/saml2_capture` mapped to port for Capture.
3. `/saml2_wcc` mapped to port for Content UI.

16.6.5.7.1 Manual Deployment of `saml2.war` File

As different SAML2 context roots will be used for each of the SAML2 applications, for each managed server or cluster, the `saml2.war` application needs to be deployed manually, except of the managed server or cluster that will use the SAML2 context root where it's already automatically deployed.

1. In the domain AdminServer console, select **Deployments**. Click **Install**.
2. Set path to `<Middleware Home>/wlserver/server/lib`.
3. Select the `saml2.war` file. Click **Next**.
4. The **Install this deployment as an application** check box is selected and click **Next**.
5. Select the managed server or cluster to deploy this. Do not make any changes to the pages and click **Finish**.
6. Select the **Configuration** tab.

7. Set the context root to match that of the OHS location:

```
/saml2_capture  
/saml2_wcc
```

8. Click **Save**.
9. Set the path for the deployment `plan.xml` file:

```
<Domain Home>/servers/<Managed Server>/plan.xml
```

For a cluster, the `plan.xml` file shouldn't be under a particular managed server directory, in case that system is down.

10. Click **Save**.
11. Restart the managed server(s).

16.6.5.8 Configuring Desktop Client

For Desktop client to be able to recognize an IDP's login page, the string `<!-- IdcClientLoginForm=1-->` needs to be added to the SSO provider's login page. As this string can't be added to the default IDCS login page, hence we need to build a custom sign-in page so that we can add the string to that page.

Creating a Custom Sign-in Page in IDCS

To configure the custom sign-in page, see [Customize the Oracle Identity Cloud Service Sign-In Page](#).

For Step 2 in the above link, *Configure an Application to Use the Custom Sign-In Page*, we need not create a new application instead use the existing SAML application for the WebCenter Content server. We need to update only the **Custom Login URL** field.

Note:

- This tutorial uses `localhost:3000` to host the sample custom sign-in application. If you deploy this application to another location, update the **Custom Login URL** field with the corresponding URL for the sign-in sample application.
- Don't deploy the custom sign-in application in the same domain, URL and server where you host your other applications. The sign-in page needs to be deployed as a single central service accessible to all other applications and users.
- After performing the above steps, the WebCenter Content server would also get redirected to the custom sign-in page instead of the default IDCS login page.

17

Managing User Types, Logins, and Aliases

This chapter describes Oracle WebCenter Content user login types, user logins, user information fields, and aliases. It also explains how to manage the logins and aliases. Oracle WebCenter Content user login types, logins, and aliases information is integrated with Oracle WebLogic Server user information by default, and with OPSS and other sources of user information according to customer configuration.

This chapter includes the following topics:

- [Introduction to User Login Types](#)
- [Introduction to User Logins and Aliases](#)
- [Managing Logins and Aliases](#)
- [User Information Fields](#)

17.1 Introduction to User Login Types

Content Server software supports the following user login types:

- [External Users](#)
- [Local Users](#)

17.1.1 External Users

The default user type supported in Oracle WebCenter Content 11g, 12c, and 14c releases is *external users*. External users are defined outside the WebCenter Content system and authenticated by external security using the Oracle WebLogic Server Administration Console and Oracle Platform Security Services (OPSS). Once authenticated, external users can access the Content Server instance through Oracle WebLogic Server. Generally, external users are users in a trusted domain to whom you grant access, but do not manage through the WebCenter Content system. Their passwords are owned by the Oracle WebLogic Server domain, the network domain, or another provider such as Oracle Internet Directory, although the User Admin app can be used to set a user password when converting an external user to a local user. Unlike local users, undefined external users are not assigned the guest role.

The first time users log in to the Content Server instance through Oracle WebLogic Server they are added to the Content Server database, and administrators can view external user information through the Repository Manager. However, external users are not automatically included in user lists, such as the Author field on a content Check In page. If an Override check box is selected on a user's User Profile page, any user information defined in the Content Server database overrides the user information derived from the external user base.

The Admin User app only shows users after they have logged in at least one time to the Content Server instance. All users from the Oracle WebLogic Server user store or other user store outside the Content Server instance are shown as external users.

By default, external security integrations map a limited set of user information (user name, password, roles, accounts, and some additional information such as email address) from the external user base to the Content Server instance. If you are using LDAP integration, then additional user information, such as email address or user locale, can be mapped from the

embedded LDAP server with the Oracle WebLogic Server Administration Console and integrated with Oracle Platform Security Services.

 **Note:**

When an OPSS policy store is used, Oracle WebCenter Content roles represent application roles (not enterprise roles). Oracle WebCenter Content honors only application role to security group grants. It ignores any grants created from user role or enterprise role to security group. Do *not* create grants from user or enterprise roles to security groups.

The following is a list of common characteristics of external users:

- **Login (authentication) is defined by:** User ID and password are stored in a user database external to the WebCenter Content system, such as:
 - Trusted domain (such as Oracle WebLogic Server)
 - Lightweight Directory Application Protocol (LDAP)
 - Other database
- **Access (authorization) is determined by:** Credentials (for example, roles) from a trusted domain or other user database (such as the Oracle WebLogic Server user store, Oracle Internet Directory, or another LDAP provider) and WebCenter Content.
- **User login:** Oracle WebLogic Server and the Content Server instance must be running for users to log in.
- **User password:** User passwords are defined on Oracle WebLogic Server or another user database (such as a LDAP server) by the administrator. Users cannot change their passwords on the Content Server instance.
- **Interface issues:** User names do not appear in the content check-in lists. However, users can participate in workflows.

 **Note:**

The ^ (caret) is a special character in WebCenter Content and it must not be used in a username, group name, or rule name. The ^ character is parsed by WebCenter Content for the StringUtils class where the character is used for string encoding and decoding.

Follow this process to set up roles, groups, and accounts for external users:

1. Set up security groups. See [Adding a Security Group on Content Server](#).
2. Establish roles. See [Creating a Role in Content Server](#).
3. Arrange permissions. See [Adding and Editing Permissions in Content Server](#).
4. (Optional) Use accounts. See [Enabling Accounts in Content Server](#).

See Create users in *Oracle WebLogic Server Administration Console Online Help*.

17.1.2 Local Users

Local users are defined by an administrator within the Content Server instance. Administrators assign these users one or more roles, which provide the user with access to security groups.

Caution:

Local users are not supported on the Oracle WebLogic Server domain. Although Content Server administrators can create and configure local users with the User Admin applet, for local users to be authenticated for access to the Content Server instance, the users and passwords also must be created with the Oracle WebLogic Server Administration Console. The default user type supported is *external users*.

The following is a list of common characteristics of local users:

- **Logins (authentication) are created by:** Administrator in the Content Server.
- **Access (authorization) is determined by:** Content Server roles, which provide access to security groups.
- **User login:** Local users cannot log in to the Content Server Admin Server because the Admin Server requires logging in through Oracle WebLogic Server.
- **User password:** Users can change their passwords.
- **Interface issues:** User names appear in the content check-in lists. Users can specify whether to change full name, email address, and user type.
- **Considerations:** Previously recommended for 1000 or fewer users, but now recommended only when required by the system administrator for purposes such as troubleshooting Content Server. Because of performance considerations, do not configure more than 1000 local users.

Note:

The ^ (caret) is a special character in WebCenter Content and it must not be used in a username, group name, or rule name. The ^ character is parsed by WebCenter Content for the StringUtils class where the character is used for string encoding and decoding.

Follow this process to set up local users:

1. Set up security groups. See [Adding a Security Group on Content Server](#).
2. Establish roles. See [Creating a Role in Content Server](#).
3. Arrange permissions. See [Adding and Editing Permissions in Content Server](#).
4. Assign user logins. See [Adding a User Login](#).
5. (Optional) Use accounts. See [Enabling Accounts in Content Server](#).

17.2 Introduction to User Logins and Aliases

User logins are the names associated with the people who access Content Server. By default user logins must be created on the Oracle WebLogic Server domain that hosts WebCenter Content and the Content Server instance. Authentication and credentials are handled by default with the Oracle WebLogic Server user store and associated security software instead of by the Content Server. See Understanding Identities, Policies, Credentials, Keys, Certificates, and Audit in *Securing Applications with Oracle Platform Security Services*.

Note:

Instructions for using the Oracle WebLogic Server Administration Console apply to users and groups in the Oracle WebLogic Authentication provider only. If you customize the default security configuration to use a custom Authentication provider, use the administration tools supplied by that security provider to create a user. If you are upgrading to the Oracle WebLogic Server Authentication provider, you can load existing users and groups into its database. See Migrating Security Data in *Administering Security for Oracle WebLogic Server*.

Caution:

Although user logins still can be created and managed on the Content Server with the User Admin applet, they are not valid for authentication purposes unless they also have been created with the Oracle WebLogic Server Administration Console.

If you use a LDAP server and create a user login with the same name as a local user defined in the Content Server with the User Admin applet, the LDAP user is authenticated against LDAP when logging in, but receives roles assigned to the local user.

The Oracle WebLogic Server administrator assigns one or more groups to each user. A group provides the user access to files within the security groups. Undefined users are assigned to the *guest* group, which allows viewing of documents only in the Public security group by default.

You can also create a group of users that can be then referenced by a single name, or *alias*, in workflows, subscriptions, and projects. For example, it is much easier to add an alias called Support to a workflow than it is to add user1, user2, user3, and so on.

Note:

If a workflow is assigned to an alias, the users within the alias can approve or reject the content until they belong to the alias. For example, a workflow is created and assigned for review through an alias comprising Users 1 and 2. If User 1 is removed from the alias, this user can no longer approve or reject the content. Similarly, if User 3 is added to the alias, this user can approve or reject the content.

If you log in to multiple browser windows on the same computer using different login methods (such as standard login, Microsoft login, or self-registered login), the Content Server can become confused about which user is logged in to each window. Remember to close any open browser windows while testing different login methods.

 **Important:**

User logins are case sensitive.

17.3 Managing Logins and Aliases

By default, user logins must be created and managed with the Oracle WebLogic Server Administration Console. For information and instructions on creating and managing user logins, see *Create users in Oracle WebLogic Server Administration Console Online Help*. If you customize the default security configuration to use another Authentication provider, such as Oracle Internet Directory, use the administration tools supplied by that security provider to create and manage user logins.

If you need to set up a user (other than the Content Server administrator) to work with a standalone Content Server utility such as System Properties, you can use the User Admin applet in Content Server to create a local user. However, a user created with the User Admin applet cannot be authenticated for any other functions than standalone Content Server utilities, unless the user is also created with the Oracle WebLogic Server Administration Console.

The remainder of this section discusses the tasks involved in managing only Content Server user logins for standalone utilities.

- [Adding a User Login](#)
- [Editing a User Login](#)
- [Deleting a User Login](#)
- [Creating an Alias](#)
- [Editing an Alias](#)
- [Deleting an Alias](#)

17.3.1 Adding a User Login

Beginning from 11g Release 1 (11.1.1), external user logins must be added using the Oracle WebLogic Server Administration Console. Although user logins can be managed in Content Server for special purposes, they are not valid for authentication to the Content Server until they have been created with the Oracle WebLogic Server Administration Console. See *Create users in Oracle WebLogic Server Administration Console Online Help*.

 **Note:**

The ^ (caret) is a special character in WebCenter Content and it must not be used in a username, group name, or rule name. The ^ character is parsed by WebCenter Content for the StringUtils class where the character is used for string encoding and decoding.

To add a user login *only* for use with Content Server standalone utilities:

1. From the User Admin: Users tab, click **Add**.
2. Set the Authorization Type from the menu. For more information, see [Introduction to User Login Types](#).
3. Click **OK**.
4. In the Add/Edit User window, enter information about the user.
 - If you enter a password, you must reenter the same password in the **Confirm Password** field.
 - Keep in mind that the user name and password are case-sensitive.
5. Assign roles to the user.
6. If accounts are enabled, assign accounts to the user.
7. Click **OK**.

17.3.2 Editing a User Login

Beginning from 11g Release 1 (11.1.1), external user logins must be edited using the Oracle WebLogic Server Administration Console. Although user logins can be managed in the Content Server for special purposes, they are not valid for authentication to Content Server until they have been created with the Oracle WebLogic Server Administration Console. See *Modify users in Oracle WebLogic Server Administration Console Online Help*.

To edit a user login *only* for use with Content Server standalone utilities:

1. From the Users tab of the User Admin window, double-click the user name, or select the user name and click **Edit**.
2. In the Add/Edit User window or Add/Edit User: Info tab (Global User), edit the user login as necessary.

If you change the user locale for a user who has the *sysmanager* role, you must restart the Admin Server service for the Admin Server interface to appear in the user's locale language.

17.3.3 Deleting a User Login

Beginning from 11g Release 1 (11.1.1), external user logins must be deleted using the Oracle WebLogic Server Administration Console. Although user logins can be managed in Content Server for special purposes, they are not valid for authentication to Content Server until they have been created with the Oracle WebLogic Server Administration Console. See *Delete users in Oracle WebLogic Server Administration Console Online Help*.

To delete a user login *only* for use with Content Server standalone utilities:

1. In the Users tab of the User Admin window, select the user name.
2. Click **Delete**.
3. Click **Yes**.

If you delete a user who is involved in a workflow, you are prompted to confirm the deletion. You must adjust the workflow and remove the user from the list of workflow reviewers.

17.3.4 Creating an Alias

Beginning from 11g Release 1 (11.1.1), external user logins must be managed using the Oracle WebLogic Server Administration Console. Although user logins can be managed in Content Server for special purposes, they are not valid for authentication to Content Server until they have been created with the Oracle WebLogic Server Administration Console.

To define an alias *only* for use with Content Server standalone utilities:

1. Display the User Admin window Aliases tab.
2. Click **Add**.
3. In the **Alias Name** field on the Add New Alias/Edit Alias window, enter a name that identifies the group of users.
4. In the **Description** field, enter a detailed description of the alias.
5. Click **Add**.
6. In the Select Users window, select the user names from the list.
 - To narrow the list of users on the Select Users page, select **Use Filter**, click **Define Filter**, select the filter criteria, and click **OK**.
 - To select a range of users, click one user login, then hold down the Shift key while clicking another user login.
 - To select users individually, hold down the Ctrl key while clicking each user login.
7. Click **OK**.
8. Close the User Admin page.

17.3.5 Editing an Alias

Beginning from 11g Release 1 (11.1.1), external user logins must be managed with the Oracle WebLogic Server Administration Console. Although user logins can be managed in Content Server for special purposes, they are not valid for authentication to Content Server until they have been created with the Oracle WebLogic Server Administration Console.

To edit an alias *only* for use with Content Server standalone utilities:

1. Display the User Admin: Aliases tab window.
2. Highlight an alias and click **Edit**.
3. Alter the information as needed on the Add New Alias/Edit Alias window.
4. In the **Description** field, enter a detailed description of the alias.
5. Click **OK**.
6. Close the User Admin page.

17.3.6 Deleting an Alias

Beginning from 11g Release 1 (11.1.1), external user logins must be managed with the Oracle WebLogic Server Administration Console. Although user logins can be managed in Content Server for special purposes, they are not valid for authentication to Content Server until they have been created with the Oracle WebLogic Server Administration Console.

To delete an alias *only* for use with Content Server standalone utilities:

1. Display the Add New Alias/Edit Alias window.
2. Highlight the alias to be deleted and click **Delete**.
A page appears, asking you to confirm the deletion. Click **Yes** to delete the entry or **No** to retain it.
3. Close the User Admin page.

17.4 User Information Fields

User information defines the unique attributes of a user, such as full name, password, and email address. User information fields describe a user in the same way that metadata fields describe a content item. User information is stored in the Content Server database, and can be used to sort users, display user information on Content Server web pages, or customize the display of web pages based on user attributes.

The following user information fields are predefined in the system. These fields cannot be deleted, and the field name and type cannot be changed.

Name	Type	Caption	Is Option List
dFullName	Long Text	Full Name	False
dEmail	Long Text	E-mail Address	False
dUserType	Text	User Type	True
dUserLocale	Text	User Locale	True

This section covers these topics:

- [Adding a New User Information Field](#)
- [Editing an Option List](#)
- [Editing a User Information Field](#)

17.4.1 Adding a New User Information Field

To add a new user information field:

1. In the **User Admin: Information Fields** tab, click **Add**.
2. Enter a new field name in the Add Metadata Field Name window. Duplicate names are not allowed. Maximum field length is 29 characters. The following are not acceptable: spaces, tabs, line feeds, carriage returns and ; ^ ? : @ & + " # % < * ~ |
3. Click **OK**.
4. In the Edit Metadata field window, configure the properties for the field, and click **OK**.
5. Click **Update Database Design**.

17.4.2 Editing an Option List

To edit an option list key:

1. In the Edit Metadata Field window, select **Enable Option List**.
2. Click **Edit**.
3. Add, edit, or delete option values on the Option List window.

- Each value must appear on a separate line.
 - A blank line will result in a blank value in the option list.
4. To sort the list, select sort options and click **Sort Now**.
 5. Click **OK**.

17.4.3 Editing a User Information Field

To edit a user information field:

1. Double-click the field, or select the field and click **Edit**.
2. Add, edit, or delete option values on the Edit Metadata Field window.
3. Click **OK**.

18

Managing Security Groups, Roles, and Permissions

This chapter provides information on the use and management of security groups, roles, and permissions on Oracle WebCenter Content Server.

This chapter includes the following topics:

- [Introduction to Content Server Security Groups](#)
- [Managing Content Server Groups](#)
- [Introduction to Content Server Roles and Permissions](#)
- [Managing Content Server Roles and Permissions](#)

18.1 Introduction to Content Server Security Groups

A security group is a set of files grouped under a unique name. Every file in the Content Server repository belongs to a security group. Access to security groups is controlled by the permissions, which are assigned to roles in Content Server. Roles are assigned to users where they are managed with Oracle WebLogic Server.

Users are assigned groups with the Oracle WebLogic Server Administration Console. When a user logs in to the Content Server instance, the user's groups are mapped to Content Server roles. Oracle WebLogic Server user groups that start with a @ ("at") symbol are mapped to Content Server accounts.

For Oracle WebLogic Server groups to be recognized in Content Server, roles with the exact same names must be created in Content Server and assigned to security groups. If this is not done, the Oracle WebLogic Server groups assigned to users have no impact on users' privileges on Content Server.

Security groups enable you to organize content files into distinct groups that can be accessed only by specific users. For example, files could be assigned to a security group with the name HRDocs, which could represent documents under the Human Resources designation, and could be accessed only by people who worked in the Human Resources department. There are two predefined security groups:

- **Public:** By default, any user can view documents in the Public group without logging in.
- **Secure:** System files are stored in the Secure group and are available only to the system administrator.

18.1.1 Best Practices for Working with Security Groups

Keep these considerations in mind when you define security groups:

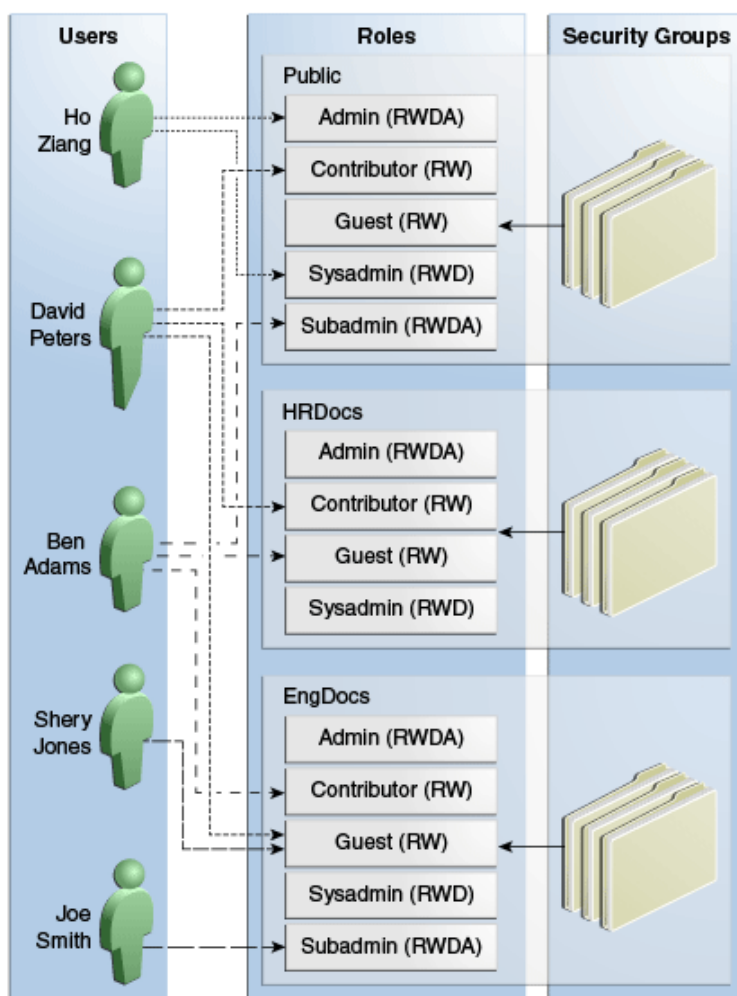
- Define security groups *before* anyone checks in files that must be secure.
- The number of security groups should be kept at a minimum to provide optimum search performance and user administration performance. If your security model requires more than 50 security classifications, you should enable accounts and use them to control user

permissions. This number varies depending on [Search Performance](#) and [User Admin Performance](#).

- To create instance folders, a user group should have at least admin (RW) access.
- Put all files that share the same access into one security group.
- Set up a logical naming convention for your security groups. For example, use department names if you are setting up an intranet, and use levels of security (internal, classified, and so forth) if you are setting up an extranet.

For example, [Figure 18-1](#) shows three defined security groups (Public, HRDocs, and EngDocs). They are associated with five users assigned different roles (Admin, Contributor, Guest, Sysadmin, Subadmin) and specific sets of permissions (Read, Write, Delete, Admin).

Figure 18-1 Example of Defining Security Groups



18.1.2 Performance Considerations

Your user access choices for security groups and roles can affect the following system performance areas:

- [Search Performance](#)

- [User Admin Performance](#)

18.1.2.1 Search Performance

Search performance is affected by the number of security groups a user has permission to access. To return only content that a user has permission to view, the database WHERE clause includes a list of security groups. The WHERE clause either includes all of the security groups the user has permission to access, or it includes all of the security groups the user does *not* have permission to access. Which approach is taken depends on whether the user has permission to more than 50% or fewer than 50% of the defined security groups.

For example, if 100 security groups are defined, and a user has permission to 10 security groups, the 10 security groups will be included in the WHERE clause. In contrast, for a user with permission to access 90 security groups, the WHERE clause includes the 10 security groups the user does *not* have permission to access.

Therefore, if a user has permission to almost 50% of the security groups, the search performance is less efficient. If a user has permission to all or none of the security groups, the search performance is more efficient.

18.1.2.2 User Admin Performance

The total number of security groups multiplied by the total number of roles determines the number of rows in the *RoleDefinition* database table, which affects the performance of the User Admin application for operations involving local users. To determine the approximate time required to perform an operation in the User Admin application, such as adding a security group or changing permission for a role, use the following formula:

$$(\# \text{ of security groups}) \times (\# \text{ of roles}) / 1000 = \text{Time of operation in seconds}$$

For example, using a PC with a 400 MHz processor, 128 MB of RAM, it took approximately 10 seconds to add a security group, or role, or both, using the User Admin application when the *RoleDefinition* table has 10,000 rows.

As the number of security groups increases, administration performance is affected more than consumer search performance.

18.2 Managing Content Server Groups

The following tasks are used to manage security groups using Content Server.

- [Adding a Security Group on Content Server](#)
- [Deleting a Security Group on Content Server](#)

See Managing Security Information in *Administering Security for Oracle WebLogic Server*.

18.2.1 Adding a Security Group on Content Server

To create a security group and assign permissions:

 **Note:**

The ^ (caret) is a special character in WebCenter Content and it must not be used in a username, group name, or rule name. The ^ character is parsed by WebCenter Content for the StringUtils class where the character is used for string encoding and decoding.

1. From the User Admin window, choose **Security**, then **Permissions by Group**.
2. In the Permissions By Group window, click **Add Group**.
3. In the Add New Group window, enter a group name and description.
4. Click **OK**.
5. Set permissions for the security group:
 - a. Select the security group.
 - b. Select the role to edit.
 - c. Click **Edit Permissions**.
 - d. After enabling the permissions that you want the role to have for the group, click **OK** to close the Permissions by Group page.

18.2.2 Deleting a Security Group on Content Server

 **Note:**

Never delete a security group or account if it is associated with a content item stored in the Content Server repository.

To delete a security group:

1. Make sure that no content items are assigned to the security group you want to delete. You cannot delete a security group if content still exists in that security group.
2. From the User Admin window, choose **Security**, then **Permissions by Group**.
3. In the Permissions By Group window, select the group you want to delete.
4. Click **Delete Group**.
5. Click **Yes**. The security group is deleted.
6. After you have deleted the security group, click **OK** to close the Permissions by Group page.

18.3 Introduction to Content Server Roles and Permissions

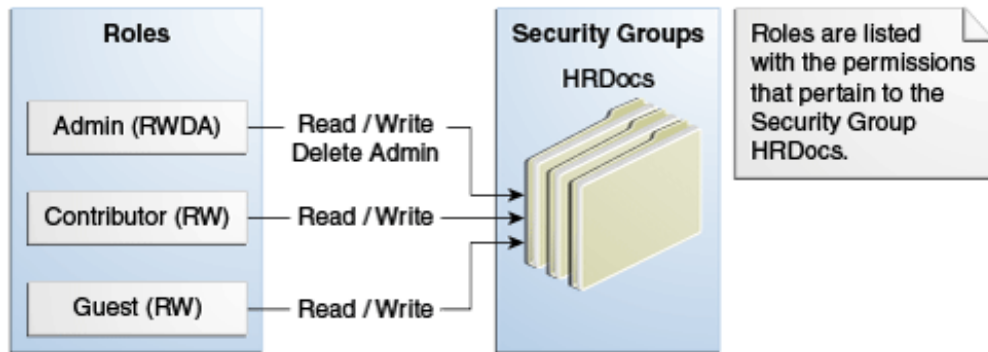
A role is a set of permissions (Read, Write, Delete, Admin) for each security group. You can think of a role as a user's job. Users can have different jobs for various security groups. Users can also have different jobs to identify the different teams in which they participate. You can:

- Define roles.

- Assign multiple roles to a user.
- Set up multiple users to share a role.
- Set the role's permissions to multiple security groups.

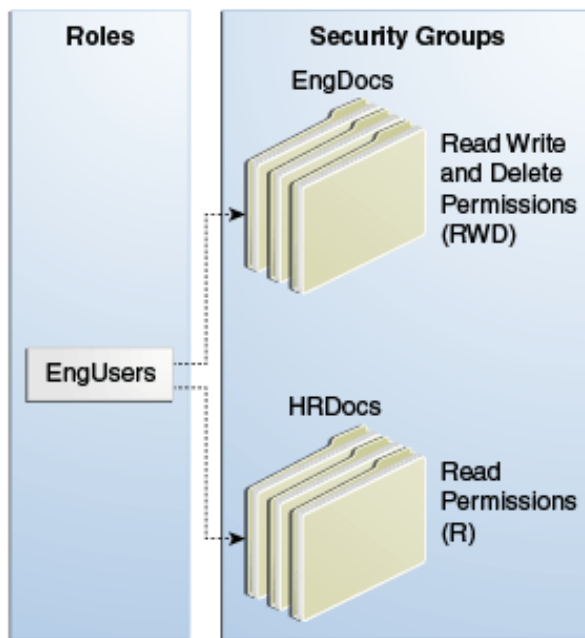
For example, [Figure 18-2](#) shows three roles and the permissions those roles have to the same security group.

Figure 18-2 Example of Roles and Their Permissions



Roles are assigned to one or more users by the system administrator to provide access to the security groups. [Figure 18-3](#) shows the EngUsers role with only Read permission to the HRDocs security group. However, this role provides Read, Write, and Delete permissions to the EngDocs security group. This provides an added measure of security, ensuring that only users who need access to certain documents can modify them.

Figure 18-3 Example of Roles and Security Group Access



18.3.1 Predefined Roles

The following roles are predefined in Content Server:

Roles	Description
admin	The <i>admin</i> role is assigned to the system administrator. By default, this role has Admin permission to all security groups and all accounts, and has rights to all administration tools.
contributor	The <i>contributor</i> role has Read and Write permission to the Public security group, which enables users to search for, view, check in, and check out content.
guest	The <i>guest</i> role has Read permission to the Public security group, which enables users to search for and view content.
sysmanager	The <i>sysmanager</i> role has privileges to access the Admin Server links from the Administration menu in the user interface.

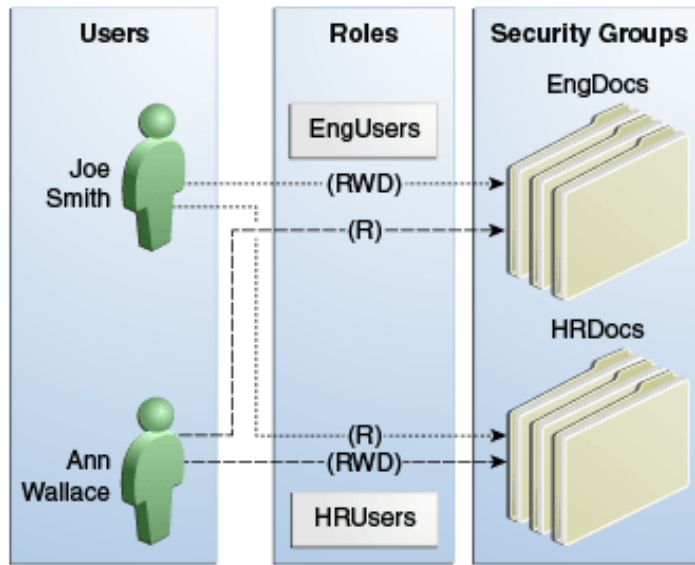
18.3.2 About Permissions

Each role allows the following permissions for each security group: Read (R), Write (W), Delete (D), Admin (A), Standard Annotation (S), Restricted Annotation (T), or Hidden Annotation (H). The permission that a user has to access the files in a security group is the *highest permission defined by any of the user's roles*. If a user has the guest and contributor roles, where guest is given Read permission and contributor is given Write permission to the Public security group, the user will have Write permission to content in the Public security group. When a user is assigned the Standard Annotation, Restricted Annotation, or Hidden Annotation permission, the Read permission is given by default to that user.

As shown in [Figure 18-4](#), Joe Smith and Ann Wallace have permissions to two security groups:

- Joe Smith has Read, Write, and Delete permission to the EngDocs security group, but only Read permission to the HRDocs security group. As a member of the EngUsers role, he has been given Read, Write, and Delete access to Engineering Documents, but only Read access to Human Resource documents.
- Ann Wallace has Read, Write, and Delete permission to the HRDocs security group, but only Read permission to the EngDocs security group. As a member of the HRUsers role, she has been given Read, Write, and Delete access to Human Resource documents, but only Read access to Engineering documents.

Figure 18-4 Example of Assigned Permissions



18.3.3 Predefined Permissions

Each role allows the following permissions to be assigned for each security group:

Permission	Description
Read	Allows viewing documents in the security group.
Write	Allows viewing, checking in, checking out, and getting a copy of documents in the security group. An author who has Write permission in the a security group can change the security group setting of a document.
Delete	Allows viewing, checking in, checking out, getting a copy, and deleting documents in the security group. If the configuration variable AuthorDelete is set to true, and Content Server is configured to use Folders (enabled by the FrameworkFolders component), the author can delete the author's own revisions as long as the author has Read privilege, otherwise the author would need Delete privilege to the content item's security group.
Admin	Allows viewing, checking in, checking out, getting a copy, and deleting files in the security group. If the user has Workflow rights, the user can start or edit a workflow in the security group. The user can check in documents in the security group with another user specified as the Author. As a non-author of a document, the user can change the security group setting of the document if the user has Write permission in the new security group.
Standard Annotation	Allowed to create, modify, and delete standard annotations. An user who can access a document can view the standard annotations on the document.
Restricted Annotation	Allowed to create, modify, and delete restricted annotations. Any user can view restricted annotations on a document if they can access that document.

Permission	Description
Hidden Annotation	Allowed to create, view, modify, and delete hidden annotations.

 **Note:**

- Users require this permission to view any hidden annotation on a document even if they can access that document.
- Redaction can only be of standard or restricted type. A hidden redaction is not supported.

18.4 Managing Content Server Roles and Permissions

Roles and permissions are defined and managed in Content Server. Roles are assigned to user logins, which by default are managed with the Oracle WebLogic Server Administration Console.

The following tasks are used to manage user roles.

- [Creating a Role in Content Server](#)
- [Deleting a Role in Content Server](#)
- [Assigning Roles to a User with Oracle WebLogic Server](#)
- [Assigning Roles for a Similar User with Oracle WebLogic Server](#)
- [Adding and Editing Permissions in Content Server](#)

18.4.1 Creating a Role in Content Server

To create a role and configure permissions in Content Server:

 **Note:**

The ^ (caret) is a special character in WebCenter Content and it must not be used in a username, group name, or rule name. The ^ character is parsed by WebCenter Content for the StringUtils class where the character is used for string encoding and decoding.

1. From the User Admin window, choose **Security**, then **Permissions by Role**.
2. In the Permissions By Role window, click **Add New Role**.
3. In the Add New Role window, enter a Role Name.
 - The Role Name is limited to 255 characters. However, you must ensure that the role names are unique in the first 30 characters.

- The following characters are not allowed: spaces, tabs, line feeds, returns, and ; : ^ ? & + " # % < > * ~ |
 - Initially, a role is assigned Read (R) permission to the Public security group and no permissions to any other security groups.
4. Set permissions for the role:
 - a. Select the role.
 - b. Select the security group to edit.
 - c. Click **Edit Permissions**.
 - d. Edit the permissions.
 - e. Click **OK** and close the Permissions By Role page.

18.4.2 Deleting a Role in Content Server

To delete a role in Content Server:

1. Make sure that no users are assigned to the role to delete. (You cannot delete a role if any users are assigned to it.)
2. From the User Admin window, choose **Security**, then **Permissions by Role**.
3. In the Permissions By Role window, select the role to delete.
4. Click **Delete Role**.
5. Click **Yes**.

18.4.3 Assigning Roles to a User with Oracle WebLogic Server

To assign roles to a user for Content Server, use the Oracle WebLogic Server Administration Console. While roles are defined in Content Server, roles must be assigned to users with the Administration Console. For more information, see the Oracle WebLogic Server Administrator's Guide.

Users also can be assigned groups with the Oracle WebLogic Server Administration Console. For Oracle WebLogic Server groups to be recognized in Content Server, roles with the exact same names as the groups must be created in Content Server and assigned to security groups.

18.4.4 Assigning Roles for a Similar User with Oracle WebLogic Server

To assign roles when creating a user for Content Server that has similar access to that of another user login, use the Oracle WebLogic Server Administration Console. While roles are defined in Content Server, they must be assigned to users with the Administration Console. For more information, see the *Oracle WebLogic Server Administrator's Guide*.

Users also can be assigned groups with the Oracle WebLogic Server Administration Console. For Oracle WebLogic Server groups to be recognized in Content Server, roles with the exact same names as the groups must be created in Content Server and assigned to security groups.

18.4.5 Adding and Editing Permissions in Content Server

To add permissions to a role or edit existing permissions in Content Server:

1. From the User Admin window, choose **Security**, then **Permissions by Role**.
2. In the Permissions By Role window, either select an existing role, or add a new role. The permissions associated with the security groups are displayed.
3. Select an item in the Groups/Rights column.
4. Click **Edit Permissions**.
5. In the Edit Permissions window, specify the permissions to associate with this role and security group. For more information about permissions, see [Predefined Permissions](#).
6. Click **OK**.

19

Managing Accounts

This chapter provides information on Content Server accounts, which are defined and managed in Content Server. Account permissions are assigned to user logins with the Oracle WebLogic Server Administration Console.

This chapter includes the following topics:

- [Introduction to Content Server Accounts](#)
- [Managing Content Server Accounts](#)
- [A Content Server Accounts Case Study](#)

19.1 Introduction to Content Server Accounts

Accounts give you greater flexibility and granularity in your security structure than security groups alone provide. Accounts and account permissions are assigned to users with the Oracle WebLogic Server Administration Console, and the server maps groups to Content Server roles and accounts. An account also can be assigned to each content item. To access a content item that has an account assigned to it, the user must have the appropriate permission for the account.

Oracle WebLogic Server user groups that start with a @ ("at") symbol are mapped to Content Server accounts.

Note:

If you enable accounts and use them, then later choose to disable accounts, you can have the perception of losing data. The repository remains intact. However, if you make certain changes to the security model, then you also must update the users' access rights so they can continue to access the secure content.

To avoid this situation, examine your requirements and the WebCenter Content security model of groups and accounts to determine what would best match your needs. Unless you are certain that you want to use accounts, do not enable them.

Some ways accounts can be created:

- The Content Server administrator creates *predefined accounts* using the User Admin tool. For details, see [Creating Predefined Accounts in Content Server](#).
- A user administrator creates an account while checking in content. For details, see [Creating Accounts When Checking In Content in Content Server](#).

 **Note:**

It is recommended not to use stopwords in account names. Stopwords are words that a search engine filters out or ignores in a search query when they are combined with other keywords. When a search on the account names is conducted using the OracleTextSearch component, returned search results may be adversely affected if the query contains stopwords. For more detailed information about using stopwords or for instructions on how to remove them, refer to the Oracle Text Reference document.

You must enable accounts to use them. For more information, see [Enabling Accounts in Content Server](#).

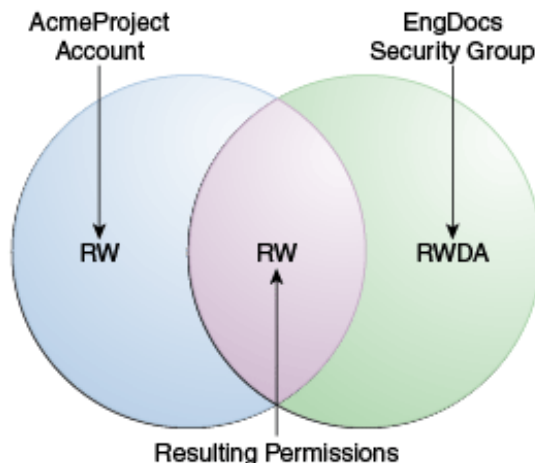
19.1.1 Accounts and Security Groups

When accounts are used, the account becomes the *primary permission* to satisfy before security group permissions are applied. You can also think of a user's access to a particular document as the *intersection* between their account permissions and security group permissions.

For example, the EngAdmin role has Read, Write, Delete, and Admin permission to all content in the EngDocs security group. A user is assigned the EngAdmin role, and is also assigned Read and Write permission to the AcmeProject account. Therefore, the user has only Read and Write permission to a content item that is in the EngDocs security group and the AcmeProject account.

[Figure 19-1](#) shows the intersection of the AcmeProject account and EngDocs security group permissions.

Figure 19-1 Example of Security Group Permissions

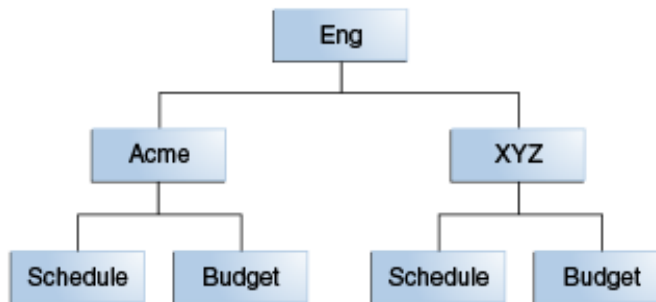


Security group permissions are ignored if the account does not permit access to any content. Remember that the account acts as a filter that supersedes the permissions defined by the user's roles.

19.1.2 Hierarchical Accounts

Accounts can be set up in a hierarchical structure, which enables you to give some users access to entire branches of the structure, while limiting permissions for other users by assigning them accounts at a lower level in the structure. [Figure 19-2](#) shows a typical hierarchical account structure.

Figure 19-2 Example of Hierarchical Account Structure



- If you use slashes to separate the levels in account names (for example, Eng/Acme/Budget), Content Server creates a weblayout directory structure according to your account structure. (However, each actual directory will not be created until a content item is assigned to the account during the check-in process.) Each lower level in the account name becomes a subdirectory of the upper level, with an @ symbol prefix to indicate that the directory is an account level.

! Important:

When using an embedded LDAP server, do not use the slash. The usage of back slashes (/) and forward slashes (\) is not recommended for security groups when using an Oracle WebLogic Server Console.

- If a user has permission to a particular account prefix, they have access to all accounts with that prefix. For example, if you are assigned the Eng/XYZ account, you have access to the Eng/XYZ account and any accounts that begin with the Eng/XYZ prefix (such as Eng/XYZ/Schedule and Eng/XYZ/Budget).

! Important:

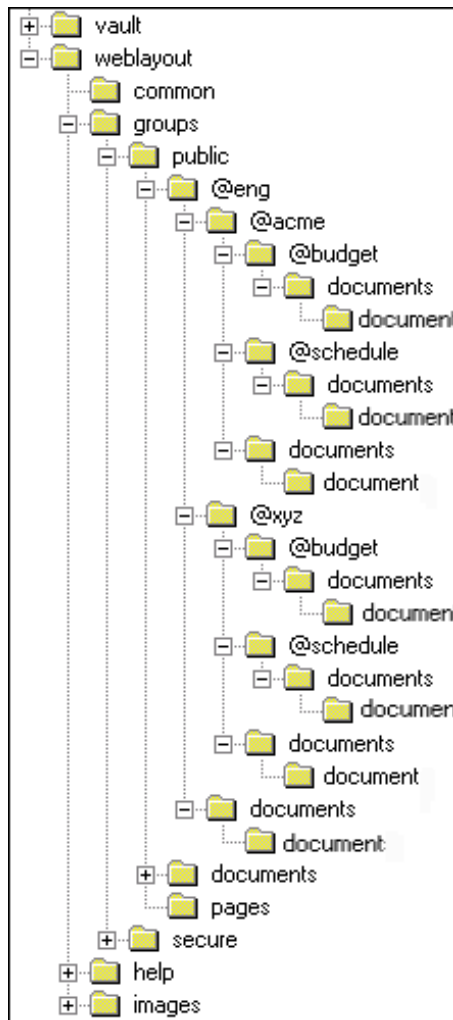
The account prefix does not have to include slashes. For example, if you have accounts called abc, abc_docs, and abcdefg, all users who have access to the abc account will have access to the other two accounts as well.

To handle the security structure depicted above, you would create the following accounts:

- Eng
- Eng/Acme

- Eng/XYZ
- Eng/Acme/Schedule
- Eng/Acme/Budget
- Eng/XYZ/Schedule
- Eng/XYZ/Budget

Figure 19-3 Example of a Security File Structure



19.1.3 Performance Considerations

Consider the following performance issues when using accounts in your security model:

- Theoretically, you can create an unlimited number of accounts without affecting Content Server performance. A system with over 100,000 pieces of content has only limited administration performance problems at 200 accounts per person; however, there is significant impact on search performance with over 100 accounts per person. (Note that these are explicit accounts, not accounts that are implicitly associated with a user through a hierarchical account prefix. A user can have permission to thousands of implicit accounts through a single prefix.)

- For performance reasons, do not use more than approximately 50 security groups if you enable accounts.
- Ensure that your security groups and accounts have relatively short names.

19.1.4 External Directory Server Considerations

Accounts are available whether or not your Content Server instance is integrated with an external directory server (such as the default Oracle WebLogic Server). When you use accounts with an external directory, ensure that you follow these guidelines:

- Set up a global group with the appropriate users in it to match the account.
- Associate group names to either a role or an account by configuring mapping prefixes.

19.2 Managing Content Server Accounts

The following tasks are involved in managing accounts.

- [Enabling Accounts in Content Server](#)
- [Creating Predefined Accounts in Content Server](#)
- [Creating Accounts When Checking In Content in Content Server](#)
- [Deleting Predefined Accounts in Content Server](#)
- [Assigning Accounts to a User with Oracle WebLogic Server](#)

19.2.1 Enabling Accounts in Content Server

To enable accounts in the Content Server instance:

Important:

If you enable accounts and use them, then choose to disable accounts, you can have the perception of losing data. The repository remains intact. However, if you make certain changes to the security model, then you also must update the security settings for users so they can continue to access the content.

1. In the Content Server portal, choose **Administration**, then **Admin Server**, then **General Configuration**.
2. On the General Configuration page, select **Enable Accounts**.
3. Save the changes.
4. Restart the Content Server instance.

Alternately, you can add the following line to the **Additional Configuration Variables** field on the General Configuration page, which shows the contents of the `DomainHome/ucm/cs/config/config.cfg` file:

```
UseAccounts=true
```

Save the changes, and restart the Content Server instance.

19.2.2 Creating Predefined Accounts in Content Server

To create a predefined account on the Content Server instance:

1. From the User Admin page, choose **Security**, then **Predefined Accounts**.
2. In the Predefined Accounts window, click **Add**.
3. In the Add New Predefined Account window, add the name of the new account. Keep the names short and consistent. For example, set up all of your accounts with a three-letter abbreviation by location or department (MSP, NYC, etc.). Account names can be no longer than 30 characters, and the following are not acceptable: spaces, tabs, line feeds, carriage returns, and the symbols : ; ^ ? : & + " # % < > * ~.
4. Click **OK**.
5. If you already have content checked in to Content Server repository and you are using a database with full text indexing, rebuild your search index.

If you are using only the metadata database search indexer engine, you do not need to rebuild your search index.

19.2.3 Creating Accounts When Checking In Content in Content Server

Generally, you should create predefined accounts rather than creating an account during content check-in. For more information about predefined accounts, see [Creating Predefined Accounts in Content Server](#).

To create an account at the time you check in a content item, you must have User Admin rights:

1. Display the **Content Check In Form** page.
2. Enter all required and optional information.
3. Type an account name in the **Account** field.
4. Click **Check In**. The new account is assigned to the content item.

Note:

If you have write (W) privileges to an account, you can create another account with this account as a prefix while checking in a content item. For example, if you have write privileges to the **br** account, then you can create the **brown** account and associate it with a content item during check-in.

19.2.4 Deleting Predefined Accounts in Content Server

You can delete an account even if content with that account still exists. The account value will remain assigned to the content item, but will be considered a user-defined account.

! Important:

Never delete an account if it is associated with a content item stored in the Content Server repository.

To delete a predefined account in the Content Server instance:

1. From the User Admin page, choose **Security**, then **Predefined Accounts**.
2. In the Predefined Accounts window, select the account to delete.
3. Click **Delete**. The account is deleted immediately.

19.2.5 Assigning Accounts to a User with Oracle WebLogic Server

To assign an account to a user, use the Oracle WebLogic Server Administration Console to create a group and then assign it to one or more users. The group name must start with the @ sign and end with permissions delimited by an underscore. The following example creates a group named *testaccount* and assigns it Read, Write, and Delete permissions: @testaccount_RWD. You must also change the JpsUserProvider and ensure an underscore is in the **Accounts Permissions Delimiter** field. For more information about JpsUserProvider, see [When to Use a JpsUser Provider](#).

Accounts assigned to a user on Oracle WebLogic Server are mapped to the Content Server instance. See *Create users in Oracle WebLogic Server Administration Console Online Help*.

19.3 A Content Server Accounts Case Study

In this example, Xalco is a worldwide software company with offices in London, New York, and Paris. They have a Content Server instance hosted in the London office, with access from the other offices through the corporate WAN. At the same time, Xalco is replicating some files out to an area of their public website. Initially, the Sales and Finance departments at each location want to use their instance to publish files. The New York office is small and has no Sales department.

The following sections provide sample information for the Xalco case study:

- [Xalco Security](#)
- [Xalco Accounts](#)
- [Xalco Roles](#)
- [Roles and Permissions Table](#)
- [Roles and Users Table](#)
- [Accounts and Users Table](#)

19.3.1 Xalco Security

- Xalco staff and security levels:
 - **London:** David Smith, Worldwide CFO, and Jim McGuire, UK Sales Manager
 - **New York:** Catherine Godfrey, Regional Finance Manager
 - **Paris:** Helene Chirac, Finance Clerk (Europe)

- Xalco levels of security clearance (security groups) for Xalco content:
 - **Public:** Files suitable for consumption by members of the public (public content is replicated to the Xalco website)
 - **Internal:** Files which have unrestricted access internally, but are not suitable for public consumption
 - **Sensitive:** Files which are commercially sensitive, and restricted to middle managers and above
 - **Classified:** Highly-sensitive files, suitable only for board members
- Xalco staff access:
 - **David Smith:** As Worldwide CFO, he requires full access to all files held in the instance.
 - **Jim McGuire:** As UK Sales Manager, he must have full control of Sales files in London, and have visibility of sales activities in Paris. As a manager, he has clearance to the Sensitive level.
 - **Helene Chirac:** Based in the Paris office, she must view only files relating to Finance in Europe, and she has clearance only to the Internal level.
 - **Catherine Godfrey:** As a Regional Finance Manager based in New York, she must contribute Finance files for New York and view all other Finance documents. As a manager, she has clearance to Sensitive level.

19.3.2 Xalco Accounts

Access varies by location and job function, so this is reflected in the account structure:

- London has Finance and Sales departments, so it needs two accounts:
 - London/Finance
 - London/Sales
- New York has only a Finance department:
 - NewYork/Finance
- Paris has both Finance and Sales departments:
 - Paris/Finance
 - Paris/Sales

This results in three top-level accounts (London, NewYork, Paris) and five lower-level accounts.

19.3.3 Xalco Roles

Two roles must be created for each security group (one for Consumers and one for Contributors)

- PublicConsumer
- PublicContributor
- InternalConsumer
- InternalContributor
- SensitiveConsumer

- SensitiveContributor
- ClassifiedConsumer
- ClassifiedContributor

19.3.4 Roles and Permissions Table

To give specific users the ability to start workflows, you would need to add Admin permission and Workflow rights to the Contributor role.

Role	Public	Internal	Sensitive	Classified
PublicConsumer	R			
PublicContributor	RWD			
InternalConsumer		R		
InternalContributor		RWD		
SensitiveConsumer			R	
SensitiveContributor			RWD	
ClassifiedConsumer				R
ClassifiedContributor				RWD

19.3.5 Roles and Users Table

Role	David Smith	Helene Chirac	Jim McGuire	Catherine Godfrey
PublicConsumer		X		
PublicContributor	X		X	X
InternalConsumer		X		
InternalContributor	X		X	X
SensitiveConsumer				
SensitiveContributor	X		X	X
ClassifiedConsumer				
ClassifiedContributor	X		X	X

19.3.6 Accounts and Users Table

It would be sufficient to give David Smith RWDA permission on London, New York, and Paris accounts.

Account	David Smith	Helene Chirac	Jim McGuire	Catherine Godfrey
London/Finance	RWDA	R		R
London/Sales	RWDA		RWDA	
NewYork/Finance	RWDA			RW
Paris/Finance	RWDA			R
Paris/Sales	RWDA		R	

Managing Access Control List Security

This chapter provides information on Content Server access control lists (ACLs), which are lists of users, groups, or enterprise roles with permission to access or interact with a content item.

This chapter covers the following topics:

- [Introduction to Access Control List Security](#)
- [Configuring Access Control List Security](#)
- [Metadata Fields](#)
- [Access Control List Permissions](#)

20.1 Introduction to Access Control List Security

In addition to the standard Content Server security roles, security groups, and accounts, the Content Server can be configured to support access control lists (ACLs). An access control list is a list of users, groups, or enterprise roles with permission to access or interact with a content item.

When access control list security is configured, three new fields are available for use in several locations in the interface, including checking in content items, updating content items, and searching for content items. The fields are:

- User Access List
- Group Access List
- Role Access List

After the access control list security feature is configured for Content Server, you can use Oracle Platform Security Services (OPSS) to manage the access control lists, including the Oracle Access Manager (OAM) Authentication provider, which works with the Oracle WebLogic Server domain. See *Introduction to Oracle Platform Security Services* in *Securing Applications with Oracle Platform Security Services*.

 **Note:**

When using the RoleEntityACL component with Oracle WebCenter Content: Records, the component does not affect any retention objects such as categories or records folders. Therefore, the ability to use ACLs on a Records role is not enabled on the category creation page or folder creation page even if the RoleEntityACL component is enabled. The role ACL functionality is, however, enabled on the content check-in page.

 **Caution:**

The NeedToKnow (NtkDocDisclosure, or NTK) component supports customization for Content Server security; however, it may not work together with access control lists because of conflicting security models. For more information, see [Managing the Need to Know Component](#).

20.2 Configuring Access Control List Security

To set up access control lists (ACLs), configure the following items in Content Server:

- To support user and group access control lists, the following configuration variables must be set in the Content Server `config.cfg` file:
 - `UseEntitySecurity`: Set this variable to `true`.
 - `SpecialAuthGroups`: Set this variable to the name of the Content Server security group that will use the ACL security. Out-of-the-box Content Server has only two security groups: Public and Secure. Usually a site will create a third security group for which ACL security is to be applied.

 **Note:**

By default, security groups are not added to the `SpecialAuthGroups` list.

To set the variables:

1. Use the Administration interface for your Content Server instance to select the General Configuration page.
2. On the page, enter the variables in the **Additional Configuration Variables** field.
3. Click **Update**.

The configuration variable `UseEntitySecurity=true` sets Content Server security to always evaluate the user and group access control lists for content items. This parameter creates two metadata fields: `xClbraUserList` and `xClbraAliasList`.

- To support the enterprise role access control list, the RoleEntityACL component must be enabled in Content Server. This component is installed (disabled) by default with Content Server. To enable the component:
 1. Use the Administration interface for your Content Server instance to select the Component Management page.
 2. Click **advanced component manager** in the description paragraph of the page.
 3. In the list of Disabled Components, select the component **RoleEntityACL** then click **Enable**.
 4. Restart the Content Server instance.

 **Note:**

Ensure that the role names are either under 30 characters in length or are unique within the first 30 characters. If existing external role names are longer than 30 characters, map them to shorter names using a credential map.

For information about credential maps, see [Credential Mapping](#).

The RoleEntityACL component configures Content Server to work with other applications to evaluate the enterprise role access control list. This component turns on the `UseRoleSecurity` parameter, which sets Content Server security to integrate enterprise role access list information for content items. The `UseRoleSecurity` parameter creates the `xClbraRoleList` metadata field.

The benefit of defining roles for ACLs is that the user roles come from the enterprise security directory (for example, OID, Active Directory, and so forth), therefore the WebCenter Content administrator does not need to define them like they do with ACL groups. For more information, see the [About Access Control Lists for Roles](#) blog.

- If you want non-administrator users to be able to use the Add User menu to select users for the User Access List when checking in content items, set the configuration variable `AllowQuerySafeUserColumns=true`. If this variable is not set, no values are displayed in the menu for the **User Access List** field.

20.3 Metadata Fields

Access control lists are computed based on the values in three metadata fields: `xClbraUserList`, `xClbraAliasList`, and `xClbraRoleList`. When the metadata values are populated with user, group, or enterprise role names and permissions to a content item, they affect which users, groups, and enterprise roles are allowed to search or act on the content item.

These metadata fields are populated from the User Access List, Group Access List, and Role Access List fields, which can be viewed or accessed when checking in a content item, updating a content item, and performing a search using the expanded form.

Administrators can use scripts to specify values to populate the metadata fields for the access lists.

20.3.1 xClbraUserList Metadata Field

The `xClbraUserList` metadata field is used to specify users and their permissions for a content item.

The following list describes requirements for administrators to specify `xClbraUserList` values in scripts:

- Each user name is preceded by an ampersand (&) symbol.
- Each user's permissions follow the user name in parentheses.
- User names are separated by commas.
- **Example:** `xClbraUserList=&sysadmin(RWDA),&user1(RW),&guest(R)`

20.3.2 xClbraAliasList Metadata Field

The xClbraAliasList metadata field is used to specify groups and their permissions for a content item.

Note:

In Content Server, an alias could be used to specify a group of users (which is *not* the same as a LDAP group). For ACLs, instead of calling the implementation an alias access list, it is called a group access list. However, the metadata field name still uses the term *alias*.

The following list describes requirements for administrators to specify xClbraAliasList values in scripts:

- Each group name is preceded by an 'at' (@) symbol.
- Each group's permissions follow the group name in parentheses.
- Group names are separated by commas.
- Example: `xClbraAliasList=@Mktg (RWDA) , @Mktg_ext (RW)`

20.3.3 xClbraRoleList Metadata Field

The xClbraRoleList metadata field is used to specify enterprise roles and their permissions for a content item.

The following describes requirements for administrators to specify xClbraRoleList values in scripts:

- Each role name is preceded by a colon (:) symbol.
- Each role's permissions follow the role name in parentheses.
- Role names are separated by commas.
- Example: `xClbraRoleList=:role1 (RWDA) , :role2 (RW)`

20.4 Access Control List Permissions

Access control list permissions determine what type of access a user, group, or enterprise role has to a content item. The following permissions can be granted:

Permission	Description
Read (R)	Allowed to view the content item.
Write (W)	Allowed to view, check in, check out, update, and get a copy of the content item.
Delete (D)	Allowed to view, check in, check out, update, get a copy, and delete the content item.
Admin (A)	Allowed to view, check in, check out, update, get a copy, and delete the content item, and check in a content item with another user specified as the Author.

 **Note:**

Access control list permissions do not apply to users with the Content Server admin role.

However, a user can access content without being included on the ACL if the user has the Oracle WebCenter Content admin role or has a role that gives the user Admin permission to the security group of the content item.

To associate access control lists with a content item, you add one or more users, groups, or enterprise roles when checking in or updating a content item. For each user, group, or role you add to an access list, you assign the appropriate permission: Read (R), Write (W), Delete (D), or Admin (A). Access control list permission levels are the same as defined for Content Server security groups and accounts. When users are added to any one of the access lists, the users have the specified permissions to access the content item.

At least one of the following must be true for a user to be granted a particular permission:

- The user's name appears in the xClbraUserList metadata field with the appropriate permission.
- The user belongs to a group that appears in the xClbraAliasList metadata field with the appropriate permission.
- The user is part of an Enterprise role that appears in the xClbraRoleList metadata field with the appropriate permission.

Access control list permissions are cumulative. If you assign Write, you automatically assign Read. If you assign Admin, you automatically assign Read, Write, and Delete.

However, users must also satisfy security criteria for access through the Content Server security group and the account (if Accounts are enabled). If any of these security criteria deny a certain permission, users will not have that permission to the content item.

When a user searches for a content item, all three ACL rights fields are combined as an "OR" condition. That result is combined in an "AND" condition with the result of the Security Group and Account fields. The user conducting the search must have Read permission to the security group, to the account (if accounts are enabled), and to at least one of the three ACL fields to be able to find the content item.

20.4.1 Empty Access Control List Fields

If all the User Access List, Group Access List, and Role Access List fields are empty, then by default permission is granted to all users. If only the User Access List and Group Access List fields are blank (and the RoleEntityACL component is *not* enabled so there is no Role Access List), permission is granted to all users. This behavior is configured with the `AccessListPrivilegesGrantedWhenEmpty` variable, which is set to TRUE by default.

If the `AccessListPrivilegesGrantedWhenEmpty` variable is set to FALSE, then when all access control lists are blank, permission is denied to all users except those with the admin role. For a user without the admin role to be able to check in documents, the user must have an access control list role (such as *testrole*) with Read/Write (RW) privileges and specify the role when checking in documents.

 **Note:**

If the Content Server instance has been upgraded from release 10g, be aware that empty access control lists will behave differently in Release 11g. Release 10g and earlier had the equivalent configuration of `AccessListPrivilegesGrantedWhenEmpty=false`. The default for releases 11g, 12c, and 14c is `AccessListPrivilegesGrantedWhenEmpty=true`.

21

Managing Additional Content Server Security Connections

This chapter provides information on additional security connection options for use with Content Server.

This chapter covers the following topics:

- [Proxy Connections](#)
- [Credential Mapping](#)
- [Secured Connections to Content Server](#)
- [Connections Using the HTTP Protocol](#)

21.1 Proxy Connections

Proxy connections, or connections between Content Server instances, provide additional levels of security for Content Server through the following functions:

- Security credentials mapping from one Content Server instance to another Content Server instance.
- Secured "named" password connections to Content Server instances (password protected provider connections).
- HTTP protocol communication between Content Server instances.

While it is possible to use both named password connections and HTTP-based Content Server communication, it is most likely that one type of connection will be more useful. For both types of connections, credentials mapping can provide additional security.



Note:

A site can have multiple Content Server instances, but each Content Server instance must be installed on its own Oracle WebLogic Server domain.

The ProxyConnections component is installed (enabled) by default with Content Server. Typical uses of Proxy Connections include the following:

- To provide the capability to perform archive replication of content items over HTTP or HTTPS. For example, a company has acquired another company, but they do not have a common infrastructure for sharing information. Both companies have a secure sockets layer (SSL) connection to the Internet. The company wants to share content between the two sites. Proxy Connections can be used to set up a secure Internet connection between the companies' servers so that content can be securely accessed from one site, replicated, and archived at the other site.
- To better restrict access to Content Server instances by using *named* passwords to target proxy connections. For example, a company wants to apply additional security to connections coming from one Content Server instance to another Content Server instance.

Using named passwords, an administrator can restrict access by incoming connections to those with preset proxy connections and named passwords.

21.2 Credential Mapping

A *credential map* is a mapping of credentials used by a Content Server instance to credentials used in a remote system, which tell the Content Server instance how to connect to a given resource in that system. Administrators can create multiple credential maps for users, roles, and accounts. Credential mapping can be useful in a proxy scenario, for example, where credentials for users, roles, or accounts created on one Content Server instance can be mapped to the users, roles, or accounts on another Content Server instance, thus allowing users controlled access to information on more than one Content Server instance for tasks such as searching.

This section covers the following topics:

- [About Credential Mapping](#)
- [Credential Values](#)
- [Matching Accounts and Roles](#)
- [Proxy Credentials Map](#)
- [Creating a Credential Map](#)

21.2.1 About Credential Mapping

When you create a credential map you enter a unique identifier for the map and specific credential values for users, roles, and accounts. In a proxy connection, when user credentials match an input value, then the user is granted the credentials specified in the output value. The user credentials are evaluated in the following order:

1. All the roles.
2. All the accounts.
3. The user name.

After the translation is performed, the user only has the attribute values that were successfully mapped from input values.

When you have created credential maps, you can specify a credential map along with a named password connection when configuring an outgoing provider. You also can specify a credential map when configuring a user provider (such as LDAP).

The default behavior for a LDAP provider is that the guest role is not automatically assigned to users.

Credential mapping implementation is duplicated in the web server plug-in and in Oracle WebCenter Content. It is designed and implemented for optimal performance, so that any changes in the mapping are applied immediately. (This can be compared to performance in NT or ADSI user storage using the NT administrator interfaces, where changes are cached and not reflected in the Content Server instance for up to a couple of minutes.)

**Note:**

For information on credential mapping outside of a Content Server instance, see Credential Mapping Providers in *Developing Security Providers for Oracle WebLogic Server*.

21.2.2 Credential Values

A credential input value is matched if there is an exact match in the case of a role or user name. An input account value is matched if one of the user accounts has a prefix, except for the case of a filter (see [Matching Accounts and Roles](#)). For example, the following credential values reduce all users who might otherwise have the admin role to instead have the guest role:

```
admin, guest
```

The following table lists the basic syntax for credential values:

Value	Prefix or Sequence	Example
User name	&	&name
Role		admin
Account	@	@marketing
Empty account	@#none	@#none
All accounts	@#all	@#all
Ignore the value or "comment out" the value	#	#comment

You can view which credentials are applied by default if no credential map is assigned. Use the following mapping, which maps everything without change. This mapping first filters all roles, then all accounts.

```
|#all|,%%
@|#all|,@%%
```

For more information about mapping syntax see [Matching Accounts and Roles](#).

▲ Caution:

If your credential map does not at least assign the minimum set of privileges that an anonymous user gets when visiting the Content Server website, then logged in users may experience unusual behavior. For example, a common reaction for a browser that receives an `ACCESS DENIED` response is to revert back to being an anonymous user. In particular, a user may experience unpredictable moments when it is possible or not possible to access a document (depending on whether at that moment the browser chooses to send or not to send the user's authentication credentials). This is particularly true of NTLM authentication because that authentication has to be renewed periodically.

21.2.3 Matching Accounts and Roles

A special filter is available for matching accounts and roles. For example, the syntax for an account filter is designated by starting the account value with specifying the prefix `@|` and ending with a `|` (for example, `@|accountname|`). The pipe (`|`) represents a command redirection operator that processes values through the filter. For proxy connections a space-separated list of accounts is specified; each account optionally starts with a dash (`-`) to denote a negative value. A filter is matched if any of the specified account strings that do not start with a dash are a prefix for a user account and all of the account strings that do start with a dash are not prefixes for that user account.

▲ Caution:

The filter will not map the account `@#all`. The `all accounts` account value must be mapped explicitly by using `@#all`, `@#all` mapping.

Roles can be mapped (using the same rules) by removing the `@` sign from the beginning of the filter. For example, the following input value passes through all roles except those that begin with the prefix `visitor`. Note that the expression `#all` matches all roles.

```
|#all -visitor|, %%
```

21.2.3.1 Reference Input Value

The special sequence `%%` in the output value can be used to reference the input value. For example, given the following mapping, any account that did not start with `financial` as a prefix would map to the same account but with the prefix `employee/` attached at the front:

```
@|#all -financial|, @employee/%%
```

If a user had the account `marketing`, then after the mapping the user would have the account `employee/marketing`.

21.2.3.2 Privilege Levels

A particular privilege level (read, write, delete, all) can be granted to an account in the output value by following the account specification with the letters "R", "W", "D", or "A" enclosed in

parentheses. For example, all the privilege levels for all the accounts could be reduced to having read privilege by the following syntax:

```
@|#all -financial|, @employee/%%(R)
```

21.2.3.3 Substitution

In certain cases it is useful to remove a prefix before the substitution %% is applied. An offset for the substitution can be specified by using the syntax %%[n] where n is the starting offset to use before mapping the input value into the %% expression. The offset is zero based so that %%[1] removes the first character from the input value. For example, to remove the prefix DOMAIN1\ from all roles, the following expression can be used:

```
|domain1\|, %%[8]
```

Another use for this function might be to replace all accounts that begin with the prefix marketing/ and replace it with the prefix org1/mkt. The expression for this would look like the following:

```
@|marketing|, @org1/mkt/%%[10]
```

21.2.3.4 Special Characters

In certain cases roles have unusual characters that may be hard to specify in the input values. The escape sequence %xx (where xx is the ASCII hexadecimal value) can be used to specify characters in the input value. For example, to pass through all roles that begin with #, & |@ (hash, comma, ampersand, space, pipe, at) the following expression can be used:

```
|%35%2c%26%20%7c%40|, %%
```

21.2.4 Proxy Credentials Map

A proxy credentials map is applied after initial credentials are assigned to the user. This mapping example takes an account value assigned to the user (not to a LDAP group) and grants them the same account value:

```
@|Public|, @Public
```

If you do not apply a suffix such as (R), then whatever privileges the account had before the mapping, it will have after the mapping. If you want to degrade the privileges from the defaults assigned by the LDAP map, try this construction:

```
@|Public|, @%%(R)
```

The %% refers to the *input* account value that was matched by the prefix: Public. For example, if the user has the account Public/mysuffix, then %% would have the value Public/mysuffix when it is picked up by the |Public| prefix filter.

21.2.5 Creating a Credential Map

To create a credential map:

1. Open a new browser window and log in to the Content Server instance as the system administrator.
2. Choose **Administration**, then **Credential Maps**.

3. In the Credential Maps page, enter the unique identifier for the credentials map you are creating.

More than one named password connection can be used to connect to a Content Server instance. Each named password connection can have a different credential map.

4. Enter values in two columns with a comma to separate the columns and a carriage return between each row of values. The first column specifies input values and the second column specifies output values.

5. Click **Update**.

To apply a credential map to roles and accounts retrieved using NT integration, set the Content Server configuration entry `ExternalCredentialsMap` to the name of the credential map of your choice.

21.3 Secured Connections to Content Server

Secured connections to Content Server instances can be supported by creating password protection on incoming requests. A Content Server instance can communicate with another Content Server instance in a password protected fashion.

This section covers the following topics:

- [About Named Password Connections](#)
- [Guidelines for Proxy Connections Data](#)
- [Creating a Proxy Connection](#)

21.3.1 About Named Password Connections

Using the Proxied Connection Authentication/Authorization Information page you can create *named* passwords, which are passwords that you assign to specific connections by name. Each named password can be associated with a host and IP address filter on both the direct socket communication to a Content Server instance and on any communication performed through the controlling web server (the HTTP filter) for a Content Server instance. When an outside agent (such as a web server for another Content Server instance) wants to communicate with the Content Server instance, it can use a named password connection. A named password connection also can be associated with a credentials map so that the privileges of users accessing the Content Server instance can be reduced or changed.

Proxy connections entry fields are provided in the forms for configuring outgoing socket providers and outgoing HTTP providers in which you can specify a named password connection. (To view provider selections for your instance, choose **Administration**, then **Providers**.)

Passwords are hashed (using SHA1 message digest) with their allowed host and IP address wildcard filter on the client side. If the copy of a stored password is exposed, it will only allow access from clients that satisfy both the host and IP address filter.

The expiration implementation for passwords means that the various servers involved must have their clocks reasonably synchronized (within a few minutes at least).

▲ Caution:

All passwords are hashed by a time-out value before being sent to a server. If a password value is exposed while in communication to a server, the password will only be usable until the expiration time (approximately fifteen minutes after the time the request is issued). Also, the password will only be usable in a replay attack from the same source host and IP address, as previously described. If firewall-protected internal host and IP addresses are not being used, a very committed attacker could spoof the host and IP addresses by hijacking any of the major DNS servers, an event that has occurred in at least a couple of cases.

21.3.2 Guidelines for Proxy Connections Data

The data you enter in the Proxied Connection Authentication/Authorization Information page defines different passwords that can be used by external agents to connect to a Content Server instance. Instead of an external agent being forced to provide a password for each user, which may be unavailable to the client for many reasons (such as message digest algorithms that do not use clear text passwords), proxy connections enable the agent to authenticate using a single named connection password. Each named password connection can be linked to rules to restrict which hosts can connect to the Content Server instance and to control the privileges granted to users. Each named password connection is uniquely identified, and the calling agent must supply the identifier along with the password.

The host name and IP address filters are used to determine which host names or IP addresses are allowed to use a named password connection when performing direct socket connections to a Content Server instance. The rules for defining the filters are identical to those defined in the System Properties editor (the wildcard symbols * = *match 0 or many* and | = *match either or* can be used to create flexible rules). If an entry is empty then it provides no restriction on its target attribute (either the host name or IP address of the client depending on which of the following two fields is involved).

Two options are implemented through the Providers page:

- Whenever you add an outgoing provider you have the option to use named password connections and to choose whether the provider is a connecting server (so that web access and security is controlled through a remote server).
- Whenever you add a user provider (such as LDAP) you can choose to use an available credentials map.

No credentials maps are defined in the Proxied Connection Authentication/Authorization Information page. For information on creating a credentials map, see [Credential Mapping](#).

21.3.3 Creating a Proxy Connection

To create a proxy connection:

1. Open a new web browser window and log in to the Content Server instance as the system administrator.
2. Choose **Administration**, then **Connection Passwords**.
3. In the Proxied Connection Authentication/Authorization Information page, enter information for the fields. If credentials maps exist, you can choose to use an existing credentials map, or you can create one to be used for the proxy connection.
4. Click **Update**.

21.4 Connections Using the HTTP Protocol

Administrators can create a proxy connection between Content Server instances using the HTTP protocol. For example, you could have two Content Server instances where both have web servers for accessing their functionality. If you have a large number of users who want to use web browsers to access information on one of the Content Server instances, but not all the users can access that server directly, this feature can be useful.

The HTTP protocol can be useful for transferring Content Server archives. The HTTP provider works with Secure Sockets Layer (SSL), the HTTPS protocol, which enables secure communication between two Content Server instances.

This section covers the following topics:

- [Using HTTP Protocol for Content Server Connection](#)
- [Configuring the HTTP Provider](#)

21.4.1 Using HTTP Protocol for Content Server Connection

Administrators can implement a httpoutgoing provider, configurable through the Providers page, which allows communication from one Content Server instance to another Content Server instance.

If you choose to add a httpoutgoing HTTP provider, you have the following additional options:

- Specify a CGI URL
- Specify a named password connection and client IP filter

To view the httpoutgoing HTTP provider selection, from the Content Server portal, choose **Administration**, then **Providers**.

Creating a proxy connection between Content Server instances can take some preparation. The Content Server instances must not use the same relative web root for their weblayout directories. It may require some component architecture changes to provide the extra navigation links between the servers.

If you set up one Content Server instance with its web server using SSL and the other server's front end uses HTTP, then users who try to access the first server by modifying the other server's URL in a web browser can get an error because of the differences between HTTPS (requiring a credential) and HTTP. To resolve this issue, use the `BrowserUrlPath` component, available with Content Server. For more information, see [Browser URL Customization](#).

21.4.2 Configuring the HTTP Provider

To configure the HTTP provider:

1. Add a httpoutgoing provider on the first Content Server instance.
 - a. In a browser, go to the Administration page and click **Providers**.
 - b. Click **Add** next to the httpoutgoing provider type.
 - c. Enter the necessary information for the httpoutgoing provider. For more information see the table for the Outgoing Http Provider page.
2. Create a proxy connection on the second Content Server instance that uses the named password connection and connection password that you specified in the previous step.

- a. On this server, choose **Administration**, then **Connection Passwords**.
- b. Fill in the information for the connection. The IP address filter entry should have the IP address of the first server.

Customizing Content Server Communication

This chapter provides information on how to customize access to and communication with a Content Server instance.

This chapter covers the following topics:

- [Login/Logout Customization](#)
- [Browser URL Customization](#)
- [Extended User Attributes](#)

22.1 Login/Logout Customization

The ExtranetLook component can be used to customize user access by suppressing the interface for users who are not authenticated by an Oracle WebLogic Server user store through error and challenge pages issued by the web server. For information about changing the interface, see *Alter the Anonymous User Interface* in *Developing with Oracle WebCenter Content*.

The ExtranetLook component is installed (disabled) by default with Content Server. To use the component, you must enable it with the Advanced Component Manager.

22.2 Browser URL Customization

The BrowserUrlPath component provides support for determining URL paths used in certain configurations of Content Server and web servers. This component is installed (disabled) by default with Content Server. To use this component you must enable it with the Advanced Component Manager.

This component is valid for a Content Server instance deployed on an Oracle WebLogic Server domain and located behind a load balancer.

This section covers the following topics:

- [About BrowserUrlPath Customization](#)
- [Affected Idoc Script Variables and Functions](#)
- [Determining the URL Path](#)
- [Changing Absolute Full Path Computation](#)

22.2.1 About BrowserUrlPath Customization

The BrowserUrlPath component overrides certain Idoc Script variables and functions, adds computation to certain variables, and provides additional configuration entries for determining URL paths. The BrowserUrlPath component is only supported with Trays and Top Menu layouts for the Content Server native user interface.

- You can configure a system with different web server front ends. One front end can use HTTP and the other can use HTTPS so that the Content Server instance can be accessed simultaneously by websites using HTTP and HTTPS. You then must apply the

BrowserUrlPath component to enable the Content Server instance to handle both types of access.

- If you are using a load balancer that forwards itself as the HTTP host header, then you must apply the BrowserUrlPath component.

BrowserUrlPath configuration variables may be placed in the *IntradocDir/config/config.cfg* file.

 **Caution:**

The BrowserUrlPath component requires extensive configuration using the variables. You may want to back up your configuration before modifying variables

In typical scenarios, the web server will forward to the Content Server instance two critical pieces of information:

- HTTP_HOST: The host header that the browser sends, identifying the host as it appears to the user in their browser address bar.
- SERVER_PORT: The port the browser uses in connecting to the Content Server instance.

The browser-based full address is used for two critical pieces of functionality:

1. Automatic creation of URLs in the side frame of the Trays layout for the Content Server instance. In particular, the side mini-search requires a prediction of the full URL, not just the relative URL.
2. The secondary URL (the #xml-http... piece following the PDF URL) that does highlighting for PDF documents.

Without any additional configuration, the BrowserUrlPath component augments the functionality of certain variables, so if SERVER_PORT has the value 433, then the component assumes the protocol is HTTPS instead of HTTP. Likewise, if SERVER_PORT does not have the value 433, then the component assumes the browser issued the request using HTTP and not HTTPS. This enhancement allows both a SSL (HTTPS) and non-SSL web server (HTTP) to access the same Content Server instance.

This component also has special functionality for WebDAV access. The configuration entry WebDavBaseUrl is augmented so that its usage is dynamic (its host and protocol vary using the "absolute" path rules).

 **Caution:**

The functionality for WebDAV access alters the behavior of CHECKOUT and OPEN functions on some Content Server pages, and alters some behavior in the Site Studio client.

22.2.2 Affected Idoc Script Variables and Functions

The BrowserUrlPath component overrides the computation of the following Idoc Script variables and functions:

- HttpBrowserFullCgiPath

- `HttpWebRoot`
- `HttpCgiPath`
- `HttpAdminCgiPath`
- `HttpImagesRoot`

The `BrowserUrlPath` component adds computation for the following variables:

- **`HttpBrowserFullWebRoot`**: Defines the full URL path to the web root of the current Content Server instance using values supplied from the user's current browser's address bar. This variable is similar to `HttpBrowserFullCgiPath` except it is for the web root instead.
- **`HttpAbsoluteWebRoot`**: Defines the universal full URL path to the web root of the current Content Server instance. It can have a different protocol or host name than the path in `HttpBrowserFullWebRoot`. For example, if the user specifies an IP address for the host name, the `HttpBrowserFullWebRoot` variable might pick up the IP address, but the `HttpAbsoluteWebRoot` variable would ignore it and use the appropriate internally configured host name.
- **`HttpAbsoluteCgiPath`**: Defines the universal full dynamic root URL for the current Content Server instance. This is the path that executes the plug-in code in the web server that makes calls for dynamic content from the Content Server instance. It can have a different protocol or host name than the path in `HttpBrowserFullCgiPath`. For example, if the user specifies an IP address for the host name, the `HttpBrowserFullCgiPath` variable might pick up the IP address, but the `HttpAbsoluteCgiPath` variable would ignore it and use the appropriately internally configured host name.

In the case of the browser path variables `HttpBrowserFullCgiPath` and `HttpBrowserFullWebRoot`, the implementation code determines what the user is currently using for protocol (HTTP versus HTTPS), port number, and host name in the browser. It bases this determination on what the web server receives in its request.

22.2.3 Determining the URL Path

The `BrowserUrlPath` component supports the following configuration entries for guessing the URL path as the browser determines it:

- **`HttpIgnoreWebServerInternalPortNumber`**: When set to true, this disables the use of the `SERVER_PORT` parameter. This entry is useful in a load balancing scenario where `SERVER_PORT` is not the port used by the browser, but is the port used by the load balancer to communicate with the web server. Enabling this entry will make it impossible (without the `BrowserUrlPath` component) for the Content Server instance to determine which port the browser used to access the web server. Without additional `BrowserUrlPath` configuration, this variable makes it impossible to both support a SSL and non-SSL address to the same Content Server instance. Using this variable prevents a load balancing configuration problem in which the load balancing server is using a different port number than the internal web server actually delivering the response to the request.
- **`HttpIgnoreServerNameForHostName`**: When set to true, this disables the fallback logic where if the `HTTP_HOST` parameter is missing, the Content Server will typically look for the parameter `SERVER_NAME` (the web server's self identification).
- **`HttpBrowserSSLPort`**: Only use this configuration entry if the `SERVER_PORT` entry is forwarded to the web server that communicates to the Content Server instance. This entry is used to decide whether a request is HTTPS or HTTP by comparing it with the `SERVER_PORT` parameter. The default `SERVER_PORT` value is 443. If you use HTTPS, but use a port other than 443, you must use this entry to set the expected HTTPS port number.

- **HttpBrowserUsesSslCookie:** If you want to look in the cookie to see if it indicates whether to use SSL or not, set this entry to true.
- **HttpBrowserIsSslCookieName:** Only use this entry if the `HttpBrowserUsesSslCookie` entry is enabled. Set the entry to the name of the cookie used to determine whether the server believes the browser is using SSL or not. The default is the cookie name `UseSSL`. The value of the cookie can be 1 or 0 (zero). If a cookie with this name is present, then it will supersede other rules for determining whether to use SSL.
- **HttpBrowserUseHostAddressCookie:** When set to true, this specifies to use a cookie to determine the full host name of the browser (the part between the protocol and the relative web address).
- **HttpBrowserHostAddressCookieName:** This entry is enabled only if `HttpBrowserUseHostAddressCookie` is enabled. Use this entry to specify the name of the cookie used to determine what the server believes is the browser's current host name. The host name part of the protocol can include the port number. For example, `HttpbrowserHostAddressCookieName=myhost:81` would specify the host `myhost` using the webport `81`. If you do use this cookie, then it is unlikely that you need to enable `HttpBrowserUsesSslCookie`, because if you use `myhost:433`, that will translate to `https://myhost/%rest-of-url%`.

22.2.4 Changing Absolute Full Path Computation

The `BrowserUrlPath` component supports the following configuration entries for changing how the absolute full path is computed. This is useful for email, where it is better to use a specific host name and protocol, even if the browser shows a different URL. This path is considered the *absolute* or *universal* path.

- **HttpBrowserAbsoluteUrlHasRelativeSSL:** When set to true, this variable allows a URL computed on the Content Info page to change from HTTP to HTTPS (or the other way if `UseSSL` is enabled in the `config.cfg` file), depending on what Content Server determines as the current use in the user's browser. The change between HTTP and HTTPS also changes the computation of the URL for creating the email body for the "email to" links. This configuration has no effect on automatically generated e-mail.
- **HttpBrowserAlternateWebAddress:** Specifies an alternate absolute host web address (host name plus optional port number). For example, `HttpBrowserAlternateWebAddresss=host_name:447`. This web address is used for the absolute path computation if the current SSL choice is different from the default for the Content Server instance. This configuration has no effect on automatically generated e-mail.
- **HttpBrowserAbsoluteUrlUsesBrowserPath:** When set to true, if browser path information can be computed, then the absolute path will use the browser path. This essentially turns off the absolute path except for background activities (such as sending notification e-mail).

22.3 Extended User Attributes

The `ExtendedUserAttributes` component enables administrators to add extended security attributes to Content Server users. The extended security attributes are merged into pre-existing user attributes and enable additional flexibility in managing users. For example, roles and accounts attributes can be added to external LDAP users without needing to perform internal setup. Also, roles and accounts attributes can be added to users for a customized application separately from base user attributes.

The ExtendedUserAttributes component is installed (enabled) by default with Content Server. Services installed for the ExtendedUserAttributes component are described in the Extended User Attributes Services in *Services Reference for Oracle WebCenter Content*.

This section covers the following Extended User Attributes topics:

- [ExtUserAttribInfo ResultSet](#)
- [Configuration Variable for Extended User Attributes](#)

In addition to these resources, there are added queries which can be used to gather data for extended user attributes. The queries can be viewed in the Component Wizard or by looking in the `WC_CONTENT_ORACLE_HOME/ucm/idc/components/ExtendedUserAttributes/resources/extendeduserattributes_query.htm` file.

22.3.1 ExtUserAttribInfo ResultSet

ExtUserAttribInfo is the ResultSet used by Content Server to handle extended user attributes. It is similar to the UserAttribInfo ResultSet used for handling regular user attributes, with some additional information.

This ResultSet has three columns. You can supply one attribute per row or multiple attributes on a single row (per application). The following columns are included:

- **dUserName:** The user whose attributes are being described.
- **dApplication:** The application to which those attributes are linked.
- **AttributeInfo:** The attribute information. This is a comma-separated entry consisting of three items:
 - **attribute type:** usually either a role or account, depending on if a security group or account is being defined for the user
 - **attribute name:** the title of the role or account
 - **attribute privilege:** a definition of rights given to the user. Rights are defined according to UNIX conventions:
 - * 1: read permission
 - * 2: write permission
 - * 4: delete permission
 - * 8: admin

For example, the entry `role,contributor,3` gives the user permission to read and write in the contributor security group.

Multiple AttributeInfo entries can be added in a single row, separated by commas. For example, this entry adds two attributes into the AttributeInfo row:

```
role,guest,15,account,\#all,15.
```

The following is an example of this ResultSet:

```
@ResultSet ExtUserAttribInfo
3
dUserName
dApplication
AttributeInfo
jsmith
appl
role,contributor,15
jsmith
```



```
app2
account,abc,15,account,xyz,15
@end
```

22.3.2 Configuration Variable for Extended User Attributes

The following configuration variable can be set in Content Server and is useful if you are working with default attributes:

- `DefaultAttributesCacheTimeoutInSeconds`: Defines how long the default attribute cache remains active (default = 600).

Part VI

Administering System Migration and Archiving

This part provides information on moving Oracle WebCenter Content system content information from and to the Oracle WebCenter Content system. Activities include moving information to and from archives, moving information between archives or system installations, and moving information from other systems to Oracle WebCenter Content.

This part contains the following chapters:

- [Understanding System Migration and Archiving](#)
- [Migrating System Configurations](#)
- [Managing Archives, Collections, and Batch Files](#)
- [Exporting Data in Archives](#)
- [Importing Data from Archives](#)
- [Transferring Files](#)
- [Replicating Files](#)
- [Migrating the Folders Structure](#)
- [Archive and Migration Strategies](#)
- [Using Archiver Replication Exceptions](#)

Understanding System Migration and Archiving

This chapter describes the various methods and software tools used to migrate and archive (back up) Oracle WebCenter Content system metadata, content, and structure.

This chapter covers the following topics:

- [Introduction to Migration Tools and Components](#)
- [Configuration Migration Utility](#)
- [Archiver Application](#)
- [Folder Archiving Application](#)
- [ArchiveReplicationExceptions Application](#)
- [Archive Tool Summary and Comparison](#)

23.1 Introduction to Migration Tools and Components

Several tools are available for archiving and migrating information from and to a Content Server instance. Each tool serves a different purpose and most can be used together.

- **Configuration Migration Utility:** Use to select elements of your Content Server instance to migrate to another instance.
- **Archiver:** A Java applet for transferring and reorganizing Content Server files and information. You can use the Archiver with the Configuration Migration utility to migrate a complete Content Server instance, including content, from one system to another. Supports Contribution Folders for moving content, but supports migrating only tables for Folders.
- **Folder Archiving:** Use to migrate the Contribution Folders structure of your Content Server instance from one location to another.
- **Folder Structure Archive:** Use to copy the Contribution Folders structure (and its content) and create an exact copy on another computer. It ensures that the folder copies and respective contents remain synchronized across different systems.
- **Archiver Replication Exceptions:** Use to prevent failed imports from stopping replication.

23.2 Configuration Migration Utility

The Configuration Migration utility (provided by the ConfigMigrationUtility component) is used to select elements of your Content Server instance to migrate to another instance. This component is installed and enabled by default with Content Server.

Overview

You can select individual elements (such as workflow tokens or content types) or entire sections (such as all user-related metadata or all metadata related to workflows). In addition, you can export and import an entire Content Server instance to create a snapshot of the Content Server instance at a certain point in time. It can be used to migrate a system from

testing to production, or to provide an upgrade path from older versions of the Content Server instance. By using the migration tool, you can keep an older version of the Content Server software in production while testing new functionality on a newer version.

Each export configuration is packaged as a *bundle* which contains the information needed to re-create the configuration on another system. A bundle is a zip file that can be easily shared with other systems.

Functions

The Configuration Migration utility is used to configure migration bundles for exporting to other systems. It is also used to upload and import bundles on an importing system. There are four main functions:

- **Upload Bundle:** used to find a copy of an exported bundle and make it available for use on a receiving system.
- **Configuration Bundles:** used to import the configuration from the uploaded bundle. This function creates new metadata fields or overwrites current fields, depending on options chosen during import.
- **Configuration Templates:** used to create *export bundles*, which can later be uploaded and imported to another Content Server instance.
- **Recent Actions:** used to view recent activity such as imports and exports and to view a log of those activities.

By using the Configuration Migration utility with the Archiver, you can create a snapshot in time of your existing Content Server instance or you can use it to keep track of incremental updates to an existing system. The Configuration Migration utility captures configuration information while the Archiver captures content.

For more information about using the Configuration Migration utility, see [Migrating System Configurations](#).

23.3 Archiver Application

Archiver can be used with the Configuration Migration utility to migrate a complete Content Server instance, including content, from one system to another.

Caution:

Do not use Archiver as your primary method of disaster recovery; use standard backup systems for the database and file system.

 **Note:**

Archiver does *not* include Digital Asset Management (DAM) video and audio renditions in the archives it creates. The archives do include the native file, thumbnail, the zip rendition that contains storyboard thumbnails, and the web-viewable `.hosp` file, but do not include any additional video and audio renditions created by Inbound Refinery.

This limitation is by design. Many video files would make the archive too large, surpassing the 2 GB limit on zip files. Also, in many production instances the video renditions are likely to be stored on a separate file system.

 **Note:**

When using the Archiver with the Electronic Signatures component, make sure to use the table archive feature to move the Esig table. If this is not done, an error is returned in the Signatures Listing section on the Signatures Information page after clicking the Signatures tab on a Content Information page.

Overview

Archiver can be run as an Admin Applet accessed from the Administration menu, or as a standalone tool. The standalone tool is necessary to:

- Create collections
- Create a new archive by copying from an existing archive
- Browse the local file system to connect to new collections

For more information, see [Running Archiver as a Standalone Application](#).

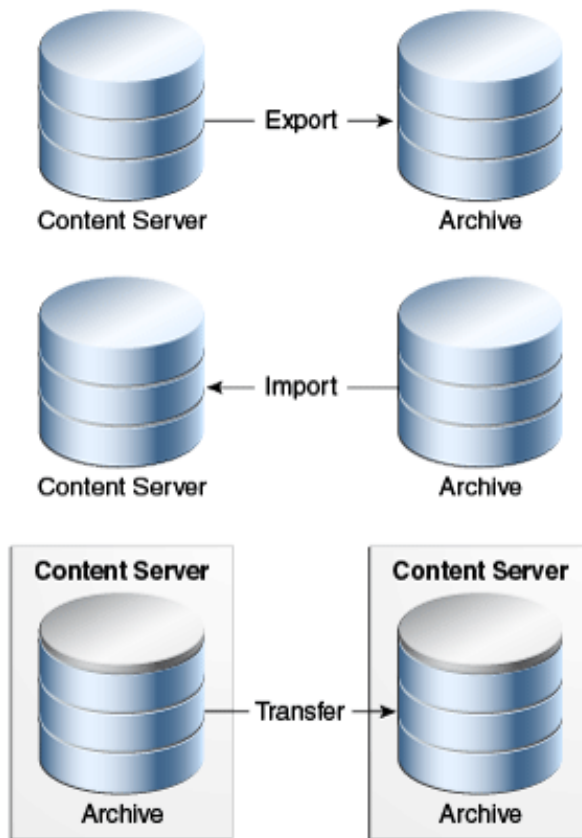
Functions

Archiver is a Java applet that is used to transfer and reorganize Content Server files and information. Archiver has four main functions:

- **Export:** Used to copy native and web-viewable files out of the Content Server instance for backup, storage, or import to another Content Server instance. You can also export content types and user attributes. You export to an *archive*, which contains the exported files and their metadata in the form of *batch files*.
- **Import:** Used to retrieve files and Content Server information from an exported archive. Importing is typically used to get a copy of content from another Content Server instance or to restore data that has been in storage. You can also change metadata values during an import.
- **Transfer:** Used to transfer content from one Content Server instance to another instance over sockets. This is typically used to move or copy content across a firewall or between two Content Server instances that do not have access to the same file system. You can also use the Transfer function to transfer archive files between Content Server instances that have access to the same file system.
- **Replicate:** Used to automate the export, import, and transfer functions. For example, you can use replication to automatically export from one Content Server instance, transfer the archive to another computer, and import to another Content Server instance.

The following illustration demonstrates these basic functions.

Figure 23-1 Archiver Functions



23.4 Folder Archiving Application

You cannot use the Archiver to move folder structure and content, but you can use Folder Archiving to migrate the total folder structure of your Content Server instance from one location to another. This does not archive the folder content, just the folder structure.

Using Folder Archiving you can export and import the folder hierarchical structure directly from the Folders administration interface. The entire folder hierarchy is exported to a text file in HDA format, which can then be read by the Content Server instance when it is imported.

23.5 ArchiveReplicationExceptions Application

The `ArchiverReplicationExceptions` component is installed (enabled) by default with the Content Server instance. It enables administrators to prevent failed imports from stopping replication. It does this by capturing failed imports and putting them into an *exceptions* archive, then sending email to the administrator that a failed import has occurred.

For content items to be processed by the `ArchiverReplicationExceptions` component, the administrator must manually set configuration entries in the `IntradocDir/config/config.cfg` file. The configuration variables customize the behavior of the importing Content Server instance to allow for certain situations and to distribute the error reporting based on the configured criteria.

23.6 Archive Tool Summary and Comparison

The tools that can be used to archive Content Server structure, content, and folders all serve different purposes. All of the tools can be used together, but sometimes one might be preferred over the other. The following table summarizes each tool and its strengths and limitations.

Feature	Configuration Migration Utility (CMU)	Archiver	Folder Archiving	Folder Structure Archive Component
Primary purpose	A 'snapshot' tool, used to migrate one Content Server instance to another or to migrate to an upgraded instance. Supports only Contribution Folders.	Primarily used for backup, storage, and transfer of data over sockets. Supports Contribution Folders. Supports only migrating tables for the FrameworkFolders component.	Used to export and import a complete folder structure or hierarchy. Supports only Contribution Folders.	Used to backup and duplicate a folder structure to synchronize the contents with another Content Server instance. Supports only Contribution Folders.
Strengths	Enables you to choose specific parts of the Content Server instance to migrate. Provides logging and trace files.	Works with older content. Provides logging and trace files.	Ensures that the collection IDs on the target match those on the source.	Can export selected portions of the folder structure.
Limitations	Cannot be used on pre-6.2 versions of the Content Server software. Migration of components can be difficult.	The standalone version is needed to create collections. Imported revisions do not automatically enter a workflow.	All current folders and content items in the folders are removed from the Content Server instance and replaced by the imported folder hierarchy.	Does not ensure that the collection ID of folders on the target match those on the source content.
What it archives	<ul style="list-style-type: none"> • Metadata • Security (roles and accounts) • Profiles • Schema • Workflow • Personalization • Add-on components • 	<ul style="list-style-type: none"> • Content • Content types • User attributes • Subscriptions • Security groups • File Formats 	<ul style="list-style-type: none"> • Complete folder hierarchy (no content) 	<ul style="list-style-type: none"> • Complete or partial folder hierarchy and content • Only changed content (if desired)

Feature	Configuration Migration Utility (CMU)	Archiver	Folder Archiving	Folder Structure Archive Component
What it does not archive	<ul style="list-style-type: none"> • Content • Workflow state • Does not synchronize: this is an additive archive 	<ul style="list-style-type: none"> • Folder structure • Metadata, security and other features which are archived by CMU • Weblayout structure 	<ul style="list-style-type: none"> • Partial or selected folder hierarchy • Collaboration folders • Content • Metadata, security (other features which are archived by CMU) 	Collaboration folders

24

Migrating System Configurations

This chapter provides information on using the Configuration Migration utility with the Archiver utility to migrate content and export configuration and customization metadata. This chapter covers the following topics:

- [Understanding the Configuration Migration Utility](#)
- [Managing Configuration Migration](#)
- [Migration Tips](#)

24.1 Understanding the Configuration Migration Utility

The Configuration Migration utility is used with the Archiver to export one Content Server instance configuration to another Content Server instance. While the Archiver is used to migrate content, the Configuration Migration utility exports the configuration and customization of the Content Server instance.

This section describes the structure of the Configuration Migration utility and how it uses templates and bundles. For an overview of this utility and how it compares to other archiving tools, see [Introduction to Migration Tools and Components](#).

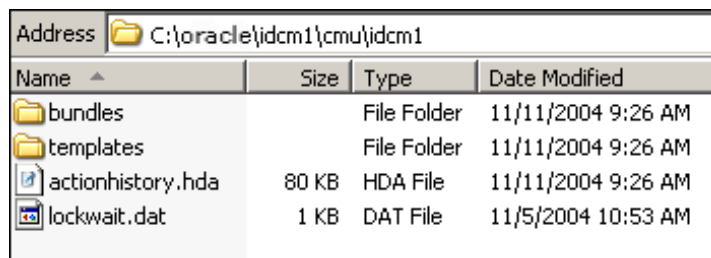
- [Migration Structure](#)
- [About Migration Templates and Bundles](#)

24.1.1 Migration Structure

A *bundle* is a set of configuration information that is packaged into a single zipped file and made ready for exporting to another Content Server instance.

Information is stored in the `DomainHome/ucm/cs/cmu/instance/` directory.

Figure 24-1 Migration Directory Structure















Name	Size	Type	Date Modified
bundles		File Folder	11/11/2004 9:26 AM
templates		File Folder	11/11/2004 9:26 AM
actionhistory.hda	80 KB	HDA File	11/11/2004 9:26 AM
lockwait.dat	1 KB	DAT File	11/5/2004 10:53 AM

The bundles subdirectory contains specific bundles and associated information. The templates subdirectory contains configuration templates which can be used for new export files.

Information is stored in the `DomainHome/ucm/cs/cmu/instance/bundles/` directory.









Figure 24-2 The Bundles Subdirectory

Address  C:\oracle\jdcml\cmu\jdcml\bundles			
Name ▲	Size	Type	Date Modified
 bundle-idcm1-25-2...		File Folder	11/10/2004 7:59 AM
 bundle-idcm1-26-2...		File Folder	11/11/2004 8:21 AM
 CompleteBundle		File Folder	11/8/2004 10:52 AM
 NewPartialBundle		File Folder	11/8/2004 9:59 AM
 NoErrorNoDepend...		File Folder	11/10/2004 6:57 AM
 PartialBundle		File Folder	11/8/2004 11:02 AM
 TestBoxBundle		File Folder	11/11/2004 8:47 AM
 tossaway		File Folder	11/9/2004 12:26 PM
 UserBundle		File Folder	11/8/2004 11:12 AM
 UserSecurityandW...		File Folder	11/9/2004 10:24 AM
 tasks.hda	4 KB	HDA File	11/11/2004 9:26 AM

Each configuration bundle is in a separate subdirectory and contains all the relevant files needed to export that bundle.

Information is stored in the `DomainHome/ucm/cs/cmu/instance/bundles/UserBundle/` directory.






Figure 24-3 Files in Configuration Bundle

Address  C:\oracle\jdcml\cmu\jdcml\bundles\UserBundle			
Name ▲	Size	Type	Date Modified
 usermetadef		File Folder	11/8/2004 11:12 AM
 aliases.hda	1 KB	HDA File	11/10/2004 7:32 AM
 manifest.hda	3 KB	HDA File	11/10/2004 7:32 AM
 roles.hda	4 KB	HDA File	11/10/2004 7:32 AM
 task.hda	4 KB	HDA File	11/10/2004 7:32 AM
 UserBundle.zip	6 KB	WinZip File	11/9/2004 1:30 PM
 usermetadef.hda	1 KB	HDA File	11/10/2004 7:32 AM

Within the specific directories, any customization that is unique to the instance in that export (such as customized metadata fields, schemas, and so on) are included in a separate subdirectory.

Information is stored in the `DomainHome/ucm/cs/cmu/instance/bundles/UserBundle/usermetadef/` directory.

Figure 24-4 Customization Stored in Directory

Address  C:\oracle\jdcml\cmu\jdcml\bundles\UserBundle\usermetadef			
Name	Size	Type	Date Modified
 usermetadef_dEmail.hda	1 KB	HDA File	11/10/2004 7:32 AM
 usermetadef_dFullName.hda	1 KB	HDA File	11/10/2004 7:32 AM
 usermetadef_dUserLocale.hda	1 KB	HDA File	11/10/2004 7:32 AM
 usermetadef_dUserType.hda	1 KB	HDA File	11/10/2004 7:32 AM

The following files are included in these different subdirectories:

File or Directory	Description
bundle directory	Each bundle has a subdirectory in the <code>bundles/</code> directory. The subdirectory is given the name assigned to the bundle when the configuration export was created.
templates directory	Contains export rules created from bundles. When a configuration export is created and saved, a name is given to that export and the configuration is stored as a template in the templates directory
<i>hda</i> files	Contains definitions and details of customization and other elements of the exported instance. Depending on how the export was defined, information can be bundled into one HDA file or into several.

24.1.2 About Migration Templates and Bundles

A migration *template* is a set of configuration options which specify what Content Server items will be exported. For example, a template named *FullCSEExport* may contain all Content Server items (schema, custom metadata, workflows, and so on). Another template named *UserCSEExport* may only contain options that pertain directly to users (security groups, roles, and so on).

These templates are used to create configuration *bundles*. A bundle uses the template to determine what to export and to create the necessary definition files which will be exported with the Content Server items. The bundle name is used to identify the finished result of an import or an export. The bundled information is put into a zipped file, containing all the necessary definition files.

24.2 Managing Configuration Migration

Migration consists of tasks such as creating migration templates, creating migration bundles, and exporting or importing the configuration.

- [Creating a Configuration Migration Template](#)
- [Editing a Configuration Template](#)
- [Importing a Template](#)
- [Creating a One-Time Export](#)
- [Exporting a Configuration](#)
- [Uploading a Bundle](#)
- [Importing a Bundle](#)

- [Downloading a Bundle](#)
- [Viewing Action Status](#)
- [Viewing Action History](#)

24.2.1 Creating a Configuration Migration Template

To create a configuration migration template:

1. Choose **Administration**, then **Config Migration Admin**, then **Configuration Templates**.
2. On the Configuration Templates page, choose **Create New Template** from the **Actions** menu.
3. On the Config Migration Admin page, choose one of the items in the Action Options list for the export.
 - To create an export template that will continue the export process even if an error is encountered, select **Continue on Error**.
The export will proceed but errors will be reported on the Action History page.
 - To have email sent to the person initiating the export, select **Email Results**.
Email will be sent to the person who performs the export, not the person who created the export template.
 - To have known dependencies added to the export or import bundle, leave the **Add Dependencies** option selected.
If this is deselected, dependencies are checked and noted with an error flag in the log file but the bundle action continues.
 - To ignore all dependencies during export or import, select **Ignore Dependencies**.
Ignoring dependencies may avoid errors during the export process, but may cause errors when an import is done.
If you are certain that all the necessary fields are present in the Content Server instance, you can deselect **Add Dependencies** and select **Ignore Dependencies** to import a field without dependencies being added.
4. You can create a custom name for this bundle. Custom names should be used sparingly to avoid possible name collisions. If a custom name is not selected, the system creates a name based on the bundle name given when you save the template. Custom names cannot contain spaces or special characters (#, \$, % and so on).
5. Choose one or more of the Content Server sections from the Content Server Sections list to be included:
 - To use all sections, choose **Select All** from the page **Actions** menu.

 **Note:**

Some Content Server sections are not displayed; not all are supported on all versions of Content Server and some cannot be safely migrated.

- To use only specific Content Server items, click **Content Server Sections**, then click the individual section name to include.

To include all items in that section, choose **Select All** from the page **Actions** menu.

To use only a subset in the section, select the individual items by putting a check in the selection box on the item's row. Some sections may have action options that are specific to that section. Select the option for the section by checking the selection box.

 **Note:**

If you want to use the majority of the metadata, choose the **Select All** menu option, then click the individual sections that you do not want to use.

6. Preview the selections you made by choosing **Preview** from the page **Actions** menu.
7. On the Preview page, continue editing and adding selections by choosing **Edit** from the page **Actions** menu.

Click **Preview** to view your changes.

8. When the template is complete, choose **Save** from the page **Actions** menu.

 **Note:**

If you do not elect to save the template, your configuration changes will be lost.

9. On the Edit Export Rule page, enter a name for the template. Names cannot contain spaces or special characters (#, \$, %, and so on). A name can include details of the date of the export (for example, *Nov10FullExport*) or describe the contents (*FullExportNoDependencies*) or can be meaningful in any way that is appropriate for your use.

Click **Save** when finished entering the name.

10. When the Config Migration Admin page opens again:
 - To create another template using the current template, choose **Save As** from the page **Actions** menu.
The Edit Export Rule window opens again where you can create a new name.
 - To alter the selections for exporting, make any changes then choose **Save** from the page **Actions** menu to change the selections and retain the name entered in step 9, or choose **Save As** from the page **Actions** menu to give it a new name on the Edit Export Rule page.
 - To export the configuration, choose **Export** from the page **Actions** menu. For more information, see [Exporting a Configuration](#).

After creating the configuration, you can export it and create a bundle for use on another system. For more information, see [Exporting a Configuration](#).

24.2.2 Editing a Configuration Template

To edit a configuration template:

1. Choose **Administration**, then **Config Migration Admin**, then **Configuration Templates**.
2. Choose a template to be edited. Use one of the following methods to choose a template from the Configuration Templates page:
 - Select the template name.

- Choose **Edit** from the individual template **Actions** menu.
3. Using the Config Migration Admin page, follow the steps detailed in [Creating a Configuration Migration Template](#) to select the items you want in the revised template:
 - Choose one of the Action Options for the template.
 - Choose the sections to be included from the Content Server Sections part of the page.
 4. Preview the selections you made by choosing **Preview** from the page **Actions** menu.
 5. On the Preview page, continue editing and adding selections by choosing **Edit** from the page Actions menu.

Click **Preview** to view your selections.
 6. When the template is complete, choose **Save** from the page **Actions** menu to save the template under its current name, or choose **Save As** to give it a new name.

 **Note:**

If you do not choose to save the template, your configuration changes will be lost.

7. Enter a new template name on the Edit Export Rule page.

24.2.3 Importing a Template

To import a template from another system for use on the current instance.

1. Choose **Administration**, then **Config Migration Admin**, then **Upload Bundle**.
2. On the Upload Configuration Bundle page, use the **Browse** button to find the bundle that contains the template you want to use.
3. Select **Create Export Template**.
4. Click **Upload**.

The bundle appears on the Configuration Bundles page. To use the template associated with that bundle, see [Editing a Configuration Template](#).

If you import a template to use for exporting and if the importing system does not have the same metadata fields, you must upload the template, import the configuration then use it for exporting. You cannot use the template for exporting unless the metadata fields are in place on the system that imported the template.

24.2.4 Creating a One-Time Export

To create an export template and immediately export the Content Server configuration:

1. Choose **Administration**, then **Config Migration Admin**, then **Configuration Templates**.
2. On the Configuration Templates page, choose **Create New Template** from the page **Actions** menu.
3. Using the Config Migration Admin page, follow the steps detailed in [Creating a Configuration Migration Template](#) to select the items you want in the configuration:
 - Choose one of the Action Options.
 - Choose the sections to be included from the Content Server Sections part of the page.

4. Preview the selections you made by choosing **Preview** from the page **Actions** menu.
5. On the Preview page, continue editing and adding selections by choosing **Edit** from the page **Actions** menu.
Click **Preview** to view your changes.
6. When the template is complete, choose **Export** from the page **Actions** menu.
The configuration is immediately exported and the name of the exported bundle appears in the Latest Action page with a unique identifier similar to the following:

```
bundle-idcm1-25-20131110T135912
```

The initial portion of the name (`bundle-idcm1`) indicates the default bundle name (`bundle`) and the instance name (`idcm`). The next portion indicates the sequence number (25). The date follows (20131110 for November 11, 2013). Finally a unique control number is used to identify the exported bundle.

24.2.5 Exporting a Configuration

To export a configuration:

1. Choose **Administration**, then **Config Migration Admin**, then **Configuration Templates**.
2. Use one of the following methods to choose an export configuration template from the Configuration Templates page.
 - Click the configuration name.
 - If you want to view the items that will be exported, choose **Preview** from the individual **Actions** menu.
3. On the Preview page, choose **Export** from the page **Actions** menu.
If you choose **Export** without previewing the bundle first, you are prompted to confirm that you want to perform the export.
The Latest Action page refreshes automatically to show the most recent activities and their status.
4. To view details of the migration action, click the message in the Status column. For more information, see [Viewing Action Status](#).

After exporting, the bundle name appears on the Configuration Bundles page, indicating that it has been bundled. A date and time indicator is appended to the configuration name, as in the following example:

```
Nov23Bundle-idcm-1-20131123T122436
```

The initial portion of the name is the original bundle name. The instance name follows (`idcm`), followed by the date (20131123 for November 23, 2013) and the time (122436 to indicate 12:24:36). From this Import page, you can download the bundle to a new location so it can be uploaded onto another system.

The original template name (`Nov23Bundle`) continues to appear on the Configuration Templates page, where it can be re-exported at another time.

24.2.6 Uploading a Bundle

Before a configuration can be imported it must be first uploaded.

To upload a bundle from another Content Server instance:

1. Choose **Administration**, then **Config Migration Admin**, then **Upload Bundle**.
2. On the Upload Configuration Bundle page, use the **Browse** button to find and select the zipped bundle file you want to use.
3. If you want to use the template included with the bundle, select **Create Export Template**.
4. If you want the new bundle information to overwrite existing Content Server configuration information, select **Force Overwrite**.
5. Click **Upload** to load the bundle.

 **Note:**

If you are uncertain about the contents of a bundle, it is always safe to upload the bundle and preview the configuration contents. The bundle configuration is not applied to the importing system until you choose to import it.

24.2.7 Importing a Bundle

After a bundle is uploaded and resides on the importing system, it can be imported for use.

To import a bundle:

1. Choose **Administration**, then **Config Migration Admin**, then **Configuration Bundles**.
2. On the Configuration Bundles page, choose **Configuration Bundles** from the Configuration Migration Administration page or from the top menu of any Migration page.
3. Select the name of the bundle you want to import.

The Config Migration Admin page opens with **Overwrite Duplicates** in place of the **Custom Name** field. Selecting this field will permit the importing bundle to overwrite any duplicate fields. If not selected, the import will error on duplicates and stop. It will continue if **Continue on Error** was checked but a status of **fail** appears on the Latest Action page.

4. Select an action from the page **Actions** menu:
 - To preview the import configuration, click **Preview**.
On the Preview page you can either choose **Edit** from the page **Actions** menu to edit the configuration options, or you can choose **Import** to import the selections as is.
 - To import the configuration without previewing, choose **Import** from the Configuration Bundles page **Actions** menu.

You are prompted to confirm that you want to import the configuration without previewing it first.

 **Important:**

You should verify that you want to import the settings in the Server Config portion of the Content Server sections. These settings determine configurations such as the type of web server used, the mail server, and other system-specific items. You may not want to import those configuration settings on a new Content Server instance.

5. After you choose **Import** from either the Preview Page or the Configuration Bundles Page, the Latest Action page opens showing the status of the import.

This page refreshes automatically to show the most recent history and status.

6. To view details of the action, click the message in the Status column of the Latest Action page. For more information, see [Viewing Action Status](#).

24.2.8 Downloading a Bundle

A bundle can be downloaded and stored in an easily accessible location for other Content Server instances to use.

To download a bundle:

1. Choose **Administration**, then **Config Migration Admin**, then **Configuration Bundles**.
2. On the Configuration Bundles page, choose **Download** from the bundle **Actions** menu of the bundle to be downloaded.

A prompt appears for the bundle location.

3. Enter the appropriate bundle location and click **Save**.

24.2.9 Viewing Action Status

To view status information for any import or export actions:

1. Choose **Administration**, then **Config Migration Admin**, then **Latest Action**.

The Latest Action page opens with information on action Time, Section, and Message.

2. You can use the **Page Refresh (In Seconds)** menu to select a different number of seconds for the refresh (from 5 seconds to 300 seconds).

Note:

The Action History page automatically appears after an export or an import.

24.2.10 Viewing Action History

To view the history of migration actions:

1. Choose **Administration**, then **Config Migration Admin**, then **Action History**.
2. On the Action History page, for each action you can view the name, source, action, start time, and status.
3. Using the **Actions** menu, you can select a specific action history or clear the Action History.

24.3 Migration Tips

It is important to remember that migration entails the bundling and copying of information *about* the Content Server instance. It does not include any of the actual content that is in the Content Server instance. The Archiver utility is used to export content. You should take care that if you archive specific content and plan to export it to another system, the metadata information for that content is also migrated using the Configuration Migration utility.

When migrating information from one Content Server instance to another, there is not a merging of information. *Migration is an additive process.* The exporting configuration bundle of metadata information is added to the metadata that currently exists in the importing Content Server instance. If metadata information currently exists that matches the metadata being imported, and if the Force Overwrite rule has been selected during import, then duplicate bundles are replaced. For information about the Force Overwrite option, see [Uploading a Bundle](#).

Configuration Migration administration tasks must be performed using a specific node of a cluster. If you do not use a specific node, then an error might occur because the job number assigned to an action is known only to the node that started the action.

You cannot import a configuration on a 6.2 version of the Content Server instance. The Edit, Preview, and History options will not appear on the bundle's options on the Configuration Bundles page on a 6.2 version Content Server instance.

If you import a template to use on another Content Server instance and if the importing system does not have the same metadata fields, you will not be able to use that template for export later. You must upload the template, import the configuration, and then use it for exporting. For details about the import process, see [Importing a Template](#).

24.3.1 Limitations

Keep the following limitations in mind when using the Configuration Migration utility:

- When exporting workflow configuration information, only the workflow definition is exported. The state of the workflow is not exported.
- If importing and overwriting existing workflows, ensure that you have the same step names for each workflow.
- If you import a workflow to a new Content Server instance, the workflow will not retain the same state information as that of the exporting Content Server instance. For this reason, you should not plan to export active workflows.
- This utility is not a cloner. It does not synchronize information with another system, it only copies and moves information.
- This utility cannot be set up to migrate automatically.
- Errors may arise when migrating docmeta information from earlier versions of the Content Server instance because of the use of schemas in later versions of the Content Server instance.
- You cannot import users from a 6.2 or 7.0 version of Content Server to a later version due to Archiver limitations.
- Migrating the `config.cfg` file may have errors because some values are not migrated for safety reasons (for example, `IDC_Name`). Others values, such as that for `AutoNumberPrefix`, are migrated.
- Migrating components can be difficult because no preference prompts (for example, in Folders or RMA) and no database tables can be migrated.
- No support is provided for bundles in components.

24.3.2 Migration Logs

You can track activity during migration events by examining migration trace logs.

To enable Content Server migration trace logs, choose **Administration**, then **System Audit Information**. In the Tracing Section Information portion of the page, choose **Active Sections**, then **cmu**. Configuration Migration utility logs will be included in the trace files that are run.

To access the logs, click **View Server Output** from the **Actions** menu on the page. The Configuration Migration utility log information is included with other tracing logs that are generated.

25

Managing Archives, Collections, and Batch Files

This chapter describes how to manage Oracle WebCenter Content Server content archives, collections, and batch files using the Archiver application.

This chapter covers the following topics:

- [Understanding How the Archiver Works](#)
- [Managing Archives](#)
- [Managing Collections](#)
- [Managing Batch Files](#)

25.1 Understanding How the Archiver Works

Archiving Content Server content consists of three elements: the archive itself, a collection, and a batch file. This section describes the structure of the Archiver application and how it uses collections and targets. For an overview of Archiver and how it compares to other archiving tools, see [Introduction to Migration Tools and Components](#).

- [Archive Structure](#)
- [Collections](#)
- [Batch Files](#)
- [Archive Targets](#)
- [Using Archive Logs](#)

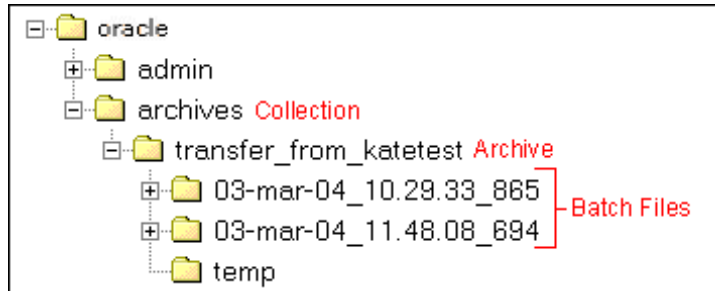
25.1.1 Archive Structure

An *archive* is a set of exported content files and their associated batch files. Each archive has its own subdirectory in the collection it belongs to.

 **Caution:**

Do not edit any of the files created by Archiver.

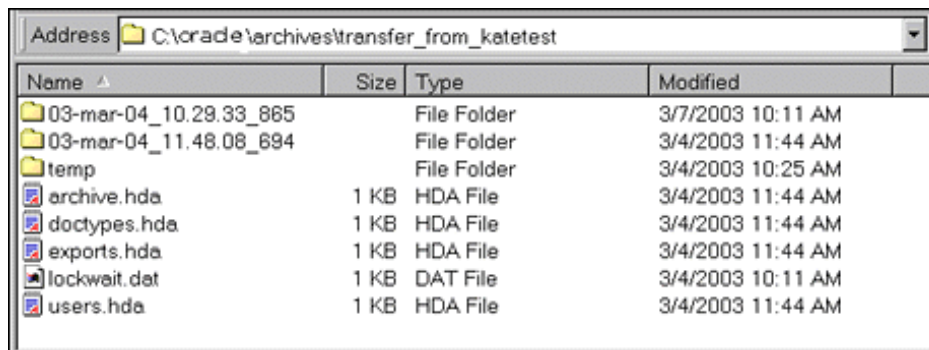
Figure 25-1 Archive Directory Structure



An archive subdirectory includes the following:

File or Directory	Description
Batch file directories	Each batch file has a subdirectory in the archive. The subdirectory name reflects the date and time of the export, with a default format of <i>yy-MMM-dd_HH.mm.ss_SSS</i> . For example, <i>03-feb-04_15.04.14_174</i> .
temp directory	Contains transferred Zip files.
archive.hda file	Specifies information about the archive, such as export and import settings, the export query, field and value import maps, archiving history, and so forth.
doctypes.hda file	Lists the content types (<i>DocTypes</i> database table) in the source Content Server instance. This file is present only if content types were exported.
exports.hda file	Specifies the batch files that are included in the archive.
users.hda file	Lists the user attributes (<i>Users</i> database table) in the source Content Server instance. This file is present only if user attributes were exported.

Figure 25-2 Archive Subdirectory Structure



25.1.2 Collections

This section provides information about collections.

Summary

A *collection* is a set of archives on a particular Content Server instance.

- Each instance has a default collection, which is located in the *IntradocDir/archives/* directory. Additional collections can be created, but are necessary only in rare situations. For example, you could create a new collection if you want to save disk space by archiving to another system that does not have Content Server on it.
- Collections can be created only through the standalone Archiver application. For details about using the standalone Archiver, see [Running Archiver as a Standalone Application](#).
- A collection can be removed from a Content Server instance, but this only makes it unavailable from Archiver; the archive and batch files remain until you delete them from the file system.

 **Note:**

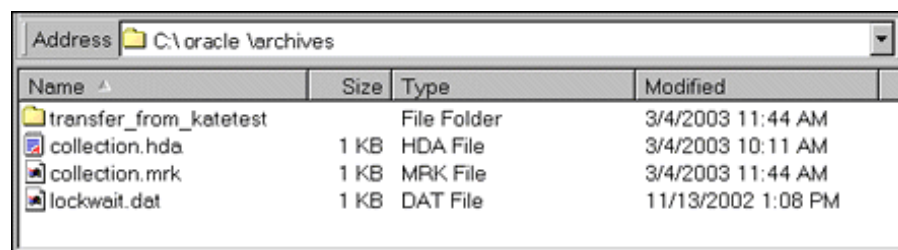
Archiver collections are normally compatible between different versions of Content Server instances. One possible exception would be User Configuration information that was archived from a pre-3.0 version Content Server instance. The format of the Users database table changed in version 3.0, so this information might not be compatible between pre- and post-3.0 version Content Server instances.

Structure

An archive collection includes the following:

File or Directory	Description
<i>collection.hda</i> file	Specifies the archives that are included in the collection.
<i>collection.mrk</i> file	Internal file used by Archiver.
Archive directories	Each archive has a subdirectory in the collection.

Figure 25-3 Collection Structure



25.1.3 Batch Files

This section provides information about batch files.

Summary

A *batch file* is a text file that contains the file records for archived content items. Batch files describe the metadata for each exported revision.

- A new batch file subdirectory is created each time an archive is exported.

- Each batch file contains up to 1000 file records. If an export contains more than 1000 revisions, a new batch file is created.

 **Note:**

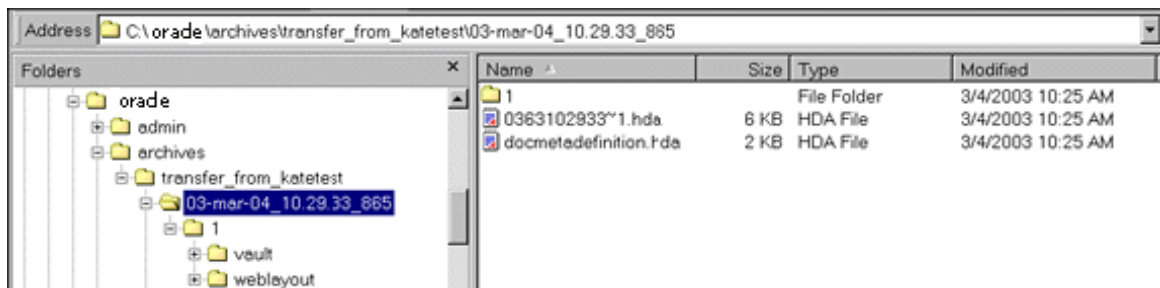
Archiver batch files are not the same as the batch files that are used with the Batch Loader application.

Structure

A batch file subdirectory includes the following:

File or Directory	Description
Content files	A subdirectory named '1' in the batch file directory contains a <i>vault</i> structure that is copied from the source Content Server instance. If web-viewable files are being archived, this subdirectory also contains a <i>weblayout</i> structure.
Batch file	Specifies the metadata for each revision that was exported. Batch files are HDA files that are named with a unique number generated by Archiver. For example, <i>0335150414-1.hda</i> .
docmetadefinition.hda file	Lists the custom metadata fields in the source Content Server instance (<i>DocMetaDefinition</i> database table). This file is used by Archiver to create import maps.

Figure 25-4 Batch File Structure



25.1.4 Archive Targets

You can use Archiver to archive the following content:

- Native files with associated standard metadata values
- Web-viewable files (.pdf, .html, and so forth)
- Metadata fields and changes
- User information fields
- Security groups (user attributes and settings)
- User updates
- Subscription types

- File formats
- Document types
- Content types
- User attributes (such as user login, full name, password, email address, and so forth)

 **Note:**

Content types and user attributes can be exported and imported manually, but cannot be transferred or archived automatically through replication. Table replication can be used, though, to replicate user information.

 **Caution:**

Archiver cannot be used to move or copy data between two instances that share the same Content Server instance name (*IDC_Name*). To do so will corrupt the data on the target system.

25.1.5 Using Archive Logs

If you are experiencing Archiver problems, view the Archiver logs for more information.

Summary

The Archiver logs are listed by date and time. They are generated once per day when the first Archiver information status, irrecoverable error, or error occurs.

Click the Archiver Logs link on the Administration page to view information about imports, exports, and replications.

Click the link that appears for the desired log file. A table showing the type, date and time, and description of each action is displayed. It also includes the name of the Content Server instance that created the archive.

Figure 25-5 Archive Log File

Archiver -- Log File Created: 8/30/04 11:12 AM		
Type	Time	Description
Info	8/30/04 11:12 AM	Log organization created by application.
Info	8/30/04 11:12 AM	Event generated by user 'sysadmin' at host 'jwilsonnote'. Added archive 'JeanTest' to collection 'idcm1'.
Info	8/30/04 1:37 PM	Event generated by user 'sysadmin' at host 'jwilsonnote'. Edited properties for archive 'JeanTest' in collection 'idcm1'. Updated values: aExportQuery = Standard Query ValuePanel UseExportDate 0 AllowExportPublished 0 AllRevisions 1 LatestRevisions 0 NotLatestRevisions 0 CurrentIndex 0 Clauses dDocName:sqlEq:002Tutorial CustomQuery dDocName%=%'002Tutorial' IsCustom 1.

Log Entries

The following types of archiver log entries are generated:

- **Info:** Displays basic status information. For example, status information is logged when an export and an import starts and finishes.
- **Error:** Displays user and administration errors that occur but do not stop the software from functioning. For example, an error is logged if there is no file information for a content item that you are trying to export.
- **Fatal:** Displays errors that stop the software from functioning. For example, an irrecoverable error is logged if the Content Server instance cannot access the database. Check the connection string, user name, and password.

25.2 Managing Archives

After archives are created, they can be added to collections and manipulated as a group.

- [Creating a New Archive](#)
- [Copying an Existing Archive](#)
- [Creating a New Archive by Copying](#)
- [Deleting an Archive](#)
- [Running Archiver as a Standalone Application](#)

25.2.1 Creating a New Archive

To create a new, undefined archive:

1. Display the Main Archiver window in either standalone or browser mode.
For instructions in using standalone mode, see [Running Archiver as a Standalone Application](#).

2. If necessary, open the collection where you want to create the new archive. For more information, see [Opening a Collection](#).
3. From **Edit**, select **Add**.
4. In the Add Archive window, enter the archive name and description. The archive name cannot contain spaces.
5. Click **OK**.

25.2.2 Copying an Existing Archive

To copy an existing archive to a different directory location:

Note:

This procedure copies the files in an archive. It does not create a new collection or update the `collection.hda` file if the archive is copied to a collection directory.

1. Display the archiver in standalone mode.
For instructions, see [Running Archiver as a Standalone Application](#).
2. If necessary, open the collection that contains the archive to be copied. For more information, see [Opening a Collection](#).
3. Select the archive to be copied.
4. From **Edit**, select **Copy To**.
5. In the Copy Archive window, accept the original archive name, or change the name as necessary.
6. In the **Copy Archive To Directory** field, enter the directory path where the archive will be copied.
7. Click **OK**.
The archive files are copied to the specified directory.

25.2.3 Creating a New Archive by Copying

You can copy archives from your system for storage or to your system from another archive if you are using the Archiver standalone version.

To create a new archive in the current collection by copying an existing archive:

1. Display the archiver in standalone mode.
For instructions, see [Running Archiver as a Standalone Application](#).
2. If necessary, open the collection where you want to create the new archive. See [Opening a Collection](#).
3. From **Edit**, select **Add**.
4. In the Add Archive window, enter the archive name and description. The archive name cannot contain spaces.
5. Select **Copy From**.
6. Click **Browse**.

7. Navigate to and select the desired archive file (*archive.hda*).
8. Click **Open**.
9. Click **OK**.

The archive files are copied to the default archive directory in the local Content Server instance.

25.2.4 Deleting an Archive

To delete an archive from a collection:

1. Open the archive collection.
2. Select the archive to delete in the Current Archives list.
3. From **Edit**, select **Delete**. You are prompted to confirm the action.
4. Click **OK**.

The archive is deleted from the collection.

25.2.5 Running Archiver as a Standalone Application

The following information details how to run Archiver as a standalone application, which is required to create collections.

25.2.5.1 Running the Archiver in Windows

You can run the archiver in both Windows and Unix.

To run Archiver on a Windows operating system:

1. Select the application from the Windows **Start** menu, then choose **Programs**, then **Content Server**, then *instance*, then **Analyzer**. A login window or application window opens.

 **Note:**

It may take several seconds for the login window or the application window to appear, and the window may be hidden by other windows.

2. If required, enter the administrator login name and password, then click **OK**. The Main Archiver window opens.

25.2.5.2 Running the Archiver in UNIX

You can run the Archiver in both Unix and Windows.

To run Archiver on a UNIX operating system:

1. Navigate to the *DomainHome/ucm/cs/bin/* directory.
2. Enter **.archive**
3. If required, enter the administrator login name and password.

The Main Archiver window of the application opens.

25.3 Managing Collections

Collections are a set of archives and are used to group archives for different archive functions.



Note:

The standalone mode of the Archiver application is required to create new collections or browse the local file system to connect to new collections.

- [Opening a Collection](#)
- [Creating a Collection](#)
- [Removing a Collection](#)
- [Moving the Default Archive Collection](#)

25.3.1 Opening a Collection

To open an existing archive collection:

1. Run Archiver in standalone mode.
For instructions, see [Running Archiver as a Standalone Application](#).
2. From **Options**, choose **Open Archive Collection**.
3. Select the collection from the list of existing collections on the Open Archive Collection window (shows the default collection and any other connected collections).
4. To browse to a new collection, use one of these methods:
To select the collection from a shared file system location (standalone Archiver only):
 - a. Click **Browse Local**.
 - b. In the Find Archive Collection Definition File window, navigate to and select the collection HDA file.
 - c. Click **Open**.
The Browse to Archiver Collection window opens.To select the collection from a remote Content Server instance:
 - a. Click **Browse Proxied**.
The Browse for Proxied Collection window opens with a list that includes all Content Server instances to which an outgoing provider has been set up.
 - b. Select the Content Server instance in the **Proxied Servers** list.
 - c. Select the collection in the **Collections** list.
 - d. Click **OK**.

25.3.2 Creating a Collection

To create a new archive collection:

**Note:**

You can create a new collection only on the local Content Server instance using the standalone Archiver.

1. Run Archiver in standalone mode.
For instructions, see [Running Archiver as a Standalone Application](#).
2. From **Options**, choose **Open Archive Collection**.
3. In the Open Archiver Collection window, click **Browse Local**.
4. In the Find Archive Collection Definition File window, navigate to and select the directory where you want to create the new collection.
5. Enter a file name for the new collection (`collection.hda` is the default).
6. Click **Open**.
You are prompted to create a collection definition (HDA) file.
7. Click **Yes**.
8. In the Browse To Archiver Collection window, enter a collection name in the **Name** field.
 - Collection names cannot contain spaces.
 - Use the same name for a collection and its directory to make navigation easier.
9. Enter the directory path for the weblayout and vault directories in the **Web Directory** and **Vault Directory** fields.
 - Use the same path style as shown in the **Location** field.
 - To find the directory paths, display the Configuration Information page.
10. Click **OK**.
The new collection is shown in the Open Archive Collection page.
11. Click **Open** to open the new collection.

25.3.3 Removing a Collection

To remove an archive collection:

**Note:**

You cannot remove the default collection.

1. From **Options**, choose **Open Archive Collection**.
2. In the Open Archive Collection window, select the collection to be removed.
3. Click **Remove**.
You are prompted to confirm the action.
4. Click **OK**.

The collection is removed from the Content Server instance. (The collection and archive files remain in the file system, and must be deleted manually.)

25.3.4 Moving the Default Archive Collection

You can change the file system location of the default archive collection by moving the collection and pointing the Content Server instance to the new location. For example, you might want to keep all of your archive data on a separate drive from the program files for easier backup and expansion.

Note:

The default collection is the `archives/` directory.

To move the default archive collection:

1. For data safety, close any standalone Archiver applications and stop the Content Server instance.
2. Add the `CollectionLocation` configuration variable with a specified path to the new location in the `DomainHome/ucm/cs/bin/intradoc.cfg` file:

```
CollectionLocation=path
```

3. To maintain the previously created archives for the default collection, move the contents of the `archives/` directory to the new location you specified in the `CollectionLocation` setting. If you do not move the contents, the system will create an empty collection.
4. Start the Content Server instance.

Note:

The Content Server instance re-creates the default `Domain_home/ucm/cs/archives/` directory when it is restarted, but Archiver defaults to using the collection in the new location.

25.4 Managing Batch Files

A batch file describes the metadata for exported revisions. A batch file is created each time Archiver performs an export.

- [Removing Revisions from a Batch File](#)
- [Deleting a Batch File](#)

25.4.1 Removing Revisions from a Batch File

To remove individual revisions from a batch file:

1. Open the archive collection.
For instructions, see [Opening a Collection](#).
2. Select the archive in the Current Archives list.

3. In the Main Archiver window, click **View Batch Files**.
4. In the View Batch files window, select the batch file.
5. Click **Edit**.
6. In the View Exported Content Items window, use the **Filter** element and the navigation buttons to display the revision to be deleted.
7. Select the revision to be deleted.
8. Click **Delete**.
The Status changes to Deleted for the selected revision.
9. Repeat steps 7 and 8 to delete additional revisions.
10. To undo the last deletion, click **Undo**. To return all deleted revisions to Archived status, click **Refresh**.
11. Click **Apply** to delete the specified revisions.
12. Click **Close**.

25.4.2 Deleting a Batch File

To delete a batch file from an archive:

1. Open the archive collection.
For instructions, see [Opening a Collection](#).
2. Select the archive in the Current Archives list.
3. In the Archiver window **General** tab, click **View Batch Files**.
4. In the View Batch Files window, select the batch file to delete.
5. Click **Delete**.
You are prompted to confirm the action.
6. Click **OK**.
The batch file is deleted from the archive.
7. Specify whether to replace existing batch files upon export:
 - To delete all existing batch files when the next export is initiated, select **Replace Existing Export Files**.
 - To leave existing batch files in place when the next export is initiated, deselect **Replace Existing Export Files**.
8. Specify which files to export:
 - To export the native (*vault*) and web-viewable (*weblayout*) files, select **Copy Web Content**.
 - To export only the native (*vault*) files, deselect **Copy Web Content**.
9. Click **OK**.
The export options are displayed in the **Export Options** section of the **General** tab.

26

Exporting Data in Archives

This chapter provides information on exporting data from one Oracle WebCenter Content Server instance to another instance for backup, storage, or import.

This chapter covers the following topics:

- [Understanding Exporting Data](#)
- [Managing Exports](#)

26.1 Understanding Exporting Data

The Export function in the Archiver utility is used to copy native and web-viewable files out of the Content Server instance for backup, storage, or import to another Content Server instance. This function also can be used to export content types and user attributes. Note that this exports only a copy; the original content remains.

You can export revisions that are in the following status: RELEASED, DONE, EXPIRED, and GENWWW. You cannot export revisions that are in an active workflow (REVIEW, EDIT, or PENDING status) or that are DELETED.

- [Export Uses](#)
- [Export Methods](#)

26.1.1 Export Uses

Typical uses for the Export function include:

- Copying files from an intranet to make them available to an extranet for vendor or customer viewing.
- Creating an archive of content items that will then be imported back to the same instance with different metadata.
- Removing content from the Content Server instance for permanent or temporary storage. For example, if space becomes limited or performance drops, you could remove all but the latest revision of each file.
- Copying files, content types, and user attributes from a development Content Server instance for use in a production instance.

Caution:

Do not use Archiver as your primary method of disaster recovery; use standard backup systems for the database and file system.

26.1.2 Export Methods

After you set up the export criteria, you can export archives in the following ways:

- **Manual:** A one-time export initiated from Archiver by an administrator. This creates an archive on the local Content Server instance.
- **Automatic (Replication):** Export to a local archive is initiated automatically whenever a content item that meets the export criteria is indexed.

[Manually Exporting](#) and [Replicating Files](#) discuss these processes in more detail.

**Note:**

You can export expired revisions manually, but expired revisions do not get exported automatically.

26.2 Managing Exports

This section provides information about typical tasks used in managing exports.

- [Manually Exporting](#)
- [Creating a Content Item Export Query](#)
- [Exporting Configuration Information](#)
- [Adding a Table to an Archive](#)
- [Editing the Archive Properties of a Table](#)
- [Creating a Table Export Query](#)
- [Setting Export Options](#)
- [Initiating the Export](#)

26.2.1 Manually Exporting

To export content manually:

1. Create an archive where the exported Content Server data will be stored. See [Creating a New Archive](#).
2. Select the archive in the **Current Archives** list.
3. Create an export query. See [Creating a Content Item Export Query](#).
4. Set configuration information export options. See [Exporting Configuration Information](#).
5. Set the general export options. See [Setting Export Options](#).
6. Initiate the export. See [Initiating the Export](#).

26.2.2 Creating a Content Item Export Query

Export queries define which revisions will be exported. Follow these steps to create an export query:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Main Archiver Export Data window.

4. Click **Edit** in the Export Query (Content) section.
5. In the Edit Export Query (Content) window, select a metadata field from the **Field** list.
6. Select an **Operator** from the list.
 - The available operators depend on which field is selected.
 - The available operators map to basic SQL query operators. To use other SQL query operators, create a basic expression and then edit it in the **Custom Query Expression** box (see step 10).

7. Enter the criteria in the **Value** field.

Depending on the option selected in the **Field** list, you can enter text directly, click the **Select** button and select from the available values, or select directly from a list of the available values.

8. Click **Add**.

The query expression is added to the **Query Expression** box, and the SQL version of the query expression is displayed in the **Custom Query Expression** box.

9. To add to the query expression, repeat steps 5 through 8. By default, each part of the expression is added using an AND operator.

To update an existing query, select the line to be changed in the **Query Expression** box and edit the **Field**, **Operator**, and **Value** fields as necessary. Click **Update**. The specified query expression replaces the selected line.

To delete a line from the query expression, select the line to be deleted in the **Query Expression** box. Click **Delete**. The selected line is deleted.

10. To edit the SQL expression directly:

- a. Select **Custom Query Expression**.
- b. Edit the text in the **Custom Query Expression** box.

You can use Idoc Script in the query expression. For example, to archive content more than one year old, you could use `<$dateCurrent (-365) $>` as the Release Date value. See Custom Query Expressions in *Developing with Oracle WebCenter Content*.

 **Caution:**

If you deselect the **Custom Query Expression** check box, the query expression reverts to its original definition; all modifications will be lost.

11. Specify whether to export revisions based on the last export date:
 - To export only revisions that have been released since the last export, select **Export Revisions with Release Date later than most recent Export Date**.
 - To export all revisions, deselect **Export Revisions with Release Date later than most recent Export Date**.
12. Specify whether to export revisions that were published to the Content Server instance by Oracle Content Publisher:
 - To export published revisions, select **Allow Export of Published Revisions**.
 - To export only unpublished revisions, deselect **Allow Export of Published Revisions**.
13. Specify which revisions to export:

- To export all revisions of each content item, select the **All Selected Revisions** option.
- To export only the latest revision of each content item, select the **Latest Revisions** option.
- To export all revisions except the most recent, select the **Not Latest Revisions** option.
- To export the most recent revision that matches the query, select the **Single Revision Replication** option. For details about how this option affects the replication process, see [Single Revision Replications](#).

 **Caution:**

Do not use the **Latest Revision** option and automatic replication. These options, used in conjunction, can cause unpredictable archive behavior. For more details about automatic replication, see [Replicating Files](#).

14. Click **OK**. The export query is displayed in the **Export Query** box on the **Content** tab.
15. To see a list of revisions that will be included in the export, click **Preview**.

 **Note:**

Although an unlimited number of revisions can be exported, a maximum of 100 revisions can be displayed in the Content Satisfying the Export Query page. Use the **Filter** and **Release Date since** features to display subsets of the list as necessary.

16. Review the list on the Previewing Export Queries (Content) window to ensure that the export includes the intended revisions.
17. Click **Close**.

26.2.3 Exporting Configuration Information

To export content type and user attributes:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Main Archiver Export Data window.
4. Click **Edit** in the Additional Data section.
The Edit Additional Data Page appears.
5. To export content types, select **Export Content Configuration Information**.
6. To export user data, select **Export User Configuration Information**.
7. Click **OK**.

The configuration information options are displayed in the **Additional Data** section of the **Export Data** tab.

26.2.4 Adding a Table to an Archive

To add a table to an archive:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Main Archiver Export (Table) window.
4. Select an archive from the **Current Archives** list.
5. Click **Add**.
6. In the Add New Table window, complete the fields as appropriate. These fields are used to export the parent/child relationship in any tables used in schemas.
7. Click **OK**.

The table is added to the **Table** list on the **Table** tab.

Caution:

When exporting tables, ensure that the column names are the same if you are creating a relationship between two tables. If tables are imported individually, without assigning a relationship, it is not essential to match the column names. But if tables are imported in a relationship, the column names should be the same.

26.2.5 Editing the Archive Properties of a Table

To edit the archive properties of a table:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Main Archiver Export (Table) window.
4. Select an archive from the **Current Archives** list.
5. Select a table from the **Table** list.
6. Click **Edit**.
7. In the Edit Table window, edit the fields as appropriate.
8. Click **OK**.

26.2.6 Creating a Table Export Query

To create a query that defines which tables will be exported:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Main Archiver Export (Table) window.
4. Select a table from the **Table** list.

5. Click **Edit** in the Export Query section.
6. In the Edit Export Query (Table) window, select a metadata field from the **Field** list.
7. Select an **Operator** from the list.
 - The available operators depend on which field is selected.
 - The available operators map to basic SQL query operators. To use other SQL query operators, create a basic expression and then edit it in the **Custom Query Expression** box (see step 10).
8. Enter the criteria in the **Value** field.
9. Click **Add**.

The query expression is added to the **Query Expression** box, and the SQL version of the query expression is displayed in the **Custom Query Expression** box.

10. To add to the query expression, repeat steps 6 through 9. By default, each part of the expression is added using an AND operator.
11. To update an existing query:
 - a. Select the line to be changed in the **Query Expression** box.
 - b. Edit the **Field**, **Operator**, and **Value** fields as necessary.
 - c. Click **Update**. The specified query expression replaces the selected line.
12. To delete a line from the query expression:
 - a. Select the line to be deleted in the **Query Expression** box.
 - b. Click **Delete**. The selected line is deleted.
13. To edit the SQL expression directly:
 - a. Select **Custom Query Expression**.
 - b. Edit the text in the **Custom Query Expression** box. You can use Idoc Script in the query expression. See Custom Query Expressions in *Developing with Oracle WebCenter Content*.

 **Caution:**

If you deselect the **Custom Query Expression** check box, the query expression reverts to its original definition; all modifications will be lost.

14. Click **OK**.

The export query is displayed in the **Export Query** box on the **Table** tab.
15. To see a list of tables that will be included in the export, click **Preview**.

 **Note:**

Although an unlimited number of tables can be exported, a maximum of 100 tables can be displayed in the Content Satisfying the Export Query page. Use the **Filter** and **Release Date since** features to display subsets of the list as necessary.

16. Review the list on the **Previewing Export Queries (Content)** window to ensure that the export includes the intended revisions.
17. Click **Close**.

26.2.7 Setting Export Options

To set general export options:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Main Archiver window.
4. Click **Edit** in the **Export Options** section.
5. In the Edit Export Options window, specify whether to replace existing batch files upon export:
 - To delete all existing batch files when the next export is initiated, select **Replace Existing Export Files**.
 - To leave existing batch files in place when the next export is initiated, deselect **Replace Existing Export Files**.
6. Specify which files to export:
 - To export the native (*vault*) and web-viewable (*weblayout*) files, select **Copy Web Content**.
 - To export only the native (*vault*) files, deselect **Copy Web Content**.
7. Specify whether to export content or not:
 - To export only tables, select **Export Table Only**.
 - To export content items, deselect **Export Table Only**.
8. Click **OK**.

The export options are displayed in the **Export Options** section of the **General** tab.

26.2.8 Initiating the Export

To manually export content and configuration information:

1. Open Archiver for the Content Server instance that contains the files you want to export.
2. Open the archive collection. See [Opening a Collection](#).
3. Select the archive to export to in the **Current Archives** list.
4. From **Actions**, choose **Export**.

Note:

If the **Export** option is disabled, the archive is being exported automatically. You must disable the automatic replication to perform a manual export. For details, see [Replicating Files](#) .

5. In the Export Archiver window, specify whether to delete the revisions from the Content Server instance after the export is successfully completed:

- To delete revisions after export, select **Delete revisions after successful archive**.
 - To leave revisions in the Content Server instance after export, deselect **Delete revisions after successful archive**.
6. Click **OK**.

The export process is initiated, and the status bar at the bottom of the Archiver page displays progress messages.

Importing Data from Archives

This chapter provides information on retrieving Oracle WebCenter Content Server files and information from an exported Content Server archive by using the Import function of the Archiver application. Importing is typically used to obtain a copy of content from another Content Server instance or to restore data that has been in storage.

This chapter covers the following topics:

- [Understanding Importing Files](#)
- [About Import Rules](#)
- [Importing Data](#)

27.1 Understanding Importing Files

Using the Import function of Archiver, you can move archives into the Content Server repository according to specified rules and at specified times. The data in the files can be mapped to fields in the receiving Content Server instance, but care should be taken that the correct rules are applied during import.

The Content Server instance to which you are importing must have the same metadata fields, security groups, and accounts as the instance that the archive was exported from. Errors can result if there are mismatches.

Important:

Do not use Archiver as your primary method of disaster recovery; instead use standard backup systems for the database and file system.

Note:

Imported revisions will not enter a workflow upon import, even if they meet the criteria for an active workflow.

Before beginning the import process, consider the following points:

- Determine the method to be used, either manual or automatic.
- Determine the rules to be used for updating.
- Determine the mapping and import options.
- Test your process by importing selected revisions.

This section covers these topics:

- [Import Uses](#)

- [Import Methods](#)

27.1.1 Import Uses

Typical uses for the Import function include:

- Placing data archived from an intranet on an extranet for vendor or customer viewing.
- Changing metadata for a large number of content items. For example, if an employee leaves the organization, you could export all of their content items and then import them with another user specified as the Author.
- Restoring content that was inadvertently deleted or configuration information that was inadvertently changed.
- Copying files, content types, and user attributes from a development Content Server archive to a production instance.

27.1.2 Import Methods

You can import archives in the following ways:

- **Manual:** A one-time import initiated from Archiver by an administrator.
- **Automatic (Replication):** Import from a local archive is initiated automatically, about once per minute.

For more information, see [Importing Data](#) and [Replicating Files](#) .

27.2 About Import Rules

An *import rule* defines how revisions are added, replaced, or deleted during import.

- During import, Archiver compares each revision being imported with the existing revisions in the importing Content Server instance. The import rule specifies which action to take (add, replace, delete, or ignore), depending on comparison of the following information:
 - Content ID
 - Original Content Server
 - Revision number
 - Release date
- Only one import rule can be selected for each import of an archive.

This section covers these topics:

- [Update Import Rule](#)
- [Insert Revision Import Rule](#)
- [Insert Create Import Rule](#)
- [Delete Revision Import Rule](#)
- [Delete All Revisions Import Rule](#)

27.2.1 Update Import Rule

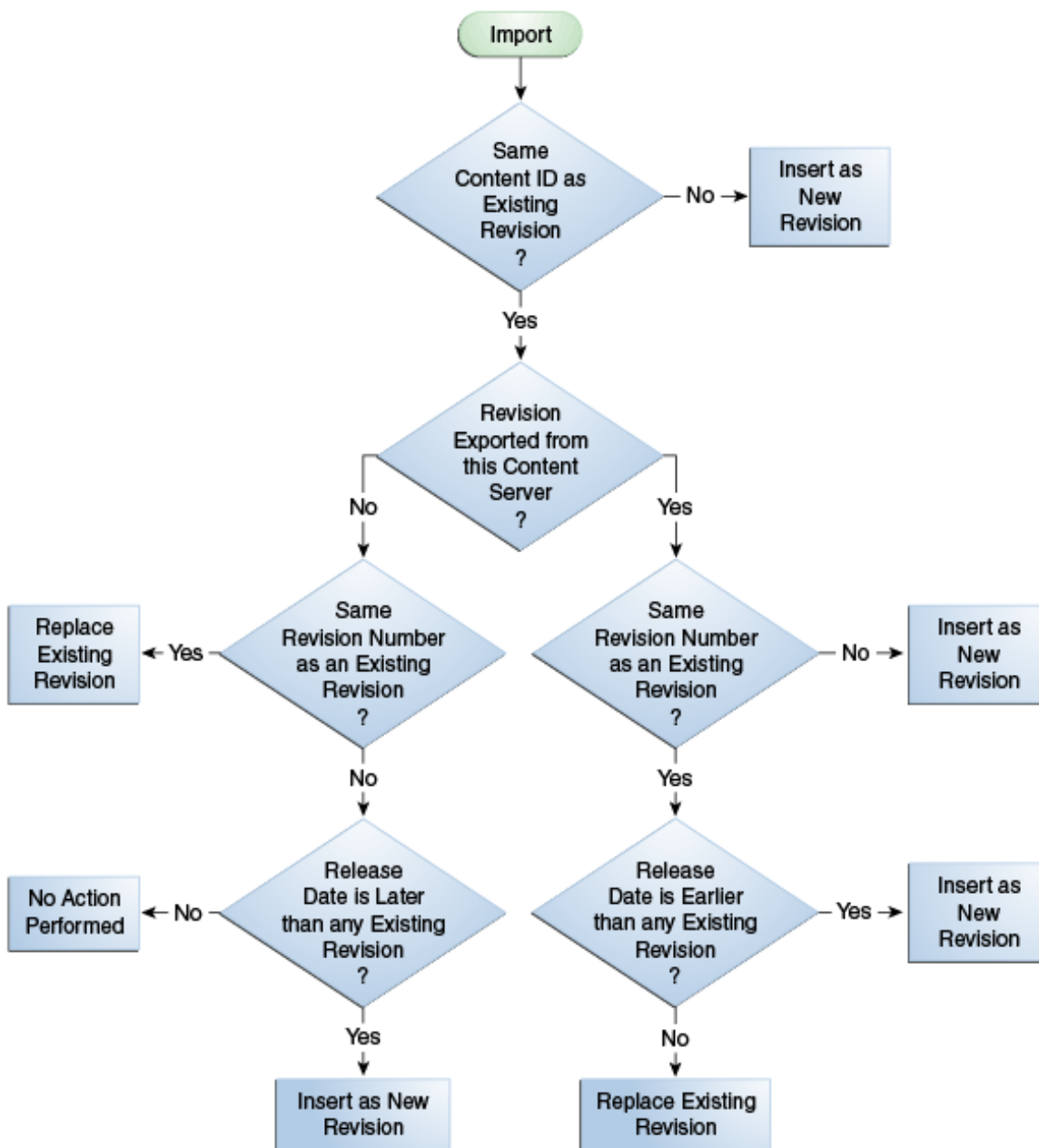
Use the Update import rule to replace existing revisions and insert new revisions.

Note:

The Update import rule will replace existing revisions without saving the existing files. *Be extremely careful when importing so you do not accidentally replace content you meant to keep.*

- If an imported revision has a different Content ID (dDocName) than any existing revision, the imported revision is inserted as a new revision.
- If an imported revision has the same Content ID (dDocName) as an existing revision, the imported revision is inserted, ignored, or replaces the latest existing revision.

Figure 27-1 Import Rule: Update

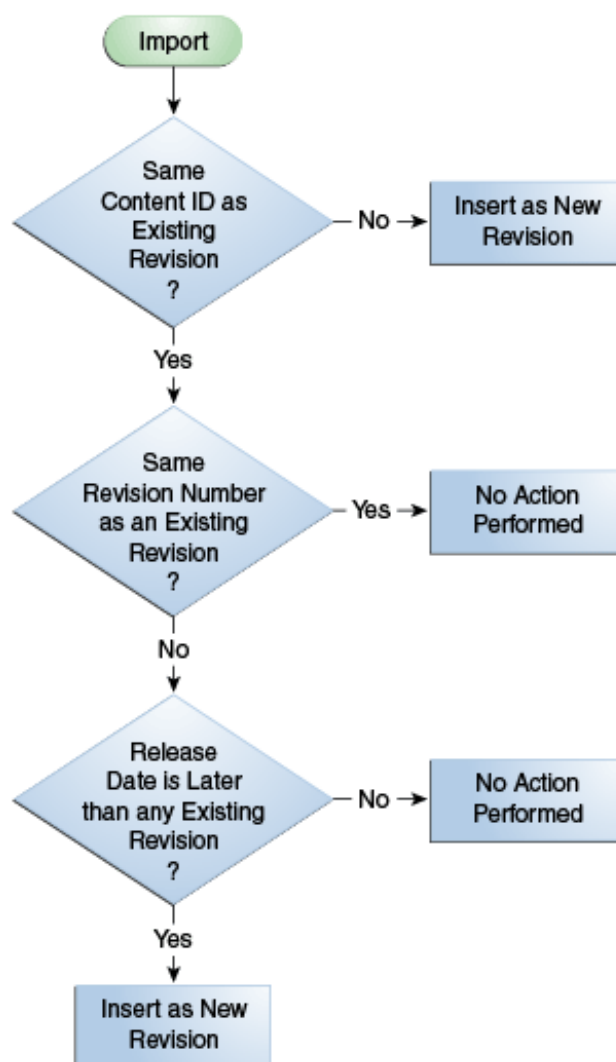


27.2.2 Insert Revision Import Rule

The Insert Revision import rule imports only revisions that have both the most recent revision number and the most recent release date.

- If an imported revision has a different Content ID (dDocName) than any existing revision, the imported revision is inserted as a new revision.
- If an imported revision has the same Content ID (dDocName) as an existing revision, but has a different Revision ID (dRevisionID) than any existing revision and a later release date (dInDate) than that of the latest existing revision, the imported revision is inserted as a new revision with a new revision label.

Figure 27-2 Import Rule: Insert Revision



27.2.3 Insert Create Import Rule

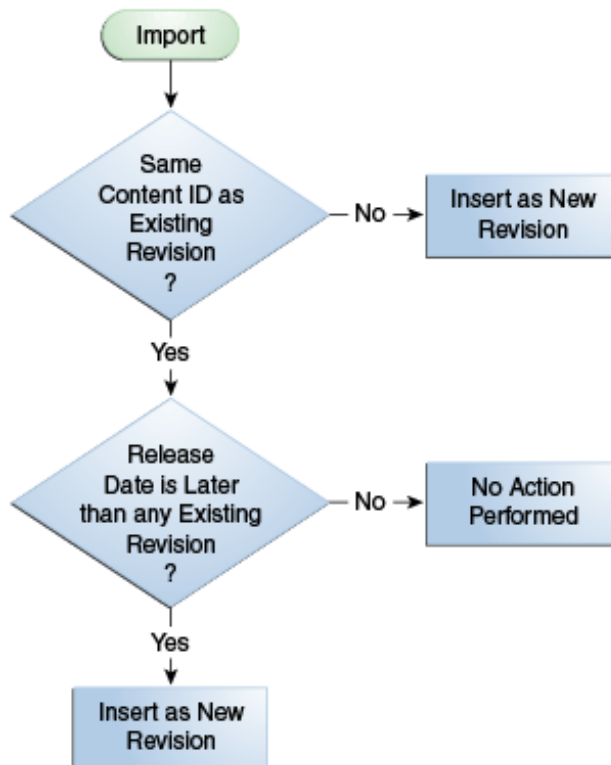
The Insert Create import rule imports only revisions that have the most recent release date, regardless of the revision number.

- If an imported revision has a different Content ID (dDocName) than any existing revision, the imported revision is inserted as a new revision.
- If an imported revision has the same Content ID (dDocName) as an existing revision, and the release date (dInDate) of the imported revision is later than that of the latest existing revision, the imported revision is inserted as a new revision with a new revision label.

 **Note:**

When an Automatic Import occurs instead of a Manual Import, the Import rule is either `update` or `deleteRev`. The `deleteRev` option is considered in case of an auto-export delete. In all the other cases, the Import rule becomes `update`. If the import rule is set as `Insert Create` and Automatic Import is used, the rule is not considered.

Figure 27-3 Import Rule: Insert Create

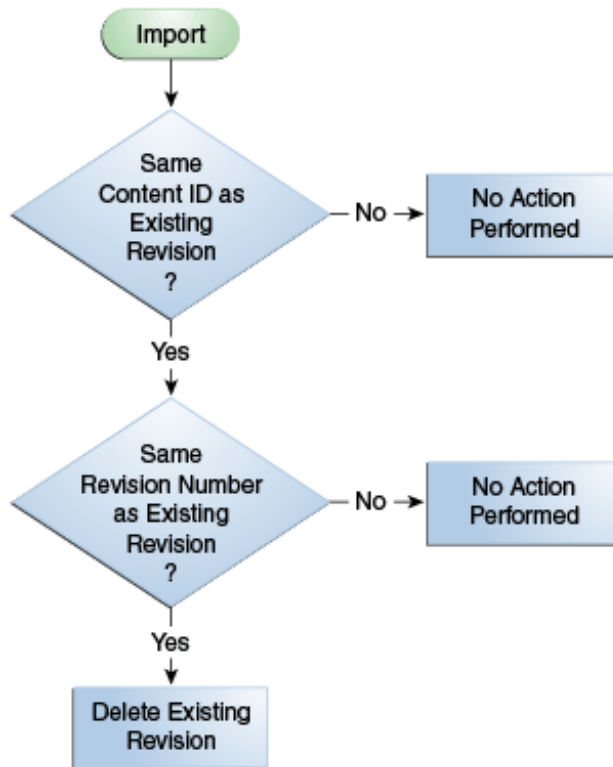


27.2.4 Delete Revision Import Rule

Use the Delete Revision import rule to delete individual revisions.

- If an imported revision has the same Content ID (dDocName) and Revision ID (dRevisionID) as an existing revision, the existing revision is deleted.

Figure 27-4 Import Rule: Delete Revision

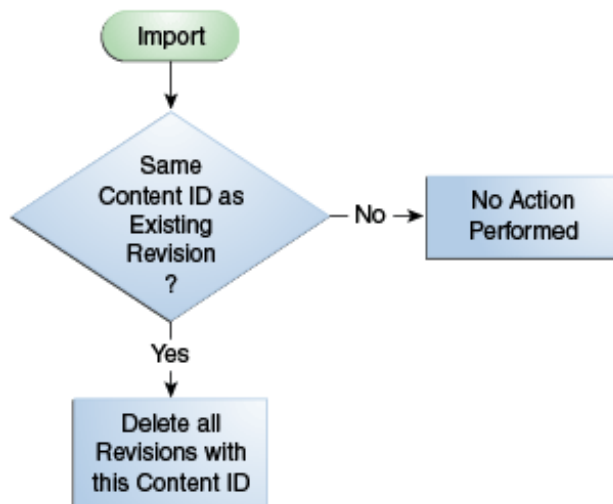


27.2.5 Delete All Revisions Import Rule

Use the Delete All Revisions import rule to delete all revisions of a content item.

- If an imported revision has the same Content ID (dDocName) as any existing revision, all existing revisions with that Content ID are deleted.

Figure 27-5 Import Rule: Delete All Revisions



27.3 Importing Data

This section provides information about the import process and tasks.

 **Note:**

To determine which archive contains the data you want to retrieve, you can prepare an Archive History report using the Web Layout Editor.

You can also examine the files generated by the archive at the file system level, but preparing a report is more efficient if you frequently need to find archived data.

 **Note:**

If you are using Sybase and you want to import an archive, you must perform the following tasks:

1. Make sure you are logged in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Desktop Client Apps**, then **Repository Manager**.
3. Select the **Indexer** tab.
4. In the Automatic Update Cycle section, click **Configure**.
5. Make sure **Indexer Auto Updates** is deselected.
6. Close **Repository Manager**.
7. Use Archiver to import the archive.
8. Open **Repository Manager** and select **Indexer Auto Updates** again.

This section covers these topics:

- [Importing Archived Data Manually](#)
- [Setting Field Maps](#)
- [Setting Value Maps](#)
- [Setting Import Options](#)
- [Importing an Individual Revision](#)
- [Initiating the Import](#)

27.3.1 Importing Archived Data Manually

To manually import archived data:

1. Open the archive collection. See [Opening a Collection](#).
2. In the **Current Archives** list, select the archive from which to retrieve data.

3. Review the batch files in the archive. If necessary, remove revisions from the batch files. See [Removing Revisions from a Batch File](#).
4. If you want to change metadata fields or values during the import, set up the field and value mappings. See [Setting Field Maps](#) and [Setting Value Maps](#).
5. Set the general import options. See [Setting Import Options](#).
6. Test the import mappings and rules on a few individual revisions. See [Importing an Individual Revision](#).
7. Initiate the import. See [Initiating the Import](#).

27.3.2 Setting Field Maps

Field maps specify how metadata values are copied from one metadata field to another during import. If you do not want to copy metadata values, do not specify any field maps.

To set up field maps:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Import Maps main window.
4. Click **Edit** in the Field Maps section.
5. In the Edit Field/Value Maps window, click **Browse For Fields**.
6. In the Browse for Fields/Values window, select a source for the list of available metadata fields:
 - To retrieve the metadata fields from the local Content Server instance, select **Local System**.
 - To retrieve the metadata fields from a batch file, select **Batch** and then select a batch file from the list.
7. Click **OK**.

The **Export Field** list is populated with the metadata fields that are associated with the Content Server instance or the selected batch file.

8. In the **Export Field** list, select the metadata field from which you want to copy metadata.
The selected metadata field is displayed in the **Export Field**. (You can also edit this field directly; make sure to use the internal field name, such as `dDocAuthor` or `xComments`.)
9. In the **Target Field** list, select the metadata field you want the Export metadata to be copied to.
10. Click **Add**.

The mapping expression is added to the **Field Maps** box.

11. To add to the mapping expression, repeat steps 8 through 10.
12. To update an existing mapping expression:
 - a. Select the line to be changed in the **Field Maps** box.
 - b. Edit the **Export Field** and **Target Field** as necessary.
 - c. Click **Update**.

The specified mapping expression replaces the selected line.

13. To delete a line from the mapping expression:

- a. Select the line to be deleted in the **Field Maps** box.
 - b. Click **Delete**.
The selected line is deleted.
14. Click **OK**.
During import, the values from the **Export** field replace any existing values in the **Target** field.
 15. To test the results of your field maps, import a few individual revisions from an archive. See [Importing an Individual Revision](#).

27.3.3 Setting Value Maps

Value maps specify how specific metadata values are to be changed during import. If you do not want to change metadata values, do not specify any value maps.

To set up value maps:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. Click the Import Maps main window.
4. Click **Edit** in the Value Maps section.
 - In the Edit Field/Value Maps window, to change all metadata values for a particular field, select **All**. Continue with step [11](#).
 - To change a specific metadata value, click **Browse For Values**.
5. In the Browse for Fields/Values window, select a batch file from the **From Batch File** list.
6. Select a metadata field from the **From Field** list.
7. Click **OK**.
The **Input Value** list is populated with the values that are associated with the selected metadata field in the selected batch file.
8. In the **Input Value** list, select the metadata value to be changed.
9. In the **Field** list, select the metadata field to be changed.
10. In the **Output Value** field, enter the new metadata value.
 - You can use Idoc Script in the output value. For example, to set the expiration date one week in the future for all imported revisions, you could use `<dateCurrent (7) $>`. For more information, see *Introduction to the Idoc Script Custom Scripting Language in Developing with Oracle WebCenter Content*.
 - To delete all values from the input metadata field, leave the output value blank.
11. Click **Add**.
The mapping expression is added to the **Value Maps** box.
12. To add to the mapping expression, repeat steps [5](#) through [11](#).
13. To update an existing mapping expression:
 - a. Select the line to be changed in the **Value Maps** box.
 - b. Edit the **Input Value**, **Field**, and **Target Value** as necessary.
 - c. Click **Update**.

The specified mapping expression replaces the selected line.

14. To delete a line from the mapping expression:

- a. Select the line to be deleted in the **Value Maps** box.
- b. Click **Delete**.

The selected line is deleted.

15. Click **OK**.

During import, the specified **Input Values** in the specified metadata Fields will be replaced with the **Target Values**.

16. To test the results of your value maps, import a few individual revisions from an archive. See [Importing an Individual Revision](#).

27.3.4 Setting Import Options

To set general import options:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. In the **General** tab of the Archiver window, click **Edit** in the Import Options section.
4. In the Edit Import Options (Select Rules) window, select an option in the **Override Import Rules** list to specify how existing revisions are added, replaced, or deleted during import. For detailed descriptions, see [About Import Rules](#).

Caution:

The *Update* import rule will replace existing revisions without saving the existing files. *Be extremely careful when importing so that you do not accidentally replace content you meant to keep.*

5. Specify whether option list values are validated during import:
 - To import only revisions with valid option list values (validated option lists only), select **Import only revisions with valid option list values**.
 - To skip option list validation, deselect **Import only revisions with valid option list values**.

Note:

The **Import only revisions with valid option list values** check box applies to all validated option lists. If you want to validate some option list fields but not all of them, you can change the **Option List Type** in the Configuration Manager. Use **Select List Validated** for option lists you want to validate; use **Select List Not Validated** for option lists you do not want to validate.

6. Specify whether to recalculate times in metadata date fields to reflect the time zone of the target Content Server instance:
 - To recalculate times, select **Translate the dates to the current system time zone**.

For example, if the time zone of the source (export) Content Server instance is Central Standard Time and the time zone of the target (import) Content Server instance is Eastern Standard Time, the release times, create times, expiration times, and any custom times will be changed to one hour later.

- To leave times unchanged, deselect **Translate the dates to the current system time zone**.
7. Click **OK**.
 8. To test the results of your import options, import a few individual revisions from an archive. See [Importing an Individual Revision](#).

27.3.5 Importing an Individual Revision

To import a specific revision:



Note:

Before importing an entire batch file, use this procedure to import a few individual revisions to test the results of your import maps and rules.

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the **Current Archives** list.
3. In the **General** tab of the Archiver window, click **View Batch Files**.
4. In the Removing Revisions from a Batch File window, select the batch file that contains the file you want to import.
5. Click **Edit**.
6. In the View Exported Content Items window, use the **Filter** feature and the navigation buttons to display the revision to be imported.
7. Select the revision.
8. Click **Import**.

If the revision was imported successfully, a confirmation message is displayed.

27.3.6 Initiating the Import

To initiate import of content and configuration information:

1. Open Archiver for the Content Server instance to which you want to import information.
2. Open the archive collection from which you want to import information. (This collection must be accessible through the file system.) See [Opening a Collection](#).
3. Select the archive in the **Current Archives** list.
4. From the **Actions** menu, choose **Import**.
5. In the Import Archiver window, specify the information to be imported:
 - To import content, select **Import Batched Revisions**.
 - To import content and tables, select **Import Tables**.

 **Note:**

The **User Configuration** and **Content Configuration** options are available only if the selected archive includes this information (`users.hda` or `doctypes.hda` file).

6. Click **OK**.

The import process is initiated, and the status bar at the bottom of the Archiver page displays progress messages.

Transferring Files

This chapter provides information on moving or copying content from one Oracle WebCenter Content Server instance to another over sockets by using the Transfer function of the Archiver utility.

This chapter covers the following topics:

- [Introduction to Transferring Files](#)
- [Understanding Transfer Types](#)
- [How Transferring Batch Files Works](#)
- [Managing Transfers](#)

28.1 Introduction to Transferring Files

You can use the Transfer function of the Archiver utility to transfer files between Content Server instances on a shared file system, but transfers *do not require* a shared file system. Transferring files between non-shared file systems requires an outgoing provider on the source Content Server instance.

Transfers are successful only between Content Server version 4.5 or newer systems.

Important:

Archiver cannot be used to move or copy data between two instances that share the same Content Server instance name (*IDC_Name*). To do so will corrupt the data on the target system.

This section covers these topics:

- [Transfer Uses](#)
- [Transfer Methods](#)
- [Transfer Terms](#)

28.1.1 Transfer Uses

Typical uses for the Transfer function include:

- Exporting and importing content over a firewall.

Note:

To transfer across a firewall, you might need to configure the firewall to permit the outgoing provider's socket to pass through it.

- Transferring content between Content Server instances in different physical locations (buildings, cities, or countries).
- Transferring content between Content Server instances using a shared drive. (A transfer over a file system share can handle large archives better than a socket transfer.)
- Avoiding the need to build a FTP or HTTP interface to move files from one file system to another.
- Combining the batch files from two archives into a single archive.

28.1.2 Transfer Methods

You can transfer files in the following ways:

- **Manual Transfer:** A one-time transfer initiated from Archiver by an administrator. This *copies* an archive to another archive.
- **Automatic Transfer:** *Moving* archive files to another archive is initiated automatically whenever the source archive is updated.

28.1.3 Transfer Terms

The following terms are related to the Transfer function:

- **local archive:** An archive that belongs to a local collection.
- **local collection:** A collection that the Content Server instance can reach by file access using a mapped or mounted network share.
- **local transfer:** A transfer between local archives. Both the source archive and the target archive are in a local collection.
- **proxied:** In Archiver, the term **proxied** refers to any Content Server instance to which the local Content Server instance is connected through an outgoing provider.
- **proxied archive:** An archive that belongs to a proxied collection.
- **proxied collection:** A collection on another Content Server instance that the local Content Server instance can reach through an outgoing provider.
- **pull transfer:** A transfer over an outgoing provider that is owned by the proxied (remote) Content Server instance.
- **push transfer:** A transfer over an outgoing provider that is owned by the local Content Server instance.
- **source archive:** An archive that contains batch files to be transferred.
- **target archive:** An archive that receives transferred batch files.
- **targetable archive:** An archive that is enabled to be a target archive.
- **transferring:** The process of copying or moving batch files and their associated content files from one archive to another. There are three types of transfers: *local*, *push*, and *pull*.
- **transfer owner:** The Content Server instance that performs and monitors a transfer.
- **transfer source:** See *source archive*.
- **transfer target:** See *target archive*.

28.2 Understanding Transfer Types

This section provides information about the different transfer types, listed in order from simplest to most complex.

- [Local Transfer](#)
- [Pull Transfer](#)
- [Push Transfer](#)

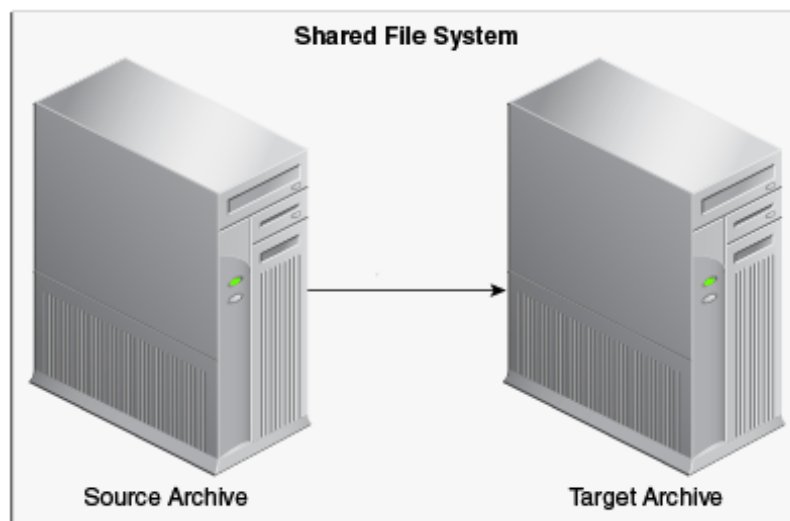
28.2.1 Local Transfer

A *local transfer* is a transfer between local archives, which belong to collections that both the source and target Content Server instances can reach through a mapped or a mounted drive. An outgoing provider is not required. This type of transfer is typically used to combine the batch files of two archives.

 **Note:**

If you are transferring between Content Server instances on a shared file system, the mapped or mounted drive must be available to both Content Server instances. The computers must be on and logged in as a user who has system access to both Content Server instances.

Figure 28-1 Local Transfer



28.2.2 Pull Transfer

A *pull transfer* is a transfer that is owned by the proxied (remote) Content Server instance, which is the instance that is the target of the outgoing provider.

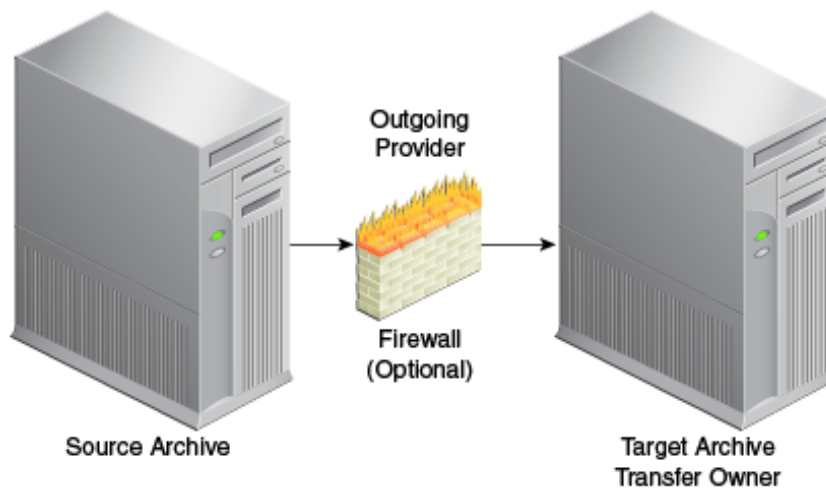
- Multiple pull transfers can be concurrent.

- If you are running a pull transfer across a firewall, you might need to configure the firewall to permit the outgoing provider's socket to pass through it.

 **Note:**

In Archiver, the term *proxied* refers to any Content Server instance to which the local instance is connected through an outgoing provider.

Figure 28-2 Pull Transfer

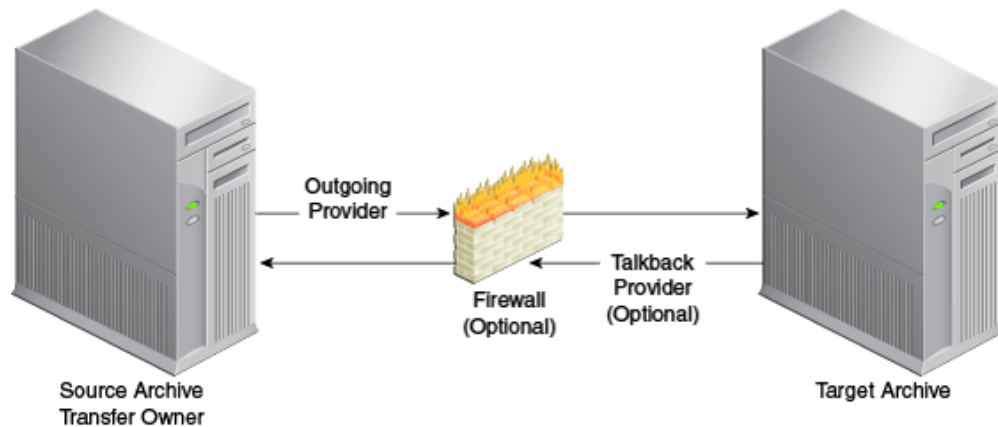


28.2.3 Push Transfer

A *push transfer* is a transfer that is owned by the local Content Server instance, which is the instance on which the outgoing provider is set up.

- For performance monitoring of a push transfer, you also should set up an outgoing provider from the target (proxied) Content Server instance back to the source (local) Content Server instance. This *talkback* provider can then notify the source Content Server instance when each transfer is complete. A push transfer will work without the talkback provider, but the source Content Server instance would not be aware of transfer completion or problems.
- Only one push transfer can be in progress at a time.
- If you are running a push transfer across a firewall, you might need to configure the firewall to permit the both providers' sockets to pass through it.

Figure 28-3 Push Transfer



28.3 How Transferring Batch Files Works

This section provides information about how transferring batch files works.

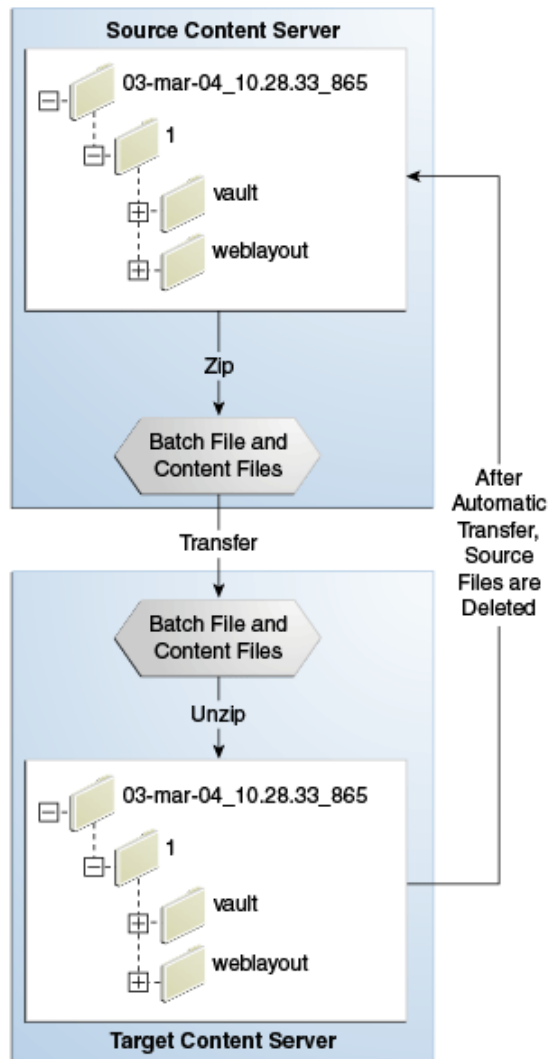
28.3.1 Transfer Process Actions

When a transfer is initiated, the following actions occur:

1. Each batch file in the archive is zipped together with its associated content files.
2. The Zip files are transferred to the target Content Server instance by a local file system move (local transfer) or by the outgoing provider (push or pull transfer).
3. The Zip files are unzipped and placed in the appropriate file system locations.
4. For an automated transfer, the batch files and their associated content files are removed from the source Content Server instance. For a manual transfer, the batch files and associated content files remain in the source Content Server instance.

The transferred archive is now available for import through the Archiver of the target Content Server instance.

Figure 28-4 The Transfer Process



28.3.2 Transfer Rules

The following list provides applicable transfer rules:

- If you are transferring between Content Server instances on a shared file system, the mapped or mounted drive must be available to both Content Server instances. The computers must be on and logged in as a user who has system access to both Content Server instances.
- The Content Server instance that has an outgoing provider set up is considered the local server, and the target Content Server instance for the outgoing provider is considered the proxied server. Files are always transferred in the direction of the outgoing provider, from the local (source) instance to the proxied (target) instance.
- To transfer multiple archives from a Content Server instance, you must set up a separate outgoing provider from the local instance for each target instance.
- Only archives that are identified as *targetable* can be transfer targets. When you are selecting a transfer target, the targetable attribute can help you find the target archive quickly.

- At least one archive in the transfer must be local to the transfer owner. For example, you cannot set up a transfer between two Content Server instances that is owned by a third Content Server instance.
- An archive can contain only one copy of each batch file. Therefore, if a batch file being transferred already exists in the target archive, the batch file and its associated content files will be ignored.

28.4 Managing Transfers

This section provides information about tasks for managing transfers.

- [Transferring Content](#)
- [Making an Archive Targetable](#)
- [Defining an Outgoing Transfer Provider](#)
- [Setting a Transfer Destination \(Target\)](#)
- [Initiating a Manual Transfer](#)
- [Deleting a Transfer](#)

28.4.1 Transferring Content

To transfer content between Content Server instances:

1. In the source Content Server instance, create the archive to be transferred and set up an export to this archive. See [Manually Exporting](#).
2. In the target Content Server instance, create the archive to receive transferred content and make the target archive targetable. See [Making an Archive Targetable](#).
3. Set up communications between the Content Server instances:
 - If the source and target archives are on a shared file system, ensure that both computers are on and logged in as a user who has system access to both Content Server instances.
 - If the source and target archives are not on a shared file system, create an outgoing provider from the source Content Server instance to the target Content Server instance. See [Defining an Outgoing Transfer Provider](#).
4. From the source archive, specify the target archive. See [Setting a Transfer Destination \(Target\)](#).
5. Initiate the transfer. See [Initiating a Manual Transfer](#).

The batch files and content files are copied to the target archive.

28.4.2 Making an Archive Targetable

To indicate that an archive can receive transfers from other archives (be *targetable*):

1. Open the archive collection that contains the target archive. See [Opening a Collection](#).
2. Select the target archive in the **Current Archives** list.
3. Click the Main Archiver Transfer window.
4. Click **Edit** in the Transfer Options section.
5. In the Transfer Options window, select **Is Targetable**.

6. Click **OK**.

28.4.3 Defining an Outgoing Transfer Provider

To create an outgoing provider for transfer purposes:

1. In the source Content Server instance, create an outgoing provider. Enter the following information:

Element	Description
Provider Name	Enter a name. This will become a subdirectory in the <i>DomainHome/ucm/cs/data/providers/</i> directory.
Provider Description	Enter a user-friendly description. For example, <i>Transfer Provider</i> .
Server Host Name	Enter the server host name of the target Content Server instance. For example, <i>extranet_server</i> .
Server Port	Enter a unique port number on which the provider will communicate with the target Content Server instance.
Instance Name	Enter the name of the target Content Server instance. For example, <i>instance_on_extranet</i> .
Relative Web Root	Enter the relative web root of the target Content Server instance. For example, <i>/company_name/</i> .

2. Using the System Properties utility of the target Content Server instance, set the **IP Address Filter** or **Hostname Filter** to the IP address or host name of the source Content Server instance. (The IP Address Filter setting is recommended.)
3. If you are setting up a push transfer (transfer owned by the local Content Server instance), consider setting up a *talkback* outgoing provider from the target Content Server instance back to the source Content Server instance.
4. If you are transferring across a firewall, configure the firewall to permit the outgoing providers' sockets to pass through it.

28.4.4 Setting a Transfer Destination (Target)

To specify the target archive to receive transferred content:

1. Open Archiver from the Content Server instance that will own the transfer.
 - For a pull transfer, the transfer owner is the target (proxied) Content Server instance.
 - For a push transfer, the transfer owner is the source (local) Content Server instance.
2. Open the archive collection that contains the source archive. See [Opening a Collection](#).
3. Select the source archive in the **Current Archives** list.
4. Click the Main Archiver Transfer window.
5. Click **Edit** in the Transfer Destination section.
6. In the Archive Collections window, select the collection that contains the target archive.
7. Select the target archive.

 **Note:**

The target archive must be identified as targetable. See [Making an Archive Targetable](#).

8. Click **OK**.

28.4.5 Initiating a Manual Transfer

To transfer content manually:

1. Open Archiver on the source Content Server instance.
2. Open the archive collection that contains the source archive. See [Opening a Collection](#).
3. Select the source archive in the **Current Archives** list.
4. Select **Actions**, then click **Transfer**.

The transfer process is initiated, and the status bar at the bottom of the Archiver page displays progress messages.

28.4.6 Deleting a Transfer

This section describes procedures for deleting a transfer.

28.4.6.1 Deleting a Transfer

To delete a transfer from the **Transfer to** tab:

1. Open the archive collection that contains the source archive. See [Opening a Collection](#).
2. Select the source archive in the **Current Archives** list.
3. Click the Main Archiver Transfer window.
4. Click **Remove** in the Transfer Destination section.
5. When prompted to confirm the action, click **Yes**.

28.4.6.2 Deleting an Automated Transfer

To delete an automated transfer from the Automation for Instances page:

1. Open the archive collection. See [Opening a Collection](#).
2. Choose **Options**, then **View Automation For Instance**.
3. In the Automation window, click the **Transfers** tab.
4. Select the automated transfer to delete.
5. Click **Remove**.

The automated transfer is removed from the list.

Replicating Files

This chapter describes how to automate the export, import, and transfer of content files by using the Archiver utility Replication function in Oracle WebCenter Content.

This chapter covers the following topics:

- [Understanding Replication](#)
- [Managing Replication](#)

29.1 Understanding Replication

If you are automating the import of WebCenter Content files using replication, each batch file is removed as soon as the automatic import is complete. You can view the archiving results by preparing an Archive History report using the Web Layout Editor. See *Working with Reports in Developing with Oracle WebCenter Content*.

If you are replicating files to a contribution server, you should map the **Security Group** and/or **Account** field so that users have only Read permission to the imported files. Otherwise, changed files in the importing instance could be overwritten by exported files during a later replication cycle.

For performance reasons, replication is not recommended for large archives (approximately 20,000 files or more). Export and import of large archives should be run manually, during periods of non-peak usage if possible.

Caution:

The Archiver utility cannot be used to move or copy data between two instances that share the same Content Server instance name (*IDC_Name*). To do so corrupts the data on the target system.

When Archiver automatic replication is configured between instances of WebCenter Content, every action is replicated between environments: Check in, Update, and Delete. For information on preventing Archiver from replicating Delete actions, see the "Preventing Deletes from Replicating In Archiver" blog.

This section covers these topics:

- [Replication Uses](#)
- [Replication Methods](#)
- [Single Revision Replications](#)

29.1.1 Replication Uses

Typical uses for the Replication function include:

- Automatically exporting content from one Content Server instance and importing to another Content Server instance to synchronize two websites.
- Copying content automatically between two contribution/consumption servers.
- Automatically moving certain documents from a contribution server to a higher-security Content Server instance.
- Automatically moving old content to a storage location.

 **Note:**

The Replication function does not import content types and user attributes.

29.1.2 Replication Methods

You can automate Archiver functions in the following ways:

- **Automatic Export:** Export to a local archive is initiated automatically whenever a content item that meets the export criteria is indexed.
- **Automatic Import:** Import from a local archive is initiated automatically, about once per minute.
- **Automatic Transfer:** Moving archive files to a different Content Server instance over sockets is initiated automatically whenever the source archive is updated.

 **Note:**

You can export expired revisions manually, but expired revisions do not get exported automatically.

29.1.3 Single Revision Replications

When using the **Single Revision Replication** option on the Edit Export Query (Content) window, be aware of the following considerations:

- If the new document matches the archiver query on check-in, it is archived. If it does not match the query, nothing happens.
- If a document has multiple revisions and the most recent matching revision is deleted or updated so it no longer matches the query, the next most recent matching revision of that document is replicated. If no revisions match the query, that document is deleted through replication.
- If a system (A) is replicating to system (B) and the **Single Revision Replication** option is used, system B will at any given time only have one revision of each document. The revLabel of each revision is 1, no matter what the revLabel was on the document that was replicated.

This archiving option allows an administrator to create a staging system and a production system. The staging system can archive all documents that have a specific metadata field set to 1. The production system will always have the most recent revision of each document that has this metadata flag set. Setting this flag to 0 on the staging system removes it from the

production system and rolls it back to the next most recent revision with that metadata field set to 1.

29.2 Managing Replication

Several tasks are involved in managing the replication process, including setting up automatic exports, imports and transfers. This section provides information about replication tasks.

- [Setting Up Automatic Export](#)
- [Setting Up Automatic Import](#)
- [Setting Up Automatic Transfer](#)
- [Disabling Automatic Import](#)
- [Disabling Automatic Export](#)
- [Disabling Automatic Transfer](#)
- [Deleting a Registered Exporter](#)

29.2.1 Setting Up Automatic Export

To set up an automatic export:

1. Set up the export and run a manual export. See [Manually Exporting](#).
2. Open Archiver on the Content Server instance that content is to be exported from.
3. Open the archive collection.
4. Select the archive to export to automatically in the Current Archives list.
5. Click the **Replication** tab.
6. Click **Edit**.
7. In the Registered Exporter window, select **Enable Automated Export**.
8. Click **Register**.

The current collection is added to the Registered Exporters box.

9. Click **OK**.

Each revision that meets the export criteria will be exported to this archive when it is indexed. The batch file is removed as soon as each export is complete.

Note:

You can export expired revisions manually, but expired revisions do not get exported automatically.

29.2.2 Setting Up Automatic Import

To set up an automatic import:

1. Set up the import and run a manual import. See [Importing Data](#).
2. Open Archiver on the Content Server instance that the archive is to be imported to.

3. Open the archive collection.
4. Select the archive to import automatically in the Current Archives list.
5. Click the **Replication** tab.
6. Click **Register Self**.
7. When prompted to confirm the action, click **OK**.

The selected archive will be imported automatically, about once per minute. All source batch files are removed as soon as each import is complete.

 **Note:**

The Replication function does not import content types and user attributes.

29.2.3 Setting Up Automatic Transfer

To set up an automatic transfer:

1. Set up the transfer and run a manual transfer. See [Introduction to Transferring Files](#).
2. Open Archiver on the source Content Server instance.
3. Open the archive collection.
4. Select the source archive in the Current Archives list.
5. Click the **Transfer To** tab.
6. Click **Edit**.
7. In the Transfer Options window, select **Is Transfer Automated**.
8. Click **OK**.
9. Test the automatic transfer:
 - a. In the source Content Server instance, check in a new document that meets the export criteria.
 - b. If the export is automated, wait until automated export occurs after indexing. Otherwise, export the source archive manually. The archive should be transferred to the target Content Server instance within a few minutes.

 **Note:**

The Replication function does not import content types and user attributes.

29.2.4 Disabling Automatic Import

This section provides information about the methods to disable an automatic import.

29.2.4.1 Unregistering an Importer from the Replication Tab

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the Current Archives list.

3. Click the **Replication** tab.
4. Click **Unregister**.
Automatic importing from the selected archive is disabled.

29.2.4.2 Disabling a Registered Importer from the Automation for Instance Page

1. Open the archive collection. See [Opening a Collection](#).
2. From **Options**, choose **View Automation For Instance**.
3. In the Automation for Instance page, click the **Importers** tab.
4. Select the registered importer to delete.
5. Click **Remove**.
The registered importer is removed from the list.

29.2.5 Disabling Automatic Export

To disable automatic export:

1. Open the archive collection. See [Opening a Collection](#).
2. Select the archive in the Current Archives list.
3. Click the **Replication** tab.
4. Click **Edit**.
5. In the Registered Exporter window, deselect **Enable Automated Export**.
6. Click **OK**.
Automatic exporting of the selected archive is disabled.

29.2.6 Disabling Automatic Transfer

To disable automatic transfer:

1. Open Archiver on the source Content Server instance.
2. Open the source archive collection. See [Opening a Collection](#).
3. Select the source archive in the Current Archives list.
4. Click the **Transfer To** tab.
5. Click **Edit**.
6. In the Transfer Options window, deselect **Is Transfer Automated**.
7. Click **OK**.
Automatic transfer of the selected archive is disabled.

29.2.7 Deleting a Registered Exporter

This section provides information about the methods to delete a registered exporter.

29.2.7.1 Deleting a Registered Exporter from the Replication Tab

1. Open the archive collection. See [Opening a Collection](#).

2. Select the archive in the Current Archives list.
3. Click the **Replication** tab.
4. Click **Edit**.
5. In the Registered Exporter window, select **Enable Automated Export**.
6. Select the Content Server instance to delete in the **Registered Exporters** list.
7. Click **Remove**.
The registered exporter is removed from the list.
8. Click **OK**.

29.2.7.2 Deleting a Registered Exporter from the Automation for Instance Window

1. Open the archive collection. See [Opening a Collection](#).
2. From **Options**, choose **View Automation For Instance**.
3. In the Automation for Instance window, select the registered exporter to delete.
4. Click **Remove**.
The registered exporter is removed from the list.

Migrating the Folders Structure

This chapter explains how to use the Archiver utility to migrate Folders structure data (but not content files) in Oracle WebCenter Content Server. Folders functionality is supported by the FrameworkFolders component.

This chapter covers these topics:

- [About Migrating Folders Structure](#)
- [Exporting Folders Structure Data](#)
- [Importing Folders Structure Data](#)

30.1 About Migrating Folders Structure

The Folders structure for a Content Server instance can be migrated (exported or imported) by using the Archiver utility.

For information about how Archiver works, see [Managing Archives Collections and Batch Files](#).

30.2 Exporting Folders Structure Data

This section describes the process and tasks for manually exporting data from the Content Server instance for backup, storage, or import to another Content Server instance. The Export function in the Archiver utility can be used to export Folders structure data. Note that this exports only a copy, the original data remains.

A manual export is a one-time export initiated from Archiver by an administrator. This creates an archive on the local Content Server instance.

Caution:

Do not use Archiver as your primary method of disaster recovery; use standard backup systems for the database and file system. For information on backup systems, see *Administering Oracle Fusion Middleware*.

To manually export Folders structure data, follow this process:

1. Create an archive where the exported Content Server data will be stored. For details, see [Creating a New Archive](#).
2. Select the archive in the Current Archives list.
3. Add tables to the archive. For details, see [Adding a Table to an Archive](#).

You must add the following tables to the archive:

- FoldersFolders
- FolderMetaDefaults

4. Initiate the export. For details, see [Initiating the Export](#).

For more information on how to manage exports using the Archiver utility, see [Exporting Data in Archives](#) .

30.3 Importing Folders Structure Data

This section describes the process and tasks for manually retrieving data from an exported archive. Importing is typically used to obtain a copy of data from another Content Server instance or to restore data that has been in storage. The Import function in the Archiver utility can be used to import Folders structure data.

The Content Server instance to which you are importing must have the same metadata fields, security groups, and accounts as the instance that the archive was exported from. Errors can result if there are mismatches.

To manually import the Folders structure data, follow this process:

1. Using Archiver, in the Current Archives list select the archive from which to retrieve data.
2. Initiate the import. For details, see [Initiating the Import](#).

For more information on how to manage imports using the Archiver utility, see [Importing Data from Archives](#) .

31

Archive and Migration Strategies

This chapter provides information about several typical archiving and migration strategies for Oracle WebCenter Content Server.



Note:

All of the scenarios described in this section can be run manually or automatically (through replication).

This chapter covers the following topics:

- [Export](#)
- [Import](#)
- [Self Export/Import](#)
- [One-to-One Archiving](#)
- [One-to-Many Archiving](#)
- [Many-to-One Archiving](#)
- [Archiver Examples](#)
- [Configuration Migration Tips](#)

31.1 Export

This section provides information about strategies for exporting.

Summary

A simple export is typically used to:

- Store and later remove outdated content on a file system.
- Store content on a file system for later retrieval.
- Retain a snapshot of a Content Server instance at a certain date and time.

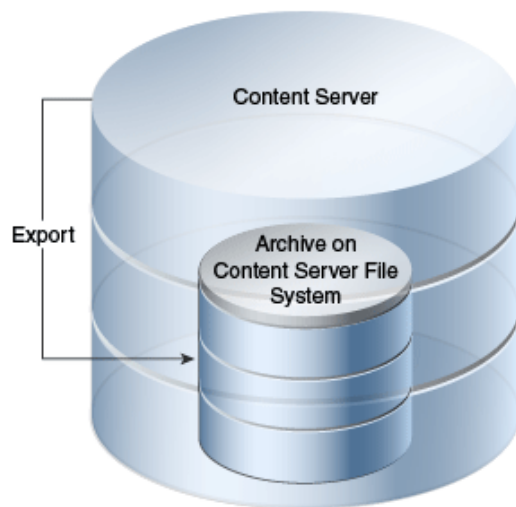
Configurations

The following are possible export-only configurations, shown in order from most to least typical:

- Export to a collection on an external file system.

Figure 31-1 Export to External File System

- Export to one of the Content Server instance's own collections.

Figure 31-2 Export to Own Collection

31.2 Import

This section provides information about importing.

Summary

A simple import is typically used to:

- Retrieve content from storage after an unintended deletion.
- Restore content from an archived 'snapshot' of a Content Server instance.

Configurations

The following are possible import-only configurations, shown in order from most to least typical:

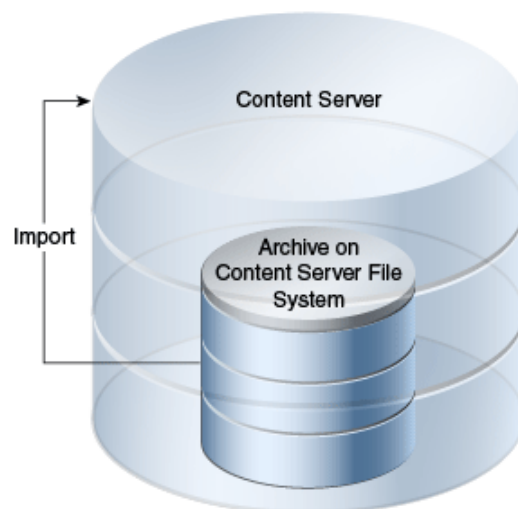
- Import from a collection on an external file system.

Figure 31-3 Import from External File System



- Import from one of the Content Server instance's own collections.

Figure 31-4 Import from Own Collection



31.3 Self Export/Import

This section provides information about self export.

Summary

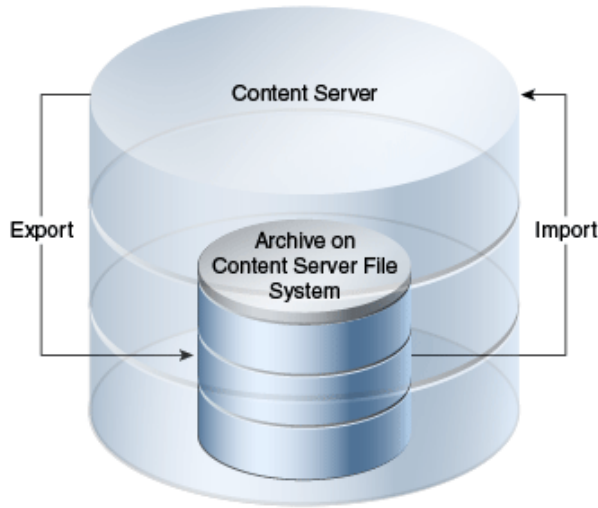
Self export/import is typically used to change content metadata to new values.

Configurations

The following are possible self export/import configurations, shown in order from most to least typical:

- Export to and import from one of the Content Server instance's own collections.

Figure 31-5 Self Export/Import from Own Collection



- Export to and import from a collection on an external file system.

Figure 31-6 Self Export/Import from External File System



31.4 One-to-One Archiving

This section provides information about one-to-one archiving.

Summary

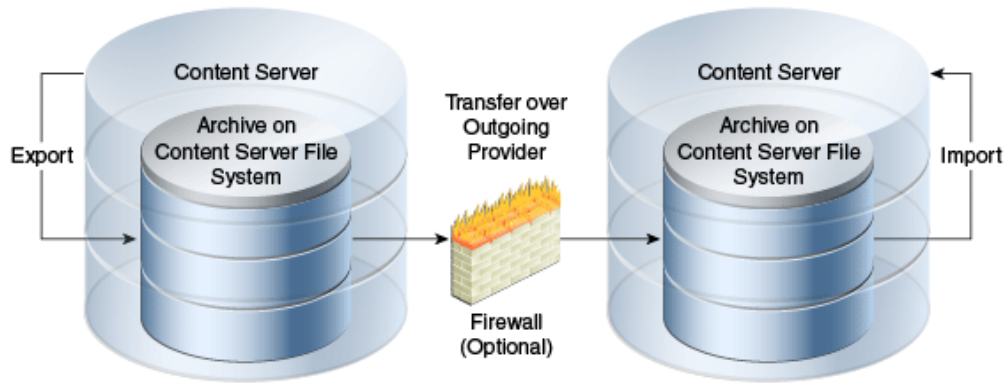
One-to-one archiving is used to copy or move content from one Content Server instance to another.

Configurations

The following are possible one-to-one archiving configurations, shown in order from most to least typical:

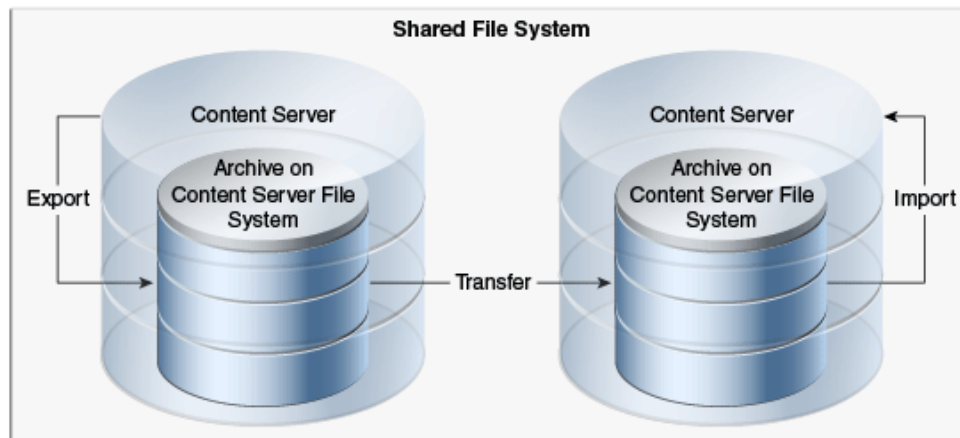
- Export, transfer, and import over sockets.

Figure 31-7 One-to-One Archiving: Over Sockets



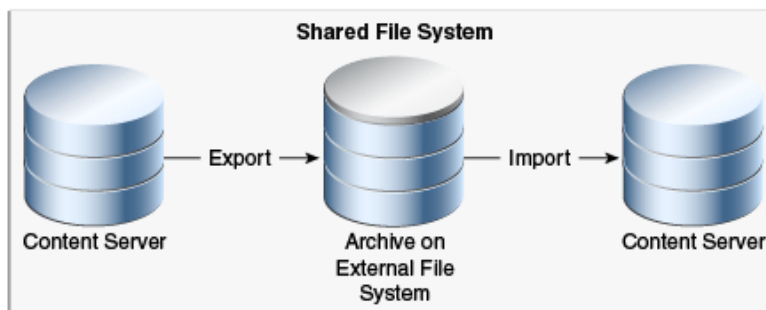
- Export, transfer, and import on a shared file system.

Figure 31-8 One-to-One Archiving: On Shared File System



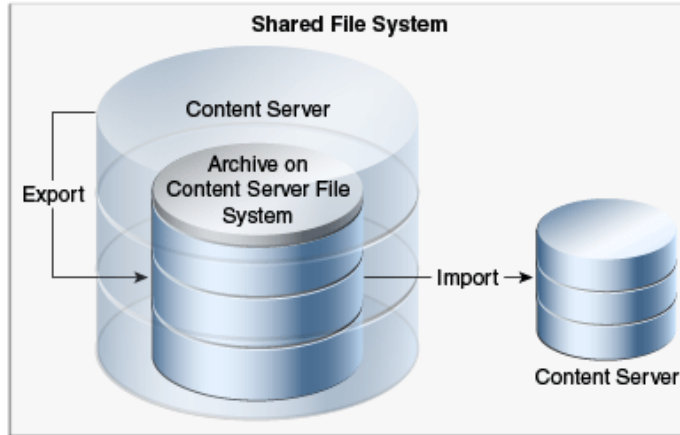
- Export to and import from a collection on a shared external file system.

Figure 31-9 One-to-One Archiving: On Shared External File System



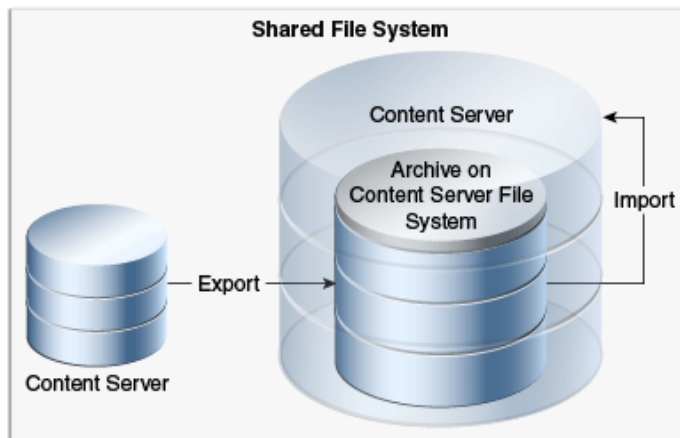
- Export to the source Content Server collection and import directly from that collection on a shared file system.

Figure 31-10 One-to-One Archiving: Export to Collection and Import from Collection on Shared File System



- Export from the source Content Server instance directly to a collection on the target Content Server instance and import from that collection on a shared file system.

Figure 31-11 One-to-One Archiving: Export from Source to Collection and Import from Collection on Shared File System



31.5 One-to-Many Archiving

This section provides information about one-to-many archiving.

Summary

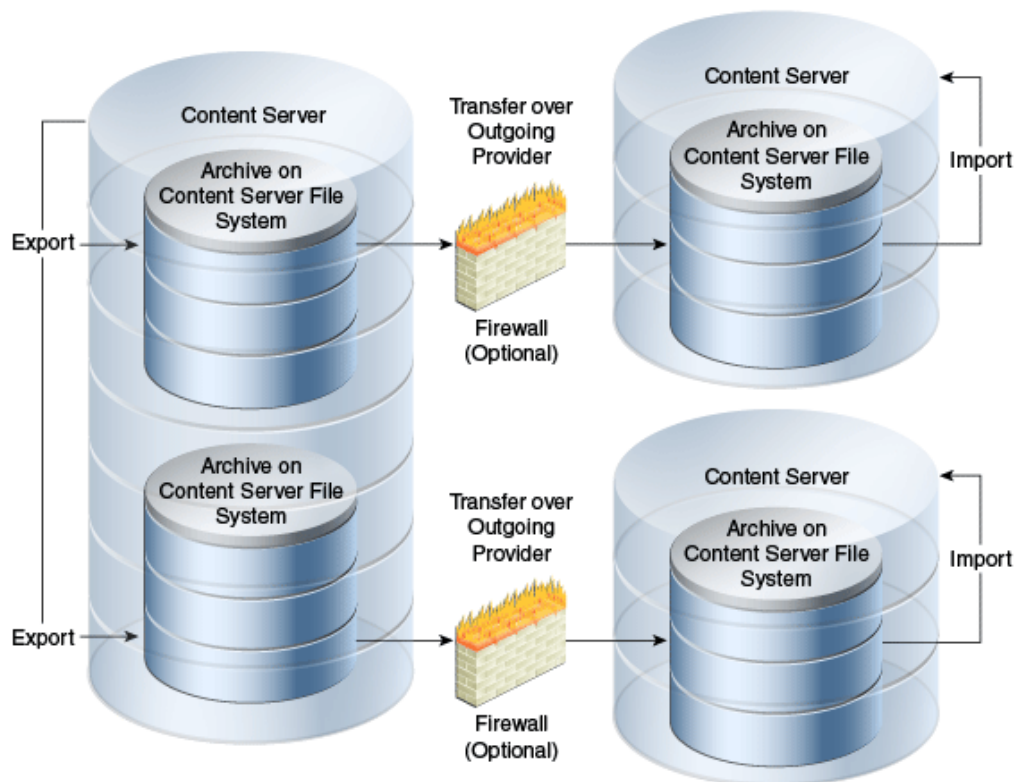
One-to-many archiving is typically used to copy or move content from a contribution server to consumption servers.

Configurations

The following are possible one-to-many archiving configurations, shown in order from most to least typical:

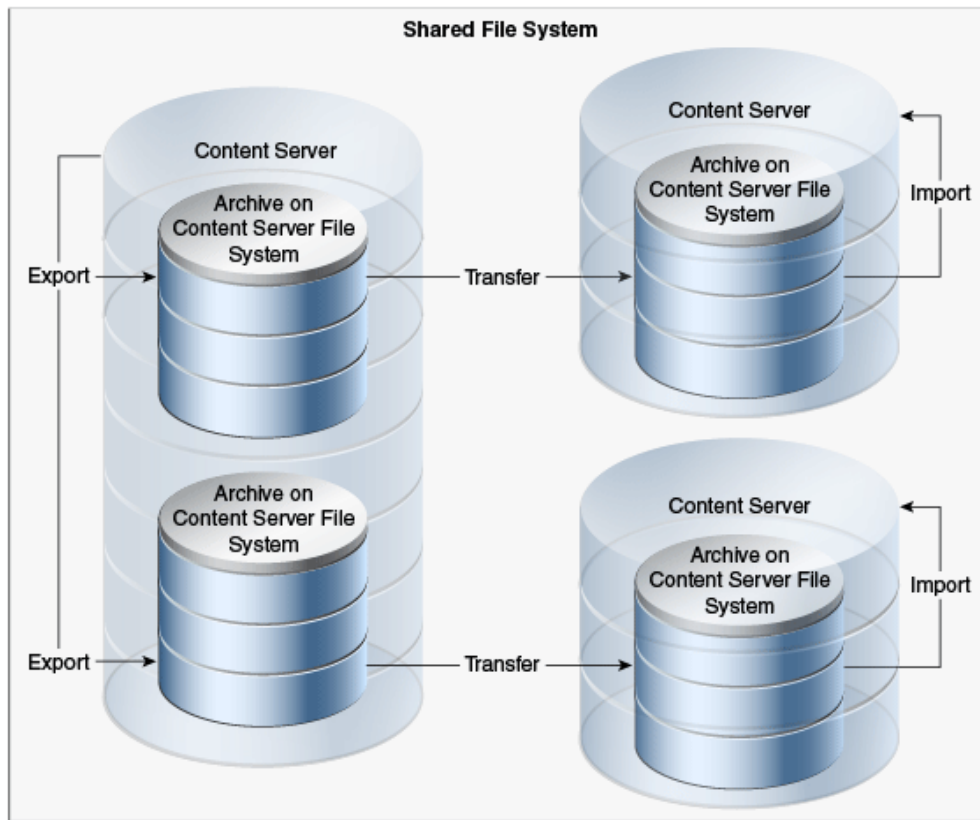
- Export, transfer, and import over sockets.
When this configuration is automated using replication, a separate export archive is required for each target server because the source files are deleted upon transfer. However, for manual transfer, you could transfer a single archive to multiple targets.

Figure 31-12 One-to-Many Archiving: Over Sockets



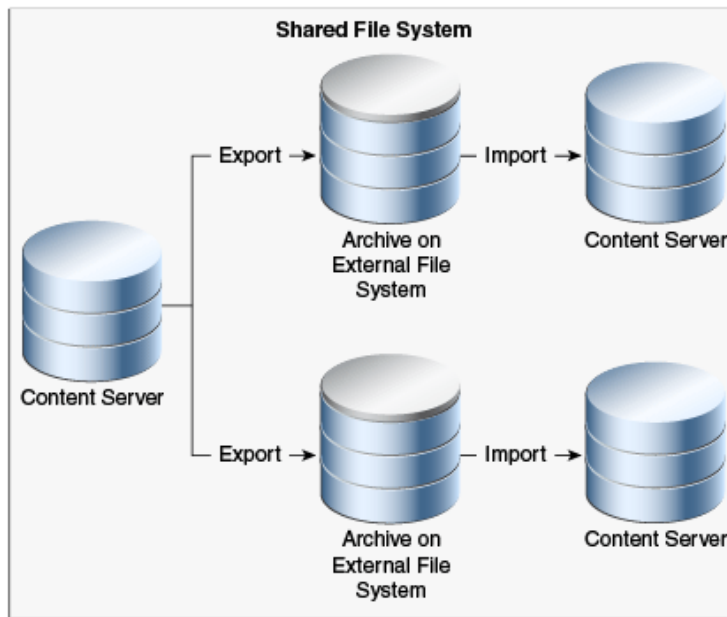
- Export, transfer, and import on a shared file system.
When this configuration is automated using replication, a separate export archive is required for each target server because the source files are deleted upon transfer. However, for manual transfer, you could transfer a single archive to multiple targets.

Figure 31-13 One-to-Many Archiving: On Shared File System



- Export to and import from a collection on a shared external file system.
When this configuration is automated using replication, a separate export archive is required for each target server because the source files are deleted upon import. However, for manual import, you could import a single archive from multiple targets.

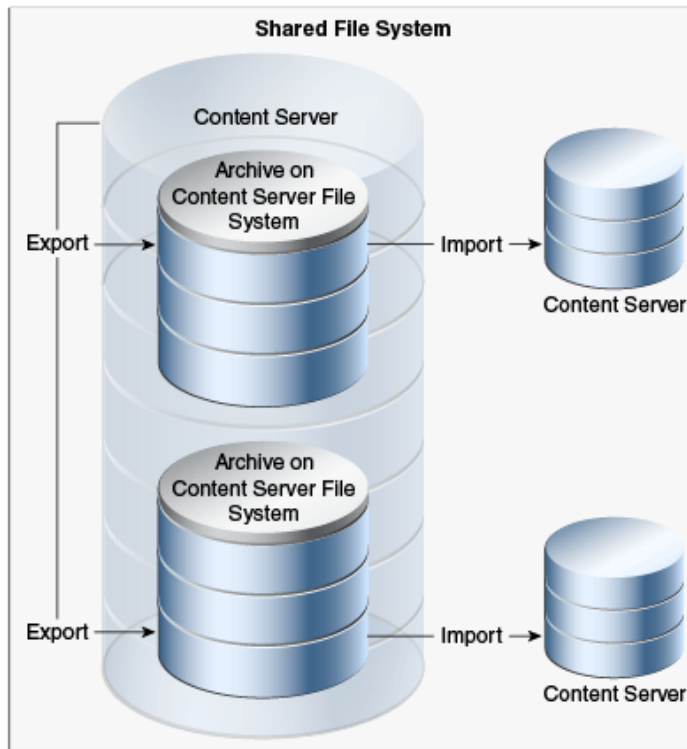
Figure 31-14 One-to-Many Archiving: On Shared External File System



- Export to the source Content Server collection and import directly from that collection on a shared file system.

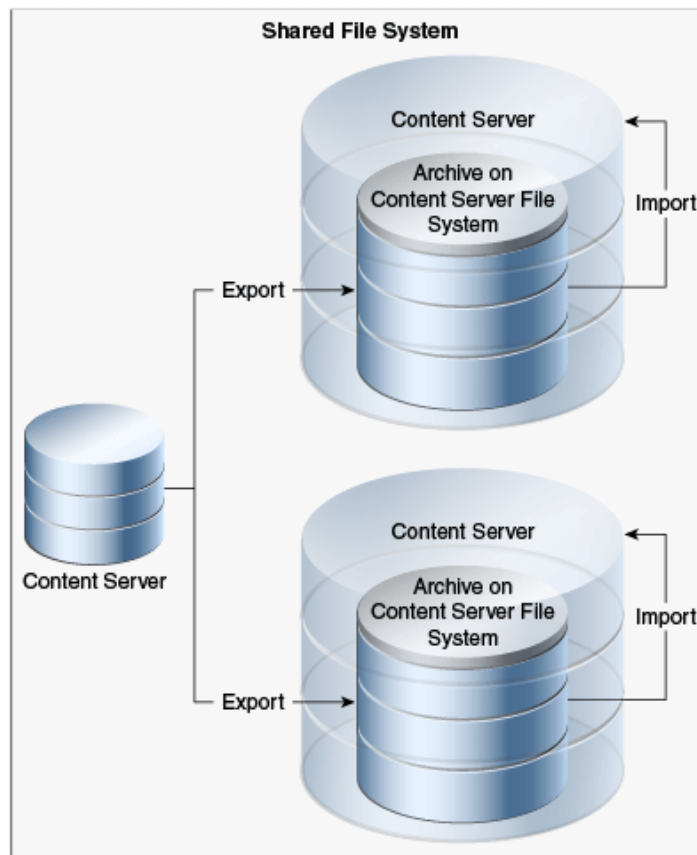
When this configuration is automated using replication, a separate export archive is required for each target server because the source files are deleted upon import. However, for manual import, you could import a single archive from multiple targets.

Figure 31-15 One-to-Many Archiving: Export to Collection and Import from Collection on Shared File System



- Export from the source Content Server instance directly to collections on the target Content Server instances and import from those collections on a shared file system.

Figure 31-16 One-to-Many Archiving: Export from Source to Collections and Import from Collections on Shared File System



31.6 Many-to-One Archiving

This section provides information about many-to-one archiving.

Summary

Many-to-one archiving is typically used to:

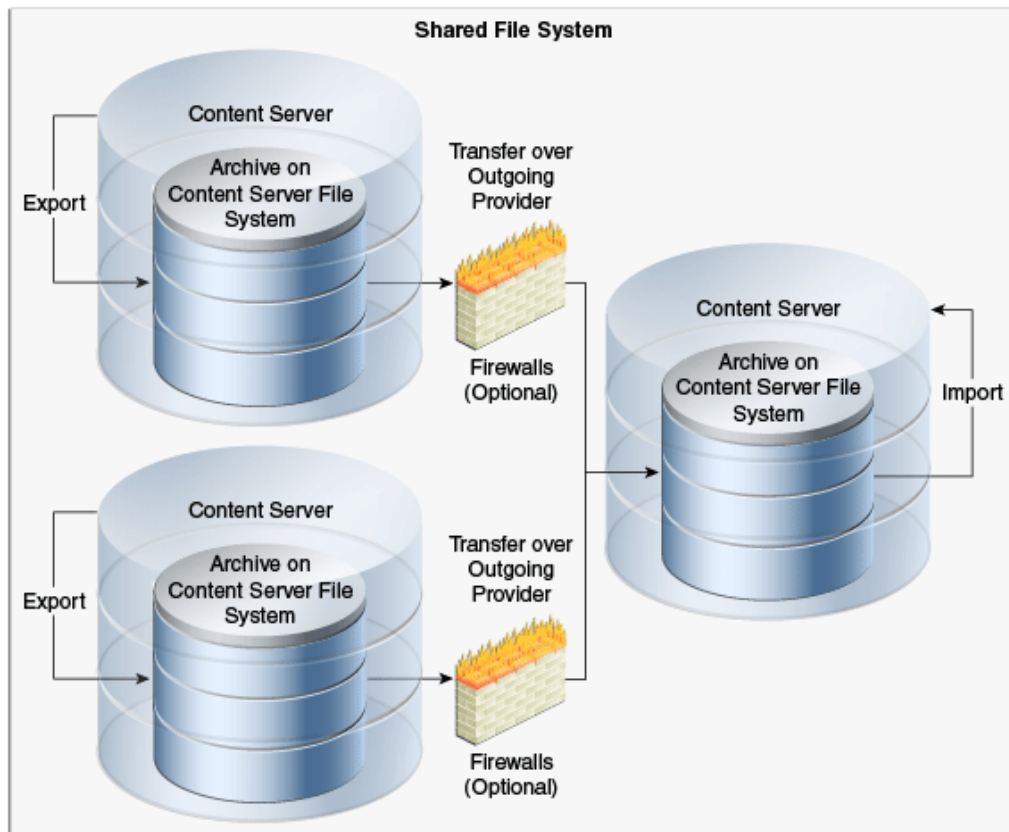
- Copy or move content from several contribution servers to one consumption server.
- Move sensitive content from several contribution servers to a more secure contribution server.

Configurations

The following are possible many-to-one archiving configurations, shown in order from most to least typical:

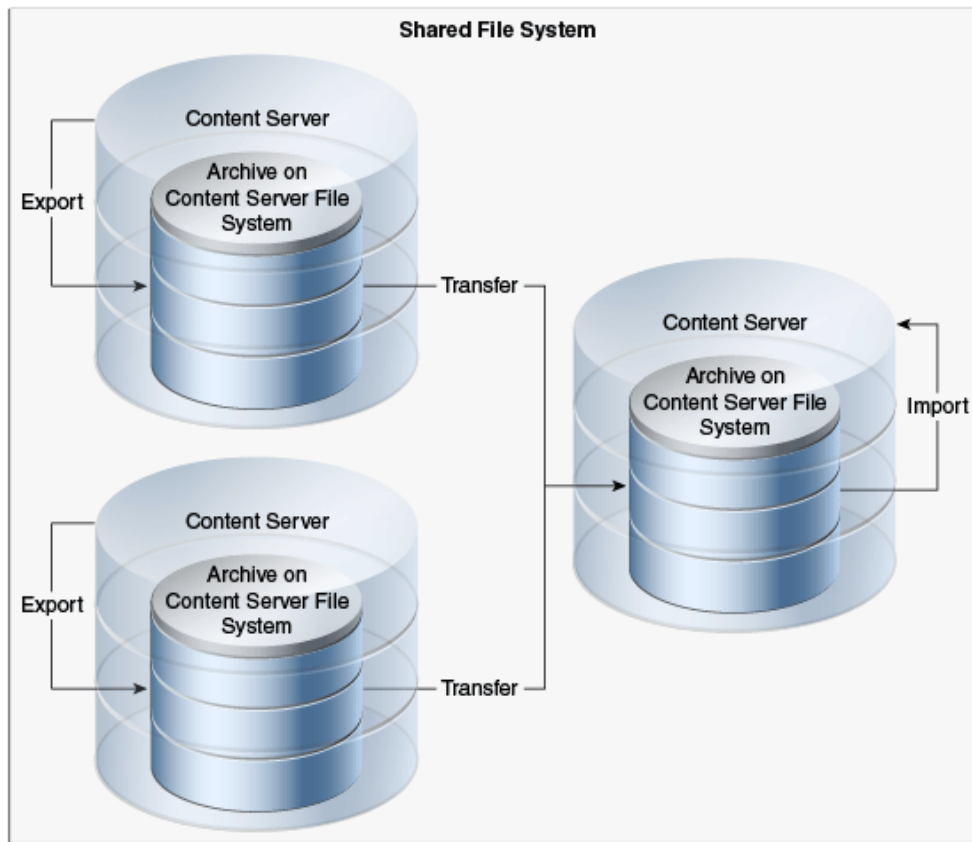
- Export, transfer, and import over sockets.

Figure 31-17 Many-to-One Archiving: Over Sockets



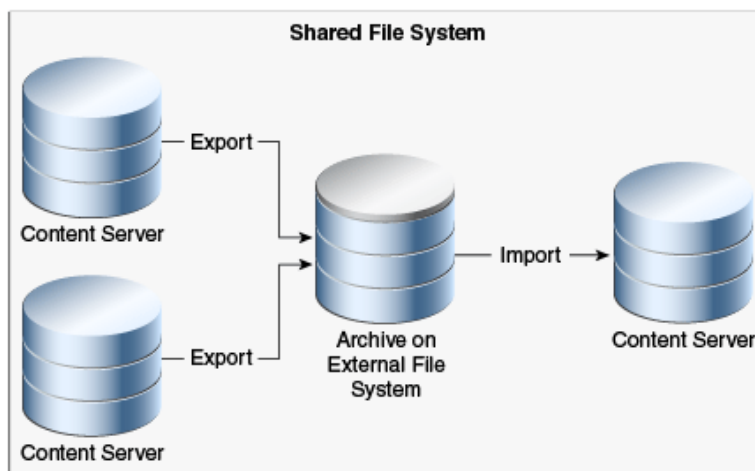
- Export, transfer, and import on a shared file system.

Figure 31-18 Many-to-One Archiving: On Shared File System



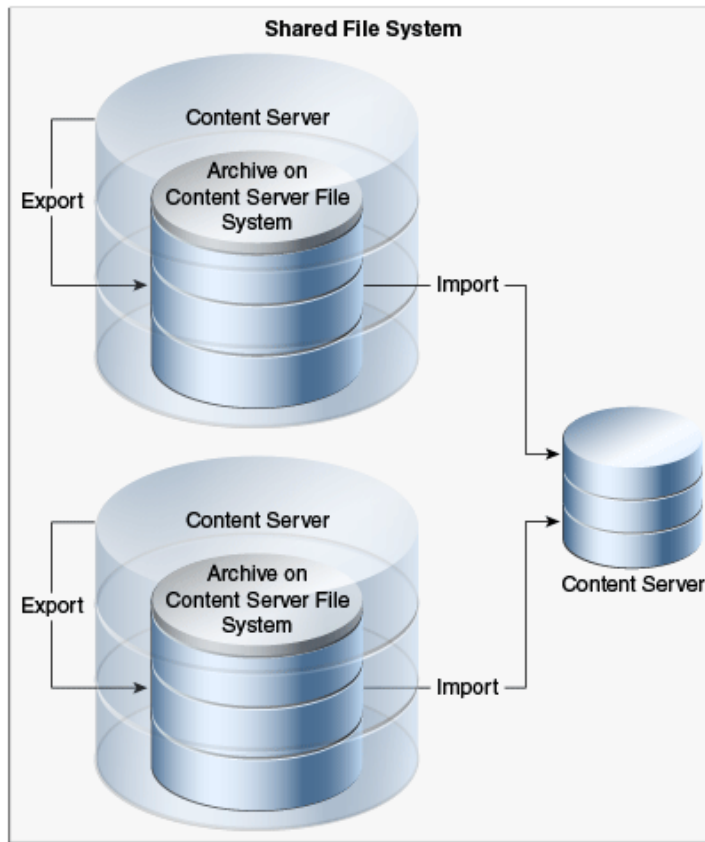
- Export to and import from a collection on a shared external file system.

Figure 31-19 Many-to-One Archiving: On Shared External File System



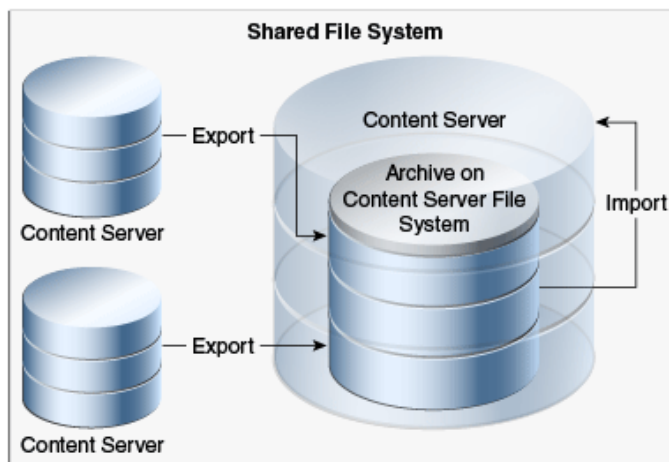
- Export to the source Content Server instances' collections and import directly from those collections on a shared file system.

Figure 31-20 Many-to-One Archiving: Export to Collections and Import from Collections on Shared File System



- Export from the source Content Server instances directly to a collection on the target Content Server instance and import from that collection on a shared file system.

Figure 31-21 Many-to-One Archiving: Export From Sources to Collection and Import from Collection on Shared File System



31.7 Archiver Examples

This section provides examples that illustrate how to use Archiver to solve common business problems.

- [Copying a Content Server Instance to a Laptop](#)
- [Transferring by Content Type and Author](#)
- [Changing Metadata Fields](#)
- [Adding Content ID Prefixes](#)
- [Changing Release Dates](#)

31.7.1 Copying a Content Server Instance to a Laptop

In this example, you want to set up a laptop computer with a copy of a Content Server instance for a colleague who will be traveling.

This procedure assumes that the source Content Server instance and the laptop computer have access to the same file system, and that the laptop computer has Content Server software installed.

1. Open Archiver on the source Content Server instance.
2. Create a new archive.
3. Because you want to export all content, you do not need to create an export query.
4. To limit the file size of the archive, choose the **Latest Revisions** option on the Edit Export Query page.
5. If content types and user attributes need to be copied to the laptop system, select **Content Configuration** and **User Configuration** on the Export Data tab.
6. Set export options from the General tab:
 - To save space on the local system, select **Replace Existing Export Files**.
 - If your colleague needs web-viewable files, select **Copy Web Content**.
7. Initiate the export manually.
8. Open Archiver on the laptop Content Server instance.
9. Open the source collection and select the archive to import.
10. If content type and user attributes were exported, select these options on the Import Archive page.
11. Initiate the import manually.

31.7.2 Transferring by Content Type and Author

In this example, you have a contribution Content Server instance where users submit content. You want to automatically archive *HR* content that is contributed by *JChang* to a Content Server instance in another building that serves as a Human Resources portal.

This procedure assumes that the two Content Server instances do not have access to a shared file system, and that the Human Resources portal server should contain only the latest revision of each content item.

31.7.2.1 Setting up an Automated Export

To set up an automated export on the Contribution Content Server instance:

1. Create an archive.
2. Set these export queries for the archive:

Field	Operator	Value
Content Type	Is	HR
Author	Is	JChang

3. In the Edit Export Query page:
 - Select **Export Revisions with Release Date later than most recent Export Date**.
 - Select the **Latest Revisions** option.
4. Set export options from the General tab:
 - To save space on the local system, select **Replace Existing Export Files**.
 - To include web-viewable files in the archive, select **Copy Web Content**.
5. Export the archive manually.
6. In the Replication tab, register the archive as an automated exporter.

31.7.2.2 Setting up an Automated Import

To set up an automated import on the HR Portal Content Server instance:

1. Create a target archive.
2. Select the target archive and ensure that the **Update** Override Action is set on the General tab.
3. Import the target archive manually.
4. In the Replication tab, register the archive as an automated importer.

31.7.2.3 Setting up an Automated Pull Transfer

To set up an automated pull transfer from the Contribution server to the HR Portal server:

1. In the Contribution Content Server instance, create an outgoing provider to the HR portal Content Server instance.
2. Open **Archiver** on the HR portal Content Server instance.
3. Open the target collection and make the target archive 'targetable.'
4. Open the source collection and select the source archive.
5. In the Transfer To tab, select the target archive as the target destination.
6. Run a manual transfer.
7. Set the transfer to be automated.

31.7.3 Changing Metadata Fields

In this example, you have a custom metadata field, *ApprovedBy*, which was used in one Content Server instance, but the field name must be changed to *Sponsor* for consistency with other Content Server instances.

1. Create the new *Sponsor* metadata field.
2. Create an archive.
3. Manually export all content to the archive. (You do not need to create an export query.)
4. Set up the following import field map for the archive:

Export Field	Target Field
xApprovedBy	Sponsor

5. From the General tab, select **Update** as the Override Action.
6. Initiate the import manually.
7. Delete the *ApprovedBy* field from the Content Server instance.

31.7.4 Adding Content ID Prefixes

In this example, you have two Content Server instances that are used as contribution servers, but you want to have all content available for consumption from both servers. You can set up an automatic transfer in both directions. However, both Content Server instances use automatic Content ID generation with similar numbering schemes, which could result in errors or overwritten revisions if you import files with Content IDs that already exist on the target Content Server instance.

- One way to avoid conflicts is to add a unique prefix in the Auto Number Prefix system property on both Content Server instances.
- Another way to accomplish this is to add a unique prefix during the import process:

To add content ID prefixes:

1. Set up the following value map on the first Content Server instance's import archive:

Input Value	Field	Output Value
All check box	Content ID	server2_<\$dDocName\$>

2. Set up the following value map on the second Content Server instance's import archive:

Input Value	Field	Output Value
All check box	Content ID	server1_<\$dDocName\$>

31.7.5 Changing Release Dates

In this example, you are copying archives to other Content Server instances using replication or transfer, but you want the release date on the target Content Server instance to be the date the content item was copied.

1. Set up an export and import for replication or transfer.

2. Select the archive to import in the target Content Server instance.
3. Set up the following import value map for the archive:

Input Value	Field	Output Value
All check box	Release Date	<\$dateCurrent()\$>

The release dates will reflect the local date and time of the target Content Server instance.

31.8 Configuration Migration Tips

There are several points to keep in mind when using the Configuration Migration utility.

- If you use directory locations on the target system that differ from the standard Content Server installation directories, you cannot use Configuration Migration but must do a manual copy of the pertinent directories.

For example, if you use partitioned file systems and want to split Content Server storage on the partitions, you must add configuration variables to the `DomainHome/ucm/cs/bin/intradoc.cfg` file to point to the correct locations for the directories that are stored elsewhere.
- If you are using different web servers for the source and the target systems, make sure to exclude the web server information when using Configuration Migration to prepare an export.
- Not all components can be exported using the Configuration Migration utility. For example, components that require an interactive installation cannot be exported. They must be installed separately on the target system.
- Dynamic Converter rules are not transferred with the Configuration Migration utility. They must be manually added to the target system by copying the `/data/conversion/cvtemplates.hda` file from the source system to the target system. In addition, you should create an archive for dynamic converter templates and transfer them to the target system before transferring other content. Otherwise an error occurs when a document that is eligible for dynamic conversion is imported.
- The Configuration Migration utility is particularly useful for propagating a part of an instance to another. For example, some customization, such as workflows or content profiles, may best be designed and tested on a development instance. After they are tested they can be migrated to your production system. Other development work, such as component development, is probably best done using the Component Wizard and Component Manager for testing and deployment.
- Problems can occur when importing archives if required fields and validated option lists are not considered. If metadata fields have been changed to be required or if option lists have been altered between one migration and another, it will be difficult to import content into another system with those same metadata field definitions. To avoid this problem, temporarily change required fields to be non-required and change option lists to be non-validated before importing data on a target system.
- You can use the Configuration Migration utility with the archiver to create a regular 'snapshot' of your instance. You should also make sure to make appropriate backups of your databases at the same time, to ensure that the entire system stays synchronized.
- You should create a configuration migration package before creating an archive package to ensure that the appropriate metadata information is available on the importing Content Server instance.

- Remember that migration is an additive process. The exporting configuration bundle of metadata information is added to the metadata that currently exists in the importing Content Server instance. If metadata information currently exists that matches the metadata being imported, and if the Force Overwrite rule has been selected during import, then the metadata on the importing Content Server instance is overwritten by the metadata from the exported bundle.

Using Archiver Replication Exceptions

This chapter explains how to use the Archiver Replication Exceptions feature to prevent failed Archiver imports from stopping replication in a Content Server instance.

This chapter covers the following topics:

- [Understanding Archiver Replication Exceptions](#)
- [Administering and Using Archiver Replication Exceptions](#)

32.1 Understanding Archiver Replication Exceptions

Archiver Replication Exceptions enables administrators to prevent failed imports from stopping replication. It does this by capturing such failed imports and putting them into an exceptions archive and sending email to the administrator that such a failed import has occurred.

The ArchiverReplicationExceptions component is installed and enabled by default with the Content Server instance.

- [How Archiver Replication Exceptions Works](#)
- [Scenario 1](#)
- [Scenario 2](#)

32.1.1 How Archiver Replication Exceptions Works

Several configuration entries must be manually added to the `IntradocDir/config/config.cfg` file to support Archiver Replication Exceptions. The configuration entries define a variety of conditions to determine the level of error reporting, to direct failed imports to an exceptions directory, and to ignore and handle multiple failed imports when a systemic error is detected. Parameters for both automatic and manual imports are provided.

32.1.2 Scenario 1

In this scenario an import of a document has failed because the content type "DOC" does not exist in the importing server. The error reporting level (ArchiverEmailErrorLevel) was set to collision, standard, severe, and the ArchiverErrorNotifyUser was set to sysadmin. The following is an example of an archiver import failure email notification:

```
Archiver Import Failure
There was a serious error during the import of a document which may prevent that
document from being properly synchronized in state with the exporting content
server. Content item 'test1' was not successfully checked in. The content
type 'DOC' is not defined in the system.
Revision Being Imported
Collection: idc
Archive Name: ar1
Source Instance: idc
Batch Name: 07-sep-24_15.15.41_766/07267151541~1.hda
Content ID: test1
Title: test1
Author: sysadmin
```


Revision: 1
Release Date: 9/24/07 3:13 PM
Create Date: 9/24/07 3:14 PM

The Document Has Been Copied To An Exceptions Archive

Collection: idc
Archive Name: ImportExceptions
Batch Name: 07-sep-24_15.15.41_766/07267151541~1.hda
Total Captured In Archive: 1

32.1.3 Scenario 2

In this scenario an import is being attempted but continually fails. The system administrator is aware that there may be problems during the import, but does not want an email notification of every failure. By setting `ArchiverMaxConsecutiveImportErrors` (default is 10), the system administrator can set several failures that can occur before the cessation of email notification. E-mail is sent until this number of errors is reached. If any import from the exporter should succeed before the set number is reached, or if the Content Server instance is restarted, the counter is reset to 0. Note that when the maximum number of errors is reached the automated import of the archive is aborted.

32.2 Administering and Using Archiver Replication Exceptions

The primary purpose for the Archiver Replication Exceptions feature is to allow filtering of failed Archiver imports to optimize the handling and notification of such failures. For content items to be processed by Archiver Replication Exceptions, the administrator must manually set configuration entries in the `IntradocDir/config/config.cfg` file. The configuration variables customize the behavior of the importing Content Server instance to allow for certain situations and to distribute the error reporting based on the configured criteria.

The following configuration variables can be used to customize behavior. These values should be set in the `IntradocDir/config/config.cfg` file under `#Additional Variables`.

By prepending any of the configuration entries with the name of an archive, with a colon (:) as a separator, that configuration entry will only apply to that archive. For example, to enable capturing exceptions for the archive `MyRemoteImportArchive`, use the following entry in the `config.cfg` file:

```
MyRemoteImportArchive:IsArchiverCapturingExceptions=true
```

If an archive name prefix is not applied, then the value set is the global default for all archives.

- **IsArchiverCapturingExceptions:** The primary functionality of this component is not enabled unless this configuration entry is turned on.
The default value is `false`.
- **ArchiverImportExceptionsArchiveName:** The name of the archive to hold failed imports. The archive will be created in the same archive collection as the archive that contained the document that failed an import.
The default value is `ImportExceptions`.
- **ArchiverMaxConsecutiveImportErrors:** The maximum number of consecutive import errors before the import of the archive is aborted.
The default value is 10.

- **ArchiverErrorNotifyUser:** The user to notify when there is an import failure. The default is `sysadmin`. The email is generated only if the import error is at a level that is configured to generate email.

The entry can be a comma separated list of user names, but all the user names have to be defined in the Content Server instance and have associated email addresses.

- **ArchiverEmailErrorLevels:** The error levels at which an import error should generate email during automated import. The possible levels are as follows:
 - **collision:** The import failed because an existing revision of a document blocked it. Usually this is caused by the importing revision having a release date (or create date depending on configuration) that is earlier than the date of the latest revision of an existing document.
 - **standard:** The import failed because of a normal error. A typical such error would be a metadata field that has an invalid value.
 - **severe:** The import failed because of a severe unexpected error in the Content Server instance. A typical reason for this might be a network failure to either the file system or database.

The configuration entry is set to a comma separated list of any of the above values. If an automated import error occurs, it is classified in one of the above levels and if the level is in the list configured for this parameter then an email is generated for that error.

The default value is `collision,standard,severe` (or all).

- **ArchiverManuallImportEmailErrorLevels:** This is similar to `ArchiverEmailErrorLevels` except it applies to manual archive imports. A manual import is one directly driven by an end user or administrator and is not part of an import done by a "registered automated importer".
The default value is empty (or `none`).
- **ArchiverCaptureExceptionErrorLevels:** A list of error levels for which an import error should capture a copy of the document and put it into the exceptions archive (see `ArchiverImportExceptionsArchiveName`). If the document is captured then the error will not stop an automated import. The automated import will delete the document from the archive when the batch file containing the document has been fully imported. See `ArchiverEmailErrorLevels` for a list of error levels and how to configure the entry.
The default value is `collision,standard`.
- **ArchiverManuallImportCaptureExceptionErrorLevels:** This is similar to the `ArchiverCaptureExceptionErrorLevels` parameter except it applies to manual archive imports (see `ArchiverManuallImportEmailErrorLevels` for more on manual imports). If an import error is captured it is copied into the exceptions archive but it does not delete it from the originating archive. If the error is captured it will not count against the maximum number of errors allowed during a manual import (see the standard Content Server configuration entry `MaxArchiveErrorsAllowed` which defaults to 50).
The default value is empty (or `none`).

- **ArchiveExceptionsMaxNumberDocuments:** The maximum number of documents that can be stored in the exceptions archive.

When this number is reached, then import failure will again prevent continued automated import. However, email is sent to `ArchiverErrorNotifyUser` indicating that the import failed and that the exceptions archive is full. Unlike the other configuration entries, if you use an archive prefix (separated by a colon) to limit the configuration entry to a particular archive, the archive name must be the name of the exceptions archive not the archive with the originating documents being imported.

The default value is 50.

The parameter `ArchiverMaxConsecutiveImportErrors` addresses the issue of skipping over errors and sending email notifications on the errors when the error is caused by a systemic problem (such as all documents having the same wrong metadata field on export). This results in numerous documents being unnecessarily captured and generating the attendant volume of unwanted email. This configuration entry helps detect such scenarios. During an automated import, if too many consecutive import errors are detected, then the current archive import is aborted. Manual imports follow the standard rules for maximum errors (see `MaxarchiveErrorsAllowed`). If any import (from any archive) is successful, then the consecutive import failure count is reset to 0.

If the same document fails an import (twice or more) sequentially email is sent out only for the first failure. If the same document fails an import but is from a different batch load file, the email for it is not suppressed if email for that document has already been sent for a previous error.

Part VII

Appendixes

This part provides information on how to integrate and manage several optional software components for Oracle WebCenter Content.

This section contains the following appendixes:

- [Managing Oracle Fusion Middleware BPEL Component for Content Server](#)
- [Managing the Need to Know Component](#)
- [Troubleshooting Oracle WebCenter Content](#)

A

Managing Oracle Fusion Middleware BPEL Component for Content Server

This appendix describes how to install and configure the BpelIntegration component for Oracle WebCenter Content, and how to configure Oracle WebCenter Content Server workflows to initiate deployed processes on the Business Process Execution Language (BPEL) server. This appendix covers the following topics:

- [Introduction](#)
- [Installation](#)
- [Configuring the Integration Component](#)
- [Configuring a Workflow in Content Server](#)

A.1 Introduction

The BpelIntegration component adds the ability to interact with Business Process Execution Language (BPEL) Process Manager from within Content Server workflows. As an administrator, you can configure Content Server workflows to initiate a deployed process on the BPEL server.

The following topics are covered in this section:

- [Hardware Requirements](#)
- [Software Requirements](#)
- [Software Distribution](#)

A.1.1 Hardware Requirements

At a minimum, the BpelIntegration component has the same hardware requirements as for Content Server and Oracle BPEL Process Manager.

A.1.2 Software Requirements

This section specifies requirements for Content Server and BPEL Process Manager.

Oracle Content Server: Content Server release 14c or higher must be properly installed and running on the target computer.

Oracle BPEL Process Manager: Oracle Service-Oriented Architecture (SOA) Suite release 14c or higher must be properly installed and running on the target computer.

A.1.3 Software Distribution

The BpelIntegration component is shipped with WebCenter Content release 14c.

A.2 Installation

These instructions assume that you have already installed the release version of Oracle SOA Suite.

This section covers the following steps:

- [Integration Instructions](#)
- [Enabling the Integration Component](#)

A.2.1 Integration Instructions

There are currently two ways to set up a content server to enable integration with Oracle SOA Suite:

- [Scenario One](#) involves installing WebCenter Content in a domain that has been extended by Oracle SOA Suite. This involves installing all parts into one domain in a particular order. The Oracle SOA Suite libraries are available to all and the class path is augmented to contain the Oracle SOA Suite libraries.
- [Scenario Two](#) involves manually copying the required libraries used by Oracle SOA Suite and augmenting the class path used to launch WebCenter Content inside of Oracle WebLogic Server.

The difference between the two scenarios is that the installation of Oracle SOA Suite augments the class path for you, while in Scenario Two this is a manual step. In the future, WebCenter Content will ship with the appropriate Oracle SOA Suite libraries.

A.2.1.1 Scenario One

Scenario One involves installing WebCenter Content in a domain that has been extended by Oracle SOA Suite.

To install WebCenter Content in a domain that has been extended by Oracle SOA Suite:

1. Create a new domain for Oracle SOA Suite.
2. Extend the Oracle SOA Suite domain by Oracle Business Activity Monitoring (BAM) and Oracle Enterprise Management (EM).
3. Extend the Oracle SOA Suite by WebCenter Content.

You may want to check that the `setDomainEnv` variable has been populated with Oracle SOA Suite-specific libraries. In particular, check that `soa-infra-mgmt.jar` is mentioned in the class path.

A.2.1.2 Scenario Two

Scenario Two involves manually copying the required libraries used by Oracle SOA Suite.

To update a WebCenter Content domain that has not been extended by Oracle SOA Suite:

1. Copy the `/soa` directory from the Oracle home for Oracle SOA Suite to the Oracle home for WebCenter Content.

Locate the Oracle SOA Suite 14c home directory for the Oracle SOA Suite server you are connecting to through WebCenter Content. There should be a directory called `soa`. Copy

this directory to the WebCenter Content home directory and leave it in the top directory, that is, copy `SOA_ORACLE_HOME/soa` to `WC_CONTENT_ORACLE_HOME/soa`.

2. Augment the class path for the WebCenter Content domain by editing the `setDomanEnv.cmd` or `setDomainEnv.sh` file, depending on your operating system.

```
set POST_CLASSPATH=%ORACLE_HOME%\soa\soa\modules\oracle.soa.mgmt_11.1.1\soa-infra-
mgmt.jar;%POST_CLASSPATH%
```

A.2.1.3 Final Steps

The final step for both scenarios is enabling the `BpelIntegration` component and starting the servers.

If your Oracle SOA Suite instance is running in a separate server than WebCenter Content, you may see the following security error:

```
vax.xml.ws.WebServiceException: java.lang.SecurityException: [Security:090398]Invalid
Subject: principals=[weblogic, Administrators]
    at com.sun.xml.ws.client.dispatch.DispatchImpl.doInvoke(DispatchImpl.java:209)
    at com.sun.xml.ws.client.dispatch.DispatchImpl.invoke(DispatchImpl.java:216)
```

If you encounter this error, you need to enable cross-domain security for both servers. Follow these instructions:

```
User will need to setup Trusted Domain on both WLS domain.
Goto WLS Console->Respected Domainsoainfra or bam ->Security
1. Make sure "Cross Domain Security Enabled"
2. Click on Save
3. Expand Advanced part of setting
4. Make sure you supplement the Credential and Confirm Credential fields.
5. Click on Save
Repeat for the same for the other WLS domain.
Finally, Restart both WLS Servers.
```

A.2.2 Enabling the Integration Component

To enable the integration component:

1. Log in to the Content Server instance as a system administrator.
2. Choose **Administration**, then **Admin Server**, then **Component Manager**.
3. In the paragraph at the top of the page, click the **Advanced Component Manager** link.
4. Notice that there are two lists of Enabled and Disabled Components. Select **BpelIntegration** in the lower Disabled Components list.
5. Click **Enable** to move the item from the lower list to the upper.
6. At the bottom of the page, click **Update**.
7. Log in to the Oracle WebLogic Server Administration Console.
8. On the left-hand side of the console, click **Domain Structure**, then **Environment**, then **Servers**. The Summary of Servers page is displayed.
9. From the **Control** tab, select your server, then click **Restart SSL**.

A.3 Configuring the Integration Component

The following topics are covered in this section:

- [Architecture](#)
- [Process Configurations](#)

A.3.1 Architecture

The integration uses BPEL client libraries to communicate with Oracle BPEL Process Manager. A process configuration is required to identify connection parameters, a BPEL process, and a BPEL operation. Additionally, a process configuration identifies document metadata fields and literal values assigned to the parameters passed to the BPEL operation.

A.3.1.1 Connection Configuration

Process configurations reside within files located in the `data/orabpel` directory. You may edit these files manually. However, there are some pages provided with the BpelIntegration component to make this job easier. The first page is a Connection Configurations page. From the Connection Configurations page you can view the defined connection configurations and add or delete connection configurations.

Figure A-1 Connections Configurations Page

Connections Configurations		
		▼ Connection Menu
1 Configurations		
Configuration ID	Description	Actions
nareshSOA		

Access the Connection Configurations page from **Administration > Oracle BPEL Administration > Connection Configurations**.

This page contains a Connection menu at top right that is used to add a new connection. Each connection has an **Actions** menu that provides the following choices.

Element	Description
Configuration Information	Allows you to view a connection configuration in more detail.
Test Configuration	Allows you to test the JNDI Properties of the connection configuration.
Delete Configuration	Allows you to delete a connection configuration.

A.3.1.1.1 Adding a Connection Configuration

To add a connection configuration, choose **Add Connection** from the **Connection** menu at the top right of the Connections Configurations page. The Add Configuration page opens.

The fields on this page are defined in the following table.

Element	Description
Configuration ID	Used to identify the connection configuration. Must be unique.

Element	Description
Description	Used to provide a description of the connection configuration.
Domain	The BPEL process domain identifier.
Initial Context Factory	The initial context factory to use to connect to the BPEL process manager. The value should be the fully qualified class name of the factory class that creates an initial context (for example, <code>com.evermind.server.ApplicationClientInitialContextFactory</code> for connecting to an Oracle Application Server running BPEL).
Provider URL	The location of the BPEL process manager. The value should contain a URL string (for example, <code>t3://servername:7003/soa-infra</code> for connecting to an Oracle Application Server running BPEL).
Security Principal	The identity of the principal for authenticating the caller to the BPEL process manager. The value should contain a user identifier for a user registered on the BPEL process manager.
Security Credentials	The credentials of the principal for authenticating the caller to the BPEL process manager. The value should contain a password for the user identifier entered as the security principal.
Confirm Security Credentials	Used to confirm the security credentials password.
CSF Key	Used to manage credentials securely.

A.3.1.1.2 Connection Configuration Information

To view detailed information about a specific connection configuration, choose **Configuration Information** from the **Actions** menu for the specific adapter in the configuration page. The Configuration Information page opens.

The following actions are available from the **Actions** menu at the top of the page.

Element	Description
Update Connection	Allows you to edit the connection configuration.
Delete Connection	Allows you to delete the connection configuration.
Test Connection	Allows you to test the JNDI Properties of the connection configuration.

A.3.2 Process Configurations

After the connections have been configured, processes can be defined and configured on the Process Configurations page. Use the **Actions** menu to change a process configuration.



Note:

Oracle WebCenter Content only supports a single namespace in SOAP request for WebCenter Content integration with BPEL process.

Figure A-2 Process Configurations Page

Process Configurations					
					Process Menu
2 Configurations					
Configuration ID	Description	Profile	Direct to SOA	Is Web	Actions
testDocRouting		Test	true	true	
HelloWorld		Test	true	true	

Access the Process Configurations page from **Administration > Oracle BPEL Administration > Process Configurations**.

Element	Description
Add Process	Allows you to add an additional process configuration.
Configuration Information	Opens the Configuration Information page for the process configuration.
Update Process	Enables you to edit the BPEL process and operation.
Update Payload	Enables you to edit the mappings from content item fields to payload properties.
Delete Configuration	Enables you to delete the process configuration.
Test Connection	Allows you to test the JNDI Properties of the connection configuration.

After you create a process configuration, you must define process properties and payload mappings. For information on how to edit process properties, see [Process Properties](#). For information on how to edit fields mappings, see [Payload Mappings](#).

A.3.2.1 Process Properties

Process properties identify the BPEL process and the BPEL operation used to initiate a new process. These properties can be edited on the Update Process page.

Figure A-3 Update Process Page

To edit process properties, choose **Update Process...** from the **Actions** menu.

Element	Description
Configuration ID	Used to identify the connection configuration. It is unique.
Description	Used to provide a description of the connection configuration.
Connection ID	Used to identify the connection.
BPEL Process	The process identifier of a deployed, active BPEL process. Each active process is listed with the Process Name and Process Revision. The default revision for each process is identified with an asterisk (*).
BPEL Service	The service identifier of a deployed, active BPEL service.
BPEL Operation	The name of an operation to initiate a process.
Profile	The name of the profile to which a document is checked-in.
Direct to SOA	Auto invokes the SOA process whenever a new document is checked-in with the selected profile.
Is Web	Invokes the SOA process using JAX/WS protocol.

A.3.2.2 Payload Mappings

Payload mappings define how Content Server fields and literal values are mapped to payload properties to initiate a process.

To edit payload mappings, click **Update Payload** from the **Actions** menu.

The Update Payload Mapping page displays a form with three columns. Each of the columns is defined in the following table.

Element	Description
Field	The name of the payload element to which values are mapped.
Type	The type of payload element. This is used to filter the options displayed in the value option list. Complex types contain other types. If the type is an array of elements, then the value mapping may be a comma-separated list that is parsed by the component.

Element	Description
Mapping	<p>Used to identify the name of a Content Server field. These fields are the standard Content Item fields (dID, dDocName, dDocTitle, and so on), custom information fields, and some special system fields. The possible special fields are:</p> <ul style="list-style-type: none"> • HttpAbsoluteCgiPath: The absolute CGI path to the Content Server. • HttpAbsoluteWebRoot: The absolute path to the Content Server web root. • idcReference: Creates a string with a value of "socket:<HttpServerAddress>:<HttpServerPort>" • DocUrl: The computed URL to the web viewable file. • ContentViewLink: The computed URL to a content view page, showing a view of the content and links to content information. • @Literal: Allows you to assign a literal value. When this option is chosen, an additional text entry field is displayed to provide the value. You can enter array values using comma-separated notation. • FormatValue: A special mapping function named Format Value is also provided, allowing mapping of any value. The format is custom concatenation of constant values as well as values from other mapping functions. The Format Value mapping function can be mapped to any payload element. However, the Format Values return type is technically a string, and care must be taken to ensure that the return value is a valid string representation of the payload schema type. • WCC Viewer URL: The URL to the WCC ADFUI Viewer link that shows the document.

Figure A-4 shows an example of field mappings.

Figure A-4 Payload Mapping Page - Field Mappings Example

Configuration ID: HelloWorld
 BPEL Process: HelloWorldComposite
 BPEL Service: client
 BPEL Operation: process
 Profile: Test
 Direct to SOA
 Is Web

Field	Type	Mapping
- Part: BPELProcess1ProcessRequest	Complex	
input	string	Title

Update Reset

On this page, the following mapping is established:

- The **input** payload field is assigned the value of the content's Title.

A.3.2.2.1 Support Content Function

The Supporting Content function maps supporting content data associated with a document to a workflow process payload element. Supporting content can be mapped to any complex node within the process payload. When the supporting content function is mapped, a supporting

content key and XPath parameter are both required. The supporting content key is used to associate the XML content with the document. The XPath expression identifies the node within the XML content to be mapped to the payload element. Complex Types in BPEL payload can have supporting content backing ensuring that .xml files can be read and values substituted from the xml file onto the payload. The Supporting Content Mapping value can be given as :Support:NAME_OF_RENDITION:XPATH_NAME / SystemSupport:NAME_OF_RENDITION:XPATH_NAME (When supporting content is a system rendition).

A.3.2.3 Preparing BPEL Composites for WebCenter Content Integration

The WebCenter Content integration with BPEL requires that the BPEL composite has a `binding.adf` entry in its service. This binding allows WebCenter Content to invoke the BPEL as a service and allows it to set the conversation ID to later query Oracle SOA Suite for status.

Consequently, when creating a BPEL composite and making it available to WebCenter Content, the following must be done:

1. Open the composite in JDeveloper.
2. Open the `composite.xml` file in source mode.
3. Find the service and the callback definitions.
4. Add the following line to the service and the callback definitions. In the following line, the `serviceName` is something meaningful of your choice. Ensure that the `registryName` is empty.

```
<binding.adf serviceName="YourUniqueServiceName" registryName="" />
```

5. In addition to the asynchronous process, create a new process for asynchronous callback in the Oracle BPEL configuration listing.
6. Change the exit condition to:

```
wfGet("conversationId")
```

and

```
obIsInstanceClosed("YourUniqueAsyncProcessCallback", wfGet("conversationId"))
```

A possible composite example is as follows:

```
<service name="receive" ui:wSDLLocation="receive.wsdl">
<interface.wsdl interface="http://example.com/sca/soapservice/aug11_app_2/
myThirdComposite/receive#wsdl.interface(execute_ptt)"/>
  <binding.ws port="http://example.com/sca/soapservice/aug11_app_2/myThirdComposite/
receive#wsdl.endpoint(receive/execute_pt)"/>
  <binding.adf serviceName="my3rdBPELService" registryName="" />
</service>
```

This can also be done using JDeveloper widgets, but they require a non-empty `registryName`. The `registryName` for a composite without ADF is empty and the composite examples given here need the registry name to be empty. If they are not empty, API calls do not work properly after invoking the composite using the standard Oracle SOA Suite.

A.3.3 Process Faults

After you have defined and configured the processes, view and verify the failed processes on the Process Faults page. Use the **Actions** menu to view the failed processes.

Figure A-5 Process Faults Page

The screenshot shows the 'Process Faults' page. At the top, there is a search form with fields for 'Start Date:', 'End Date:', 'Document Id:', and 'Process Id:', each with a calendar icon. A 'Submit' button is located below the form. Below the form, a table displays 15 faults. The table has five columns: 'Doc Id', 'Process', 'Date', 'Message', and 'Actions'. Each row represents a fault with a unique Doc Id, a process name (either 'testDocRouting' or 'HelloWorld'), a timestamp, a message stating 'Unable to find the payload definition for:!', and an 'Actions' menu icon.

Doc Id	Process	Date	Message	Actions
2001	testDocRouting	8/25/16 9:19 PM	Unable to find the payload definition for:!	
2206	HelloWorld	8/29/16 10:13 PM	Unable to find the payload definition for:!	
2203	HelloWorld	8/28/16 11:25 PM	Unable to find the payload definition for:!	
2204	testDocRouting	8/28/16 11:26 PM	Unable to find the payload definition for:!	
2205	HelloWorld	8/28/16 11:37 PM	Unable to find the payload definition for:!	
2202	HelloWorld	8/28/16 11:23 PM	Unable to find the payload definition for:!	
2203	testDocRouting	8/28/16 11:25 PM	Unable to find the payload definition for:!	
2204	HelloWorld	8/28/16 11:28 PM	Unable to find the payload definition for:!	
2205	testDocRouting	8/28/16 11:37 PM	Unable to find the payload definition for:!	
1801	HelloWorld	8/29/16 6:57 PM	Unable to find the payload definition for:!	
2202	testDocRouting	8/29/16 6:57 PM	Unable to find the payload definition for:!	

Access the Process Faults page from **Administration > Oracle BPEL Administration > Process Faults**.

The Process Faults page displays a form with five columns. Each of the columns is defined in the following table.

Element	Description
Doc Id	The Id of the doc which failed to check-in.
Process	The name of the process.
Date	The date and time when the process failed.
Message	The message for the failure of the process.

Use the **Actions** menu to clear or repair the faults.

A.4 Configuring a Workflow in Content Server

The following topics are covered in this section:

- [Configuring a Workflow](#)
- [BPEL Process Information](#)
- [Troubleshooting Workflows](#)

A.4.1 Configuring a Workflow

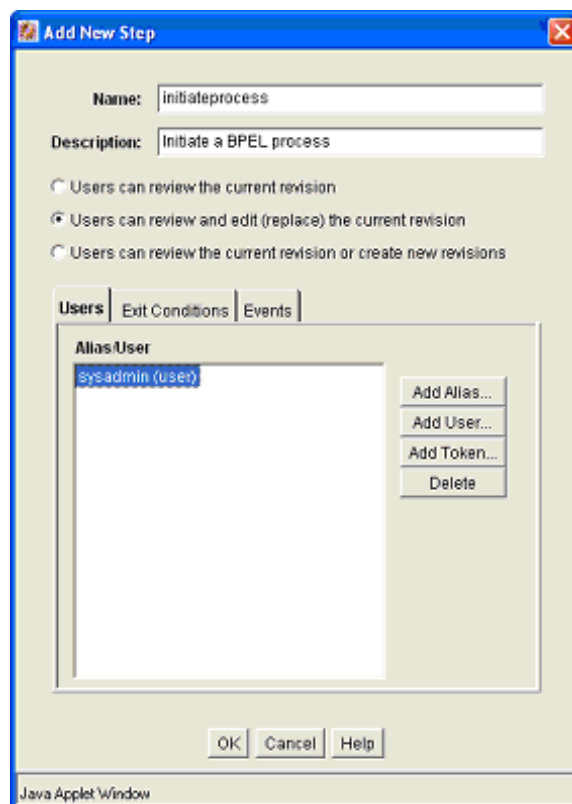
To integrate with BPEL process manager, you must first configure a Content Server workflow. There are many possible ways to configure a workflow. The following tasks configure the most basic type of workflow that integrates with BPEL process manager.

 **Note:**

Oracle WebCenter Content only supports a single namespace in SOAP request for WebCenter Content integration with BPEL process.

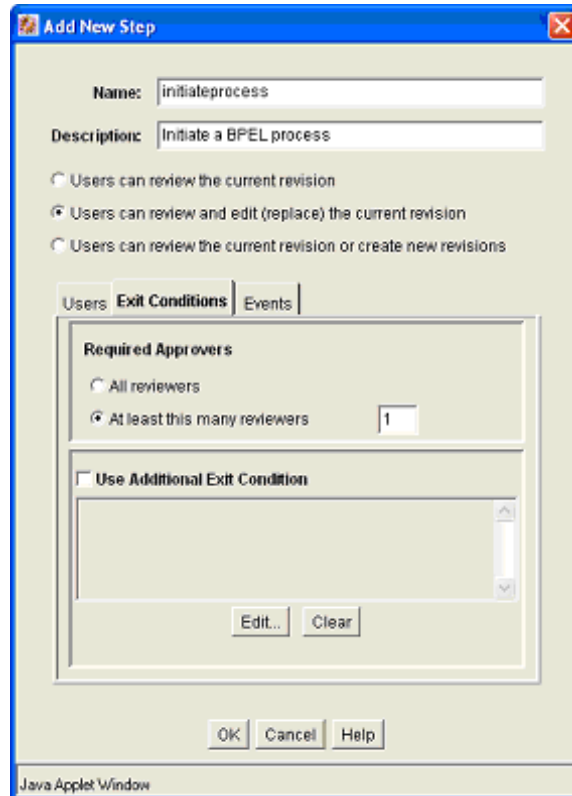
1. Start the Workflow Administration applet.
2. Add a new Criteria Workflow. For this example, the workflow name is `orabpeltest`.
3. Add a step to the workflow. For this example, use `initiateprocess` as the step name.
4. Add step users.

Figure A-6 Add New Step Dialog



5. Select the **Exit Conditions** tab and select at least one reviewer. (This is an arbitrary setting, but in this instance, it leaves the content item in this workflow step after a BPEL process is initiated.)

Figure A-7 Add New Step Dialog, Exit Conditions Tab



6. Add an exit condition by selecting the **Use Additional Exit Condition** check box and then clicking **Edit...**
7. In the Edit Additional Exit Condition dialog, check **Custom Condition Expression** and add the following script:

```
wfGet("conversationId") and  
obIsInstanceClosed("process_3", wfGet("conversationId"))
```


Figure A-8 Additional Exit Condition Dialog

Edit Additional Exit Condition

Additional Exit Condition

Field:

Operator:

Value:

Condition Clause

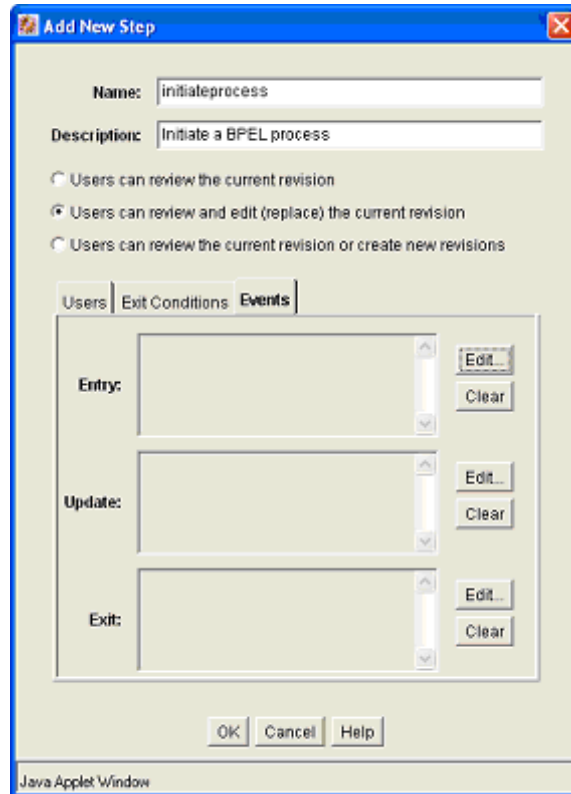
Custom Condition Expression

 **Note:**

Note that the Idoc Script function `obIsInstanceClosed` tests if the BPEL instance with the specified conversation ID is still open. The conversation ID is stored in the workflow companion data when the process is invoked.

8. On the **Events** tab, click **Edit...** for the Entry event.

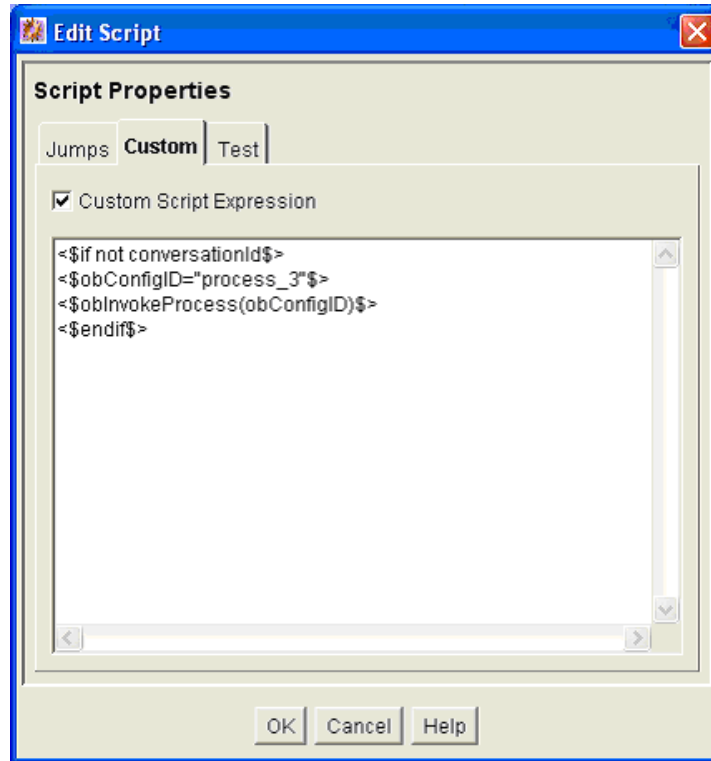
Figure A-9 Add New Step Dialog, Events Tab



9. In the Edit Script dialog, click the **Custom** tab.
10. Click the **Custom Script Expression** check box to enable the script window.
11. Type the following lines into the script window:

```
<$if not conversationId$>
<$obConfigID="process_3"$>
<$obInvokeProcess (obConfigID) $>
<$endif$>
```

Figure A-10 Edit Script Dialog



 **Note:**

The component defines Idoc Script functions that can be used to start and determine the state of an invoked process. The `obInvokeProcess` Idoc Script function takes the name of the process configuration ID as its one argument. Alternatively, you can use the `ORABPEL_INVOKE_BPEL` service. This service requires the `obConfigID` variable to be set to the name of a process configuration. The service reads the process configuration and uses it to determine how to connect to BPEL process manager.

12. Click **OK** to finish editing the script.
13. Click **OK** to finish editing the workflow step.
14. Enable the workflow.

A.4.2 BPEL Process Information

When a content item enters the workflow and initiates a BPEL process, an identifier is created and stored in the companion data file to identify the related BPEL process. This identifier is stored with the key "conversationId" and can be obtained from the companion data with custom Idoc Script in a workflow step event.

Idoc Script Functions

obInvokeProcess[obConfigID]: This function invokes the process as defined in the process configuration.

obIsInstanceClosed[obConfigID, conversationId]: This function returns true if the process as specified by the specified configuration with the given conversation ID has been closed. Closed includes completed and cancelled.

obIsInstanceOpen[obConfigID, conversationId]: This function returns true if the process as specified in the specified configuration and the given conversation ID is open.

obRetrieveStatus[obConfigID, conversationId]: This function returns true if it successfully retrieves information about the process. The data binder has information about the instance title, audit trail, trace and metadata as well as the process instance ID and revision tag.

A.4.3 Troubleshooting Workflows

To troubleshoot workflows in WebCenter Content that uses the BPELIntegration Component, you must first enable logging. To enable logging,

1. From the Administration menu in WebCenter Content, choose **System Audit Information**.
2. Enable the `requestaudit`, `idocsript`, and `bpelintegration trace` sections.
3. Select the **Verbose** and **Save** check boxes.
4. Click **Update**.

To view the system audit information, on the System Audit Information page click **View Server Output**. The output includes stack traces if there are errors in invoking the BPEL process from the WebCenter Content workflow.

B

Managing the Need to Know Component

This appendix provides information on how to install and configure the Need to Know (NTK or NtkDocDisclosure) component for Content Server. It also describes how to use the component to customize Content Server security areas including user access to content, search results, user credentials, behavior of metadata changes, and use of WHERE clause in searches. This appendix covers the following topics:

- [Introduction](#)
- [Installing the Need To Know Component](#)
- [Configuring the Need to Know Component](#)
- [Using the Need to Know Component](#)
- [Administration Interface](#)
- [Security Customization Samples](#)

B.1 Introduction

The Need to Know (NtkDocDisclosure or NTK) component supports customization for these Content Server security areas:

- **Content security:** Changing user access to content items.
- **Search results:** Modifying the display of search results.
- **Hit list roles:** Changing user credentials for query and check-in pages.
- **Content metadata security:** Altering the behavior of metadata changes for content items.
- **WHERE clause calculation:** Modifying use of the WHERE clause in searches.

For example, with standard security, users can only view content for which they have at least Read permission. The Need to Know component can change this in two ways:

- All users can be allowed to see content items from specified security groups in a search results list, even though they may not be able to view the metadata or document itself.
- Read and Write permission can be expanded or restricted within specified security groups using a query against content metadata and user attributes.

The Need to Know component provides a HTML administration interface to display security configuration status information, enable editing of security configuration values, and enable viewing and testing of Idoc Script for security configuration values.

B.1.1 Features

The Need to Know component is implemented through the following features:

- The Need to Know component is applied by security group. You must identify which security groups will use the component. All content in the specified security groups will appear in the search results for all users.

- The component provides the option of making all accounts visible, so a user can get a search *hit* on a content item regardless of its account.
- The **Security Group** list on the Search page will show all specified security groups. If accounts are enabled, all accounts will appear in the **Accounts** list on the Search page.
- A new **DocDisclosureQuery** metadata field and new *hit list* role must be created to support the Need to Know function. The hit list role is given read access to all specified security groups.
- You can create new user attribute fields or use existing ones in Need to Know queries.
- When a document is checked in, a query can be defined in the **DocDisclosureQuery** metadata field. The query conditions can include content metadata and user attributes, and the query results determine access permission to the document. Queries can be entered manually in Idoc Script, or the Disclosure Query Security applet can be used to build the query.
- Whenever a user does a search, the hit list role is dynamically applied to the user, giving them read access to all content in the specified security groups. Each content item is then checked for a query in the **DocDisclosureQuery** field, which determines the user's access to that content item.
- If the **DocDisclosureQuery** field is empty, standard security applies. Standard security can also be explicitly specified in the query field, or it can be used in a boolean combination with other document and user attributes to expand or refine the read access.
- If a query is entered for a content item that is not in a NTK security group, the query does not run, and standard security applies.
- If a user already has more than Write or higher access to the security group, the query in the **DocDisclosureQuery** field does not run, and standard security applies.
- A global query can be defined for all content, so individual queries do not have to be specified for each content item. You can set up the system to allow the global query to be overridden when a query is entered during check-in.

B.1.2 Applications

This component can be used as the starting point for a more complicated security implementation, such as:

- Providing integrated tracking for downloads of sensitive documents.
- Controlling Write or higher privileges through custom logic.
- Implementing view limits and subscription control, where documents within a certain security group may only be downloaded so many times.
- Controlling access by incorporating entries from a custom database table or results from a custom API. This is a hook for externally controlled authorization.

B.2 Installing the Need to Know Component

Install the component using either the Component Wizard or the command-line ComponentTool.

Topics

- [Installing the NTK component with Component Wizard](#)
- [Installing the NTK Component with Component Tool](#)

B.2.1 Installing the NTK Component with Component Wizard

This procedure describes how to install the Need to Know component using the Component Wizard.

1. Launch the Component Wizard. For information on using standalone applications, see [Running Administration Applications in Standalone Mode](#).
2. In the Component Wizard page, choose **Options**, then **Add**.
3. In the Add Component window, select the radio button for **Use Existing Component**.
4. Browse to the location where the WebCenter Content shiphome was installed and locate the Need to Know component directory. For example:

```
MW_HOME\WC_CONTENT_ORACLE_HOME\ucm\cs\idc\components\NeedToKnow
```

5. Select the `NeedToKnow.hda` file and click **OK**.
6. Click **Enable**.

The NTK component is enabled.

B.2.2 Installing the NTK component with ComponentTool

This procedure describes how to install the Need to Know component using the Component Tool.

Run the Component Tool and specify the `NeedToKnow.hda` file with the following path, using your configuration name and path for `WC_CONTENT_ORACLE_HOME`:

```
MW_HOME\WC_CONTENT_ORACLE_HOME\ucm\cs\idc\components\NeedToKnow\NeedToKnow.hda
```

B.3 Configuring the Need to Know Component

This section describes the procedure to set up a basic security configuration using the Need to Know component. This procedure explains how to set up security configuration variables, a custom metadata field, and a hit list role. After you have set up the basic configuration, you can use the Need to Know component interface to edit, test, and improve the security configuration.

1. On the Content Server portal, choose **Administration**, then **Admin Server**, then **General Configuration**.
2. On the General Configuration page, under the **Additional Configuration Variables** heading, scroll to the bottom of the text area, and add the following code:

```
SpecialAuthGroups=group1,group2,...
```

In the code:

- Replace `group1,group2,...` with the security groups that will use the Need to Know component.
- Security groups must be entered in lowercase letters.
- Any security groups not listed will have standard security applied.

 **Note:**

Other products such as Oracle WebCenter Content: Records also can use the `SpecialAuthGroups` configuration variable, so be careful to use unique names for security groups that use the Need to Know component.

3. If you want to specify content item-level queries, use the Configuration Manager to add a new metadata field. (This is not necessary if you will be using only the global query.) A new metadata field must be added by using the Configuration Manager; it cannot be added from the Need to Know component interface.
 - You can use any field name and title you wish, such as *DocDisclosureQuery* or *NeedToKnow*.
 - The field must be specified as a memo field.
 - After adding the field, click **Update Database Design**, then click **Rebuild Search Index**.

 **Note:**

If your Content Server instance already has a large amount of content, rebuilding the search index can take a long time (up to a couple of days). Consider rebuilding during system maintenance periods or at times of non-peak system usage.

4. Use the User Admin administration applet to add a hit list role.
 - You can use any role name you wish, such as *hitlist* or *NTKrole*.
 - Give Read access to all the security groups that were specified in the `SpecialAuthGroups` configuration entry.
 - If you want the security groups that were specified in the `SpecialAuthGroups` configuration entry to be listed on the check-in page or update page, you will need to give Write access to this role.
 - You can create two different hit list roles with different names and permissions. One role can be configured with the Need to Know component to be a Query role in a content search, and the other role can be configured with the Need to Know component to be an Update role in content check-ins and updates.
 - Do not assign this role to any users. If the hit list role is configured to be a Query or Update role, it is automatically added to the user's attributes.
5. If you want to set user access permissions that extend the limits of Need to Know security, use the General Configuration page to include extra security configuration settings in the Additional Configuration Variables section. Scroll to the bottom of the text area and enter the configuration settings as necessary.
6. If you want to add new user attribute fields for use in Need to Know queries, use the User Admin tool to add user attribute fields.
7. Restart the Content Server instance.

 **Note:**

When the Need to Know component has been installed, certain security configuration values are stored in the `IntradocDir/data/needtoknow/ntk_config.hda` file. These values can be edited by using the Need to Know administration interface, described in [Administration Interface](#) or by directly editing the `ntk_config.hda` file.

B.4 Using the Need to Know Component

This section covers the following topics:

- [Security Configuration Customization](#)
- [Disclosure Query Security Applet](#)
- [Query Syntax](#)
- [Defining a Content-Level Query](#)

B.4.1 Security Configuration Customization

The Need to Know component provides additional security configuration support focused on the following areas:

- [Content Security](#): Changing user access to content items.
- [Search Results](#): Changing the display of search results.
- [Hit List Roles](#): Changing user credentials for query and check-in pages.
- [WHERE Clause Calculation](#): Changing use of the WHERE clause in searches.
- [Content Metadata Security](#): Changing the behavior of metadata changes for content items.

B.4.1.1 Content Security

Standard security uses security roles, groups, and accounts to determine if a user has the appropriate privilege level to access a content item. The Need to Know component enables you to customize the process of determining user privilege. You can use the Need to Know component interface to set configuration fields and create Idoc Script to specify Read, Write, and Delete privilege levels. The Idoc Script also can contain user and content metadata values.

The Need to Know component computes content security uses the following process:

1. A user clicks a link to view content information.
2. If the user has the Admin role, standard security is used and the user can view the content.
3. If the security group of the content item is not a Need to Know authorization group, then standard security is used to evaluate the user's Read request.
4. If Need to Know security is not enabled at the Read privilege level, then standard security is used to evaluate the user's Read request.
5. If Need to Know security is not limited at the Read privilege level, and the user has standard security access to the content item, the user is given access to the content.
6. The Need to Know security Idoc Script (in this case the Read security script) is evaluated.

- The Need to Know access flag (in this case, `isNTKReadAccess`) is evaluated to determine if the user has access to the content. Access is allowed or denied based on the Need to Know access flag.

The Need to Know component also enables you to test security configuration scripts for each access level: Read, Write, and Delete. For a test you can specify a user and a content ID, and you have the option of specifying roles and accounts. These attributes are used in the test instead of the user's actual attributes. For example, you could test Idoc Script using an external user whose attributes may not be accessible. After the test is run, the component reports on whether the user has access to the content item, whether Need to Know security was used, and if Need to Know security was not used then the reason why.

For information on using the Need to Know component interface to configure content security, see the NTK Configuration Information page and the Content Security Configuration Information page. For samples of Idoc Script that can configure content security, see [Security Customization Samples](#).

The following Idoc Script functions can be used in the Script fields to determine content security. See Introduction to the Idoc Script Custom Scripting Language in *Developing with Oracle WebCenter Content*.

Idoc Script Function	Description
<code>allStrIntersect</code>	Takes two required comma-delimited strings and one optional Boolean flag as parameters. If all values in the second string occur in the first string, the function returns true. If the optional parameter is set to true and the second value is an empty string, the function returns true. By default, the optional parameter is false. The comparison of values in the comma-delimited strings are not case sensitive.
<code>includeNTKDeleteSecurityScript</code>	Evaluates the Delete security script and makes the <code>isNTKDeleteAccess</code> variable available for use in the Read or Write security scripts. If this function is used in the Delete security script, it is ignored.
<code>includeNTKReadSecurityScript</code>	Evaluates the Read security script and makes the <code>isNTKReadAccess</code> variable available for use in the Write or Delete security scripts. If this function is used in the Read security script, it is ignored.
<code>includeNTKWriteSecurityScript</code>	Evaluates the Write security script and makes the <code>isNTKWriteAccess</code> variable available for use in the Read or Delete security scripts. If this function is used in the Write security script, it is ignored.
<code>isDisclosureQuery</code>	Evaluates the query for the disclosure field (if specified) and returns true or false. An optional parameter can be specified to determine if the function should return true or false if the disclosure query is empty. If the disclosure field has not been specified or does not exist, this function always returns false.
<code>isMetaChange</code>	This variable is set if the content security call involves a content update or a check in.
<code>isStrIntersect</code>	Takes two required comma-delimited strings and one optional Boolean flag as parameters. If at least one value in the second string occurs in the first string, the function returns true. If the optional parameter is set to true and the second value is an empty string, the function returns true. By default, the optional parameter is false. The comparison of values in the comma-delimited strings are not case sensitive.

Idoc Script Function	Description
stdSecurityCheck	Checks standard security for the current access level. For example, if the function is in the Read security script, it checks security at the Read access level.

B.4.1.2 Search Results

The Need to Know component enables you to customize the presentation of the search results that are returned from a search query. Two configuration values can be set using the NTK interface: *Hidden Fields*, and *Script*.

The Hidden Fields value is a list of fields that can be hidden from view on the Search Results page. The values are set to empty strings. To hide the fields, the field `hideFields` must be set in the component search results Idoc Script.

Idoc Script controls the presentation of the search results. Idoc Script is evaluated for each row in the search results. A number of fields can be set in script to alter the presentation of search results. To see the list of fields and how to use the Need to Know component interface to customize script for search results presentation, see the Search Results Configuration Information page.

The Need to Know component uses the `securityCheck` Idoc Script function to determine search results presentation. The `securityCheck` function checks the security against the current content item (standard security or Need to Know security), depending on the configuration values. The function has an option parameter to determine what access level to check:

- 1 = Read
- 2 = Write
- 4 = Delete
- 8 = Admin

If no parameter is used with `securityCheck`, by default it checks the Read access level.

For examples of Idoc Script that can alter search results presentation, see [Security Customization Samples](#).

B.4.1.3 Hit List Roles

Hit list roles enable you to change user credentials for using content Search, Content Check In, and Update pages. Using the User Admin applet, you can add a hit list role with any name you wish. You do not assign the role to a user; when the role is enabled it is automatically added to a user's attributes when doing a search, check in, or update.

When creating a hit list role, you must give Read access to all the security groups that you specify in the `SpecialAuthGroups` configuration entry. If you want these security groups to be listed on the Content Check In page or Update page, you also need to add Write access to the hit list role.

Using the Need to Know component Hit List Roles Configuration Information page, you can implement hit list roles in two forms: *Query* and *Update*. A hit list role used in a query is applied to content searches. A hit list role used in an update is applied to content check-ins and updates.

For more information about how to use hit list roles, see the NTK Configuration Information page and the Hit List Roles Configuration Information page. For samples of using hit list roles, see [Security Customization Samples](#).

B.4.1.4 WHERE Clause Calculation

The Need to Know component provides two filters that enable you to customize the query WHERE clause that is used to retrieve search results:

- **preDetermineWhereClause:** Overrides the entire WHERE clause.
- **postDetermineWhereClause:** Appends to the standard security WHERE clause.

The code for these filters is located in the `NTKFilter` Java class. For samples of how these filters work, see [Security Customization Samples](#).

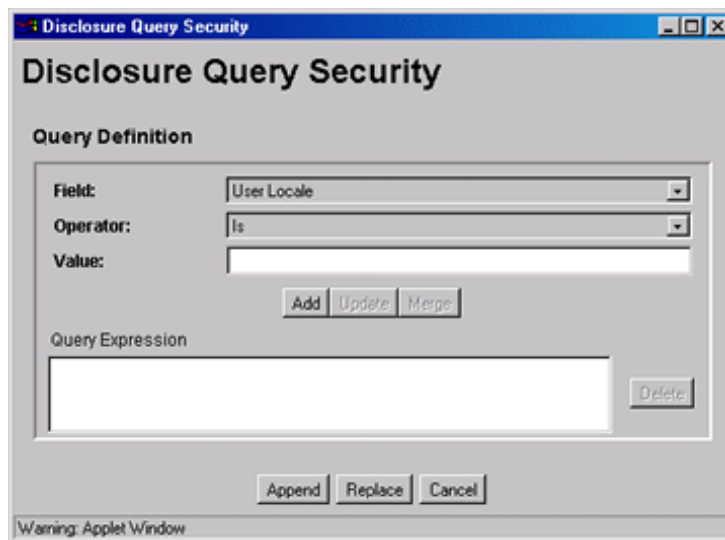
B.4.1.5 Content Metadata Security

The Need to Know component provides a filter called `checkMetaChangeSecurity` that enables you to alter the behavior of metadata changes when a content item is checked in or updated.

The code for this filter is located in the `NTKFilter` Java class. For an example of how the filter works, see [Security Customization Samples](#).

B.4.2 Disclosure Query Security Applet

The Disclosure Query Security applet is used to define a query for a particular content item during check-in.



To access the applet, click the **Update** button next to the **DocDisclosureQuery** field on the Content Check In Form page.

Element	Description
Field	Select a user attribute field to be specified in the query. This list includes User Locale, User Name, User Role, and all of your custom user attribute fields.
Operator	Select an operator to apply to the Field and Value. The following operators are used for all fields except User Role: Is: The value in the specified Field matches the specified Value. Is Not: The value in the specified Field does not match the specified Value. Begins With: The value in the specified Field starts with the specified Value. Contains: The value in the specified Field contains the specified Value. The User Role field has only one operator, Has Member, and displays a drop-down list of roles in the Value field.
Value	Enter the value to be specified in the query. <ul style="list-style-type: none"> If an option list was specified for the selected field, choose the value from the drop-down list. If no option list was specified for the selected field, type the value in the text box.
Add	Enters the query specified by the Field, Operator, and Value fields into the Query Expression text box. Each click of the Add button appends the current settings to the query as an AND clause.
Update	Updates a selected query clause with the parameters specified in the Field, Operator, and Value fields
Merge	Creates an OR clause (inserts a pipe character) for the selected query clause. This button is enabled under the following conditions: <ul style="list-style-type: none"> The Field in the drop-down list matches the Field specified in the selected query clause. The Operator in the selected query clause cannot be "Is Not". The Operator in the drop-down list cannot be "Is Not". <p>Note: The pipe character does not appear in the Query Expression for a User Roles query clause, but it will appear in the DocDisclosureQuery field.</p>
Query Expression	Displays each clause of the query as a single line.
Delete	Deletes the selected query clause.
Append	Appends the Query Expression to any existing query in the DocDisclosureQuery field on the Content Check In Form page.
Replace	Replaces any existing query in the DocDisclosureQuery field on the Content Check In Form page with the Query Expression.
Cancel	Closes the Disclosure Query Security applet without applying any query changes.

B.4.3 Query Syntax

The Disclosure Security Query applet creates queries with the correct Idoc Script syntax, but you can also enter your own queries directly in the DocDisclosureQuery field. The following Idoc Script syntax is used in disclosure queries:

- [Like Operator](#)
- [Boolean Operators](#)

- [UserName Variable](#)
- [stdSecurity Variable](#)
- [User Attribute Fields](#)
- [User Roles](#)

**Note:**

You can learn how to correctly format query clauses for direct entry in the DocDisclosureQuery field by experimenting with the Disclosure Query Security Applet.

B.4.3.1 Like Operator

The `like` operator matches substrings and wildcard strings. Enclose all strings in single quotes.

B.4.3.1.1 Substrings

Use the `like` operator to match substrings.

B.4.3.1.2 Wildcard Strings

Use wildcard strings to match variable characters and options. Wildcard strings use the syntax

* = Match 0 or more characters

? = Match exactly 1 character

| = Separates multiple options, only one of which needs to match

For example, the following code would match "MyClient", "3rd Quarter MyClient Report", "MyClient Visit", "Meeting with MyClient", and "1996 Reports". This string would not match "My Client", "All 1996 Reports", or "1996 Report".

```
dDocName like '*MyClient*|199? Reports'
```

B.4.3.2 Boolean Operators

Query clauses can be joined by `and`, `or`, and `not` Boolean operators.

- The Boolean operators must be lowercase letters.
- Each clause must be in parentheses. For example:

```
(uRoles like '*:contributor:*') and (uUserLocale like 'hg')
```

B.4.3.3 UserName Variable

The variable `UserName` is the name of the user who is currently logged in. For example, the following code would grant privileges only to the users `jgreen` or `hbrown`.

```
UserName like 'jgreen|hbrown'
```

B.4.3.4 stdSecurity Variable

The variable `stdSecurity` specifies the standard security model; it is mapped to the `stdSecurityCheck` Idoc Script function. This variable can be used in Boolean combination with other query clauses to refine access (using the `and` operator) or expand access (using the `or` operator). For example, the following code would grant access to the document if the user would normally be able to access the document or they are *jgreen* or *hbrown*.

```
stdSecurity or UserName like 'jgreen|hbrown'
```

B.4.3.5 User Attribute Fields

When specifying user attribute fields in a query, use the format `uFieldName`. For example:

```
uMyUserField like 'Value'
```

B.4.3.6 User Roles

User roles require a special form because the `UserRoles` Idoc Script function returns all the roles for the current user in comma delimited form. (In this example, a `uRoles` shortcut has been defined for this function.) For example, the `uRoles` value could be:

```
role1,role2,...,role10
```

Therefore, to specify a query string that includes the value *role1*, wildcards must be included so that the query will recognize the value regardless of its position in the role list. For example:

```
uRoles like '*role1*'
```

However, this query string would also grant security access to a user with the role *role10*, which might not be a role you want to include. To limit the `uRoles` value to only those roles specified in the query, you need to use the `DelimitedUserRoles` function and syntax, which includes single quotes and colons on each side of the role value as follows:

```
uRoles like '*:role1:*
```

To match either *role1* or *role2*, use this syntax:

```
uRoles like '*:role1:*|*:role2:*
```

B.4.4 Defining a Content-Level Query

To define a query for an individual content item:

1. Open the Content Check In Form page (for a new content item) or the Info Update Form page (for an existing content item).
2. Click the **Update** button next to the **DocDisclosureQuery** field (the name of this field will be whatever you named it during installation).
3. In the Disclosure Query Security applet, select a Field, an Operator, and a Value to create a query clause.
 - **Field:** Select from a user attribute list which includes User Locale, User Name, User Role, and all of your custom user attribute fields.
 - **Operator:** Select an operator to apply to the Field and Value. The following operators are used for all fields except User Role:

- **Is:** The value in the specified Field matches the specified Value.
- **Is Not:** The value in the specified Field does not match the specified Value.
- **Begins With:** The value in the specified Field starts with the specified Value.
- **Contains:** The value in the specified Field contains the specified Value.

The User Role field has only one operator, Has Member, and enables a drop-down list of roles in the Value field.

- **Value:** If an option list was specified for the selected field, choose the value from the drop-down list. If no option list was specified for the selected field, type the value in the text box.

4. Click **Add**.

The query clause is added to the Query Expression text box.

5. Continue building the query:

- To add another query clause with an `and` operator, enter the values and click **Add**.
- To change an existing query clause, enter the new values, select the query line you want to change, and click **Update**.
- To create an or clause, enter the new values, select the query line you want to change, and click **Merge**.
- To delete a query clause, select the query line and click **Delete**.

6. Enter the query expression in the **DocDisclosureQuery** field.

- To replace the existing query in the **DocDisclosureQuery** field with the query expression in the applet, click **Replace**.
- To append the query expression in the applet to the existing query in the **DocDisclosureQuery** field, click **Append**.

The Disclosure Query Security applet converts the query clauses to the appropriate syntax for the query and enters the query in the **DocDisclosureQuery** field on the Content Check In Form or Info Update Form page.

 **Note:**

You can learn how to correctly format query clauses for direct entry in the **DocDisclosureQuery** field by experimenting with the Disclosure Query Security applet.

7. After filling out the rest of the fields, click **Check In** or **Update**.

The disclosure query is validated, and if the query is ill-formed, an error message tells you the specific problem with the query.

B.5 Administration Interface

After the Need to Know component has been installed, the NTK Configuration Information link is available through the **Administration** tray or menu. This link provides access to the NTK Configuration Information page, which provides security configuration status information and the capability to edit the security configuration.

The Need to Know component provides the following configuration pages:

- [NTK Configuration Information Page](#)
- [Content Security Configuration Information Page](#)
- [Search Results Configuration Information Page](#)
- [Hit List Roles Configuration Information Page](#)
- [Test NTK Content Security Page](#)

B.5.1 NTK Configuration Information Page

The NTK Configuration Information page provides information about Need to Know content security configuration, search results configuration, and hit list roles configuration. This page also enables you to edit the security configuration, edit the search results configuration, edit the hit list roles configuration, view Idoc Script and hidden fields for the configuration, and test Idoc Script.

NTK Configuration Information

Content Security Configuration Information

Access Level	Enabled	Limit Access	Script
Read	No	No	View Test
Write	No	No	View Test
Delete	No	No	View Test

Disclosure Field: <none>
Security Auth Groups: <All Special Auth Groups>
Debug: No

Search Results Configuration Information

Hidden Fields: [View](#)
Script: [View](#)

Hit List Roles Configuration Information

Query Role: <none>
Update Role: <none>
Allow Hit List Role for Anonymous Users: No

To access this page, from the main menu choose **Administration**, then **NTK Configuration Information**.

Element	Description
Access Level	Displays the permission levels (Read, Write, Delete) for access to content items.
Enabled	<p>Indicates whether Need to Know security is enabled for Read, Write, or Delete access.</p> <p>No: Need to Know security is disabled for the access level. This is the default.</p> <p>Yes: Need to Know security is enabled for the access level.</p>
Limit Access	<p>Specifies whether Read, Write, and Delete access is limited by Need to Know security. If Need to Know security is used to limit user access, it does so regardless of whether the user has standard Read, Write, or Delete access to a content item. If Need to Know security is not used to limit user access, the user has standard access to a content item. This feature enables you to create a security model more restrictive than the standard security model.</p> <p>No: Access is not limited by Need to Know security. This is the default</p> <p>Yes: Access is limited by Need to Know security.</p>
Script	<p>Provides links to view or test Idoc Script that is evaluated to determine if a user has Read, Write, or Delete access to a content item. The Need to Know component uses one of three parameters as a flag to determine if access is given:</p> <p>Read access: isNTKReadAccess</p> <p>Write access: isNTKWriteAccess</p> <p>Delete access: isNTKDeleteAccess</p> <p>Click View in the row for the access level for which you want to view the Idoc Script that the Need to Know component evaluates to determine if a user has Read, Write, or Delete access.</p> <p>Click Test in the row for the access level for which you want to test the Need to Know security configuration. The NTK Test Content Security page appears. You can use this page to create and run a test of Idoc Script for security configuration. For more information, see Test NTK Content Security Page.</p>
Disclosure Field	<p>Displays the custom metadata field that is evaluated for the Idoc Script function <code>isDisclosureQuery</code>. The disclosure field can be used to create a content-specific query. The default value is <code><none></code>.</p> <p>Use the Configuration Manager to create this field, and make it a memo field type. For more information, see Installing the Need To Know Component and Configuring the Need to Know Component.</p> <p>When the disclosure field exists, an Update button appears next to the field where it appears on the Content Check In Form page. Click the button to access the Disclosure Query Security Applet (see Disclosure Query Security Applet). The applet helps you create queries based on the user metadata.</p>
Security Auth Groups	<p>Displays a list of security groups for which Need to Know security is used. The groups must be a subset of the <code>SpecialAuthGroups</code> configuration variable. If no groups are selected, all <code>SpecialAuthGroups</code> are used. The default value for <code>SpecialAuthGroups</code> is <code><All Special Auth Groups></code>.</p> <p>Use the Configuration Manager to specify a <code>SpecialAuthGroups</code> value in the <code>config.cfg</code> file. For more information, see Installing the Need To Know Component and Configuring the Need to Know Component.</p>

Element	Description
Debug	<p>Displays the status of the debugging option.</p> <p>Yes: Debugging information is written to a log file for any security check that occurs for a content item. Users with the administrator role are not logged because they always receive access to the content item.</p> <p>No: Debugging information is not written to a log file.</p>
Edit (Content Security Integration Information)	Displays the Content Security Configuration Information page, where the content security configuration can be changed
Hidden Fields	Click View to display a list of fields that can be hidden on the Search Results page.
Script	Click View to display the Idoc Script that controls the presentation of the Search Results page.
Edit (Search Results Configuration Information)	Displays the Search Results Configuration Information page, where the search results security configuration can be changed.
Query Role	Displays the name of the query role, or <none>. This role is applied on the Search query page.
Update Role	Displays the name of the update role, or <none>. This role is applied on a content check-in or update page.
Allow Hit List Role for Anonymous Users	<p>Applies the hit list role for anonymous users.</p> <p>No: The hit list role is not applied for anonymous users. This is the default value.</p> <p>Yes: The hit list role is applied for anonymous users.</p>
Edit (Hit List Roles Configuration Information)	Displays the Hit List Roles Configuration Information page, where the hit list roles security configuration can be changed.

B.5.2 Content Security Configuration Information Page

The Content Security Configuration Information page enables you to change security and access configuration for Read, Write, Delete, and other options for the Need to Know component.

Content Security Configuration Information

[NTK Configuration Information](#) --> Content Security Configuration Information

Read Options

Use Security

Limit Access

Script

Write Options

Use Security

Limit Access

Script

Delete Options

Use Security

Limit Access

Script

Other Options

Disclosure Field

Security Auth Groups All Auth Groups

Debug

To access this page, click **Edit** in the Content Security Configuration Information area of the NTK Configuration Information page.

Element	Description
Read Options: Use Security	Use security as specified in the Script field. No: Do not use Need to Know content security. This is the default value. Yes: Use Need to Know content security.
Read Options: Limit Access	Limit access permissions as specified in the Script field. No: Do not limit access permissions. This is the default value. Yes: Limit access permissions.
Read Options: Script	Enter Idoc Script in this field to specify the Need do Know security configuration for Read permission.
Write Options: Use Security	Use security as specified in the Script field. No: Do not use Need to Know content security. This is the default value. Yes: Use Need to Know content security.
Write Options: Limit Access	Limit access permissions as specified in the Script field. No: Do not limit access permissions. This is the default value. Yes: Limit access permissions.
Write Options: Script	Enter Idoc Script in this field to specify the Need to Know security configuration for Write permission.
Delete Options: Use Security	Use security as specified in the Script field. No: Do not use Need to Know content security. This is the default value. Yes: Use Need to Know content security.
Delete Options: Limit Access	Limit access permissions as specified in the Script field. No: Do not limit access permissions. This is the default value. Yes: Limit access permissions.
Delete Options: Script	Enter Idoc Script in this field to specify the Need to Know security configuration for Delete permission.
Other Options: Disclosure Field	Select the name of a disclosure field from the list. This field is used to configure security in a content-specific query. Note: If you create a metadata field for content item-level queries using the Configuration Manager, that field will appear as an option in the list.
Other Options: Security Auth Groups	Enter the <code>SpecialAuthGroups</code> to be used in content-specific queries. If you use the General Configuration page to create a specific security group for the Need to Know component, you can specify the group here. If you need to add a security group, you can also edit the Additional Configuration Variables <code>SpecialAuthGroups</code> value in the <code>config.cfg</code> file.
Other Options: All Auth Groups	Specifies that the Need to Know component use all <code>SpecialAuthGroups</code> instead of a specific group listed in the Security Auth Groups field. This check box is selected by default. Note: Other products such as Records Management can also use the <code>SpecialAuthGroups</code> variable. Be careful to specify only the security groups you want to use the Need to Know security configuration.

Element	Description
Other Options: Debug	<p>Select whether to use debugging to view security checking for a content item.</p> <p>Yes: Debugging information is written to a log file for any security check that occurs for a content item. Users with the administrator role are not logged because they always receive access to the content item.</p> <p>When debugging is used, two additional options are visible: <i>View</i> and <i>Clear</i>. Click View to view the log file of debugging information. Click Clear to empty the log file of information.</p> <p>No: Debugging is not used and information is not written to a log file. This is the default value.</p>
Update	Updates the content security information to use the new settings, restarts the Content Server instance, and returns you to the NTK Configuration Information page.
Reset	Returns the Content Security configuration settings to their last saved values.

B.5.3 Search Results Configuration Information Page

The Search Results Configuration Information page enables you to customize the search results that are returned from a search query. This does not affect what content items are returned, just how the results appear.

Search Results Configuration Information

NTK Configuration Information --> Search Results Configuration Information

Hidden Fields

<< Add

Remove >>

Available Fields

Standard

- Content ID
- Content Type
- Title
- Author
- Security Group
- Score
- Account
- Release Date
- Expiration Date

Script

Update Reset

To access this page, click **Edit** in the Search Results Configuration Information area of the NTK Configuration Information page.

Element	Description
Hidden Fields	Displays the list of fields that are hidden from view in a content search query result. The values are set to empty strings. These fields are hidden if the field hideFields is set in the search results script.
Available Fields	Displays the list of fields that are included in a content search query result.
Add	Select a field name and click Add to move the field from the Available Fields list to the Hidden Fields list, making the field hidden in a content search result.
Remove	Select a field name and click Remove to move the field from the Hidden Fields list to the Available Fields list, making the field visible in a content search result.
Script	<p>Enter Idoc Script in this field to control the presentation of search results. The Idoc Script is evaluated for each row in the search results. A number of fields can be set to alter the presentation:</p> <ul style="list-style-type: none"> • docInfo:enabled: Set to 0 to disable the content information link. • docInfo:link: Set to alter the content information page link. • docInfo:image_small: Set to alter the small image for the information link. • docInfo:image_large: Set to alter the large image for the information link. • url:enabled: Set to 0 to disable the URL link. • url:link: Set to alter the URL link. • url:image: Set to alter the image for the URL link. • revHistory:enabled: Set to 0 to disable the revision history link. • revHistory:link: Set to alter the revision history link. • checkout:enabled: Set to 0 to disable to checkout link. • checkout:linkF: Set to alter the checkout link. • actions:enabled: Set to 0 to disable the actions popup link. • checkInSimilar:enabled: Set to 0 to disable the Check In Similar link. • email:enabled: Set to 0 to disable the email link. • dynConv:enabled: Set to 0 to disable the Dynamic Converter link.
Update	Updates the configuration for search query results, restarts the Content Server instance, and returns you to the NTK Configuration Information page.
Reset	Returns the Search Results configuration settings to their last saved values.

B.5.4 Hit List Roles Configuration Information Page

The Hit List Roles Configuration Information page enables you to configure hit list roles for users.

Hit List Roles Configuration Information

[NTK Configuration Information](#) --> Hit List Roles Configuration Information

Query Role

Update Role

Allow Hit List Role for Anonymous Users

To access this page, click **Edit** in the Hit List Roles Configuration Information area of the NTK Configuration Information page.

Element	Description
Query Role	<p>Select the hit list role to be applied as the query role when the Search page is used. Security group roles with Read access are displayed in the list of selections, including any security group roles for which the user already has Read access.</p> <p>This role is separate from content security. You could have a content item appear in Search results configured for content security, but the user would not be able to view the Content Information page for that item.</p>
Update Role	<p>Select the hit list role to be applied as the update role when the Update page is used. Security group roles with Write access are displayed in the list of selections, including any security group roles for which the user already has Write access. When the content item is actually checked in or updated, this role is <i>not</i> applied.</p> <p>This field is probably most useful in conjunction with content security. For examples of using this field, see Security Customization Samples.</p>
Allow Hit List Role for Anonymous Users	<p>Applies the hit list roles for anonymous users.</p> <p>No: Do not apply the hit list roles for anonymous users. This is the default value.</p> <p>Yes: Apply the hit list roles for anonymous users.</p>
Update	<p>Updates the hit list configuration, restarts the Content Server instance, and returns you to the NTK Configuration Information page.</p>
Reset	<p>Returns the Hit List Roles configuration settings to their last saved values.</p>

B.5.5 Test NTK Content Security Page

The Test NTK Content Security page enables you to run a test security script for a user.

To access this page, click **Test** in the Script column for one of the access permission levels displayed on the NTK Configuration Information page.

Element	Description
Access Level	Displays the access level for the permissions level you select to test: Read, Write, or Delete.
Script	Enter Idoc Script for the content security configuration to be tested.
User	Enter the user ID for the test.
Set Attributes	Select the check box to automatically set the user attributes to match the user's existing attributes.
Roles	Enter the roles assigned to the user for the test. Use this field if you are testing with external users where attributes may not be accessible.
Accounts	Enter the accounts assigned to the user for the test. Use this field if you are testing with external users where attributes may not be accessible.
Content ID	Enter the content ID for the test.
Test	Click Test to test the configuration specified on the Test NTK Content Security page. The Need to Know component test returns results on whether the user has the specified access, whether Need to Know security was used, and if Need to Know security was not used then the reason why.
Reset	Returns the Test NTK Content Security configuration settings to their last saved values.

B.6 Security Customization Samples

This section contains samples of security model customization.

- [Content Security Samples](#)

- [Search Result Samples](#)
- [Hit List Roles Samples](#)

B.6.1 Content Security Samples

This section contains samples of content security customization:

- [Simple Idoc Script Function](#)
- [Using stdSecurityCheck](#)
- [Using isStrIntersect](#)
- [Using allStrIntersect](#)
- [Using includeNTKReadSecurityScript](#)

B.6.1.1 Simple Idoc Script Function

This sample allows Read access if the user *Color* custom field and the content *Color* custom field match.

```
<$if strEquals(uColor, xColor)$>  
<$isNTKReadAccess=1$>  
<$endif$>
```

B.6.1.2 Using stdSecurityCheck

This sample allows Read access if the user *Color* is *Blue* and the user has standard security to the content.

```
<$if stdSecurityCheck() and strEquals(uColor, "Blue")$>  
<$isNTKReadAccess=1$>  
<$endif$>
```

B.6.1.3 Using isStrIntersect

This sample returns true because 3 is a member of the first string.

```
<$if isStrIntersect("1,2,3,4", "5,3")$>  
<$isNTKReadAccess=1$>  
<$endif$>
```

This sample returns false because neither 5 or 6 is a member of the first string.

```
<$if isStrIntersect("1,2,3,4", "5,6")$>  
<$isNTKReadAccess=1$>  
<$endif$>
```

This sample returns false because the second string is empty and the third parameter is not specified.

```
<$if isStrIntersect("1,2,3,4", "")$>  
<$isNTKReadAccess=1$>  
<$endif$>
```

This sample returns true because the second string is empty and the third parameter is true.

```
<$if isStrIntersect("1,2,3,4", "", 1)$>  
<$isNTKReadAccess=1$>  
<$endif$>
```

This sample returns false because the second string is empty and the third parameter is false. Note that the third parameter can be a string (for example, "True" or "T") or a number (for example, 1, 0).

```
<$if isStrIntersect("1,2,3,4", "", 0)$>
<$isNTKReadAccess=1$>
<$endif$>
```

B.6.1.4 Using allStrIntersect

This sample returns false because 5 is not a member of the first string.

```
<$if allStrIntersect("1,2,3,4", "5,3")$>
<$isNTKReadAccess=1$>
<$endif$>
```

This sample returns true because 3 and 4 are members of the first string.

```
<$if allStrIntersect("1,2,3,4", "3,4")$>
<$isNTKReadAccess=1$>
<$endif$>
```

The samples in Using isStrIntersect (page 4-2) that use the third parameter would work the same with allStrIntersect.

B.6.1.5 Using includeNTKReadSecurityScript

Read script:

```
<$if strEquals(dDocType, "Document")$>
<$isNTKReadAccess=1$>
<$endif$>
```

Write script:

```
<$includeNTKReadSecurityScript()$>
<$if isNTKReadAccess and strEquals(uColor, "Red")$>
<$isNTKWriteAccess=1$>
<$endif$>
```

The user has Write access to the content item if they have read access (type is *Document*) and the user's *Color* is *Red*.

B.6.2 Search Result Samples

This section contains samples of search results customization:

- [Disabling Links](#)
- [Changing Links](#)
- [Changing Images](#)

B.6.2.1 Disabling Links

This sample disables the URL and Content Information link if the user does not have Read access to the content item. This could be used if you set the query role to show extra content items in the search results, but don't want users to see links to them.

```
<$if not securityCheck()$><$docInfo:enabled=0$><$url:enabled=0$><$endif$>
```

B.6.2.2 Changing Links

This sample alters the Content Information and URL link to another service if the *Color* of the content is *Red*.

```
<$if strEquals(xColor, "Red")$><$docInfo:link=HttpCgiPath & "?  
IdcService=GET_USER_INFO"$><$url:link="javascript:alert('Cannot view  
content.')"$><$endif$>
```

B.6.2.3 Changing Images

This sample alters the Content Information link if the *Color* of the content item is *Green*.

```
<$if strEquals(xColor, "Green")$><$docInfo:image_small=HttpImagesRoot & "oracle/  
tree_icons/historical.gif"$><$endif$>
```

B.6.3 Hit List Roles Samples

This section contains samples of hit list roles customization:

- [Using the Query Hit List Role](#)
- [Creating a Black Hole Check In](#)

B.6.3.1 Using the Query Hit List Role

If you set the Query role to be *queryRole*, and *queryRole* has Write access to the security group *NTKGroup*, then *NTKGroup* will appear in the security group option list. You could then limit what content information appears by customizing the Search Results configuration values

B.6.3.2 Creating a Black Hole Check In

By using the Update role, you could create a scenario where a user could check in a content item and then not be able to view or edit it. You would need to do the following:

1. Create a role called *updateRole* that has Read/Write access to the security group *NTKGroup*.
2. Update the Write content security script so that if a meta change is occurring and the security group is *NTKGroup*, allow access.

```
<$if isMetaChange and strEquals(dSecurityGroup,  
"NTKGroup")$><$isNTKWriteAccess=1$><$endif$>
```

C

Troubleshooting Oracle WebCenter Content

This appendix describes some problems that you might encounter when using Oracle WebCenter Content and specifically Content Server. This appendix provides information on methods and tools that can be helpful with the troubleshooting process.



Note:

For details about troubleshooting Oracle WebCenter Content features such as Inbound Refinery, Content Tracker, Records, the WebCenter Content repository, Folios, and so forth, see Troubleshooting in *Managing Oracle WebCenter Content*.

This appendix includes the following sections:

- [Introduction to Troubleshooting Oracle WebCenter Content](#)
- [Getting Started with Troubleshooting Basics for Oracle WebCenter Content](#)
- [Troubleshooting Oracle WebCenter Content Archiving](#)
- [Using My Oracle Support for Additional Troubleshooting Information](#)

C.1 Introduction to Troubleshooting Oracle WebCenter Content

This section provides guidelines and a process for using the information in this appendix. Using the following guidelines and process will focus and minimize the time you spend resolving problems.

Guidelines

When using the information in this appendix, Oracle recommends:

- After performing any of the solution procedures in this chapter, immediately retry the failed task that led you to this troubleshooting information. If the task still fails when you retry it, perform a difference solution procedure in this chapter and then try the failed task again. Repeat this process until you resolve the problem.
- Make notes about the solution procedures you perform, symptoms you see, and data you collect while troubleshooting. If you cannot resolve the problem using the information in this chapter and you must log a service request, the notes you make will expedite the process of solving the problem.

Process

Follow the process outlined in when using the information in this appendix. If the information in a particular section does not resolve your problem, proceed to the next step in the process.

Table C-1 Process for Using the Information in this Appendix

Step	Section to Use	Purpose
1	Getting Started with Troubleshooting Basics for Oracle WebCenter Content	Get started troubleshooting Oracle WebCenter Content and the Content Server instance. The procedures in this section quickly address a variety of problems.
2	Troubleshooting Oracle WebCenter Content Archiving	Perform problem-specific troubleshooting procedures for Oracle Content Server archiving issues. This section describes: <ul style="list-style-type: none"> • Possible causes of the problems • Solution procedures corresponding to each of the possible causes
3	Using My Oracle Support for Additional Troubleshooting Information	Use My Oracle Support to get additional troubleshooting information. My Oracle Support provides access to several useful troubleshooting resources, including Knowledge Base articles and Community Forums and Discussions.
4	Using My Oracle Support for Additional Troubleshooting Information	Log a service request if the information in this appendix and My Oracle Support does not resolve your problem. You can log a service request using My Oracle Support at https://support.oracle.com .

C.2 Getting Started with Troubleshooting Basics for Oracle WebCenter Content

This section provides information on using various sources of useful, detailed information that can be helpful with the troubleshooting process.

- [Using Tracing](#)
- [Using Stack Traces](#)
- [Using the Environment Packager](#)
- [Using the Content Server Analyzer](#)
- [Using Debug Configuration Variables](#)
- [Analyzing HDA Files](#)

For information about Content Server logging, see [Monitoring Oracle WebCenter Content Server](#)

C.2.1 Using Tracing

You can activate Content Server tracing to display detailed system information that may be very useful for troubleshooting and optimizing system performance.

- [Server-Wide Tracing](#)
- [Applet-Specific Tracing](#)

C.2.1.1 Server-Wide Tracing

Server-wide tracing is used to view activities throughout the system. There are two ways to activate server-wide tracing.

- [Activating Tracing From the Content Server Administration Interface](#)

- [Activating Tracing From an Applet](#)

Sometimes when troubleshooting issues, the exact cause of the issue may be difficult to find. You may run across an error appearing in the log file. But it may not have enough information about what went wrong. In such cases, event trap tracing allows you to specify keywords for content server to look for as it is writing out tracing in the server output. If that keyword is found, all of the tracing in the buffer at that time will be sent to a separate event tracing output file. For more information on event trap tracing, see the A-Team blog <http://www.ateam-oracle.com/caught-in-the-act/>.

C.2.1.1.1 Activating Tracing From the Content Server Administration Interface

You can activate server-wide tracing from the Content Server administration interface.

To activate tracing from the Content Server administration interface:

1. Choose **Administration**, then **System Audit Information**.
2. Enable **Full Verbose Tracing** to see in-depth tracing for any active section that supports it.
3. Specify the traces to activate.
4. Click **Update**.
5. Click **View Server Output**.

 **Note:**

Tracing options are lost on system restart. To ensure your settings are retained after restarting the Content Server instance, enable **Save** before clicking **Update**.

C.2.1.1.2 Activating Tracing From an Applet

You can activate server-wide tracing from an applet:

To activate tracing from an applet:

1. Start an administrative applet.
2. Choose **Options**, then **Tracing**.
3. Select **Server tracing**.
4. Select the tracings to activate or **all** and click **OK**.

The following tracing options are available. Additional tracing sections can be displayed in the list if components are added.

- **applet:** This trace contains result sets from initialized applets, such as the Configuration Manager or User Admin.
- **archiver:** This trace provides information about archiving activities, including the reading and writing of archiver data files and the time the activities were initiated and finished.
- **archiverlocks:** This trace provides information about the locks put on files during archiving activities, including time initiated.
- **chunkedrequest:** This trace displays the messages and headers that are created when large requests are 'chunked' in to smaller requests.
- **docprofile:** This trace displays the computation of content profiles, specifically the evaluation of the rules that determine which fields are labels, hidden, and so on.

- **encoding:** This trace provides information about encoding transformations that have occurred and the activities where encoding occurred.
- **filelock:** This trace displays information about short-term system locks put on directories (during activities like archiving, for example) with a focus on collisions that occur and time outs.
- **filelonglock:** This trace displays information about the creation, removal, and maintenance of long term locks imposed by the system.
- **filequeue:** This trace displays information about accesses to a file queue.
- **indexer:** This trace displays information about index functions that occur when the database is updated, including the steps taken to update the index and the time elapsed for each step.
- **indexermonitor:** This trace provides a brief summary of automatic index activities, including time started and ended.
- **indexerprocess:** This trace displays information about a manually launched index process and indicates if the process terminated properly.
- **localization:** This trace displays information about localization usage and activities.
- **mail:** This trace describes mail sent by the Content Server instance.
- **pagecreation:** This trace displays information about the creation of displayed pages, including the server thread and the time taken to generate the page.
- **requestaudit:** This trace provides summary reports on service requests, including the elapsed time for the requests and the number of requests made. For more information, see the ["Expanding on requestaudit – Tracing who is doing what...and for how long"](#) blog.
- **scheduledevents:** This trace provides a list of hourly or daily background scheduled events.
- **schema:** This trace provides information about schema publishing (tables and views published as .js files) and caching (tables cached in to Content Server memory).
- **searchquery:** This trace displays information about recent searches, including the fields used to search on and the order of sorting for results.
- **socketrequests:** This trace displays the date, time, and thread number of socket requests and the actions during the request.
- **system:** This trace displays internal system messages, such as system socket requests and responses.
- **systemdatabase:** This trace provides information about database activities, including queries executed, index updates, threads used, and time initiated.
- **transfermonitor:** This trace displays information about the archiver and the batch file transfer activities.
- **userstorage:** This trace describes the access of external user repositories, including what actions were taken during access.
- **workflow:** This trace displays a list of metadata on content items going through workflow, including document title and revision number.

 **Note:**

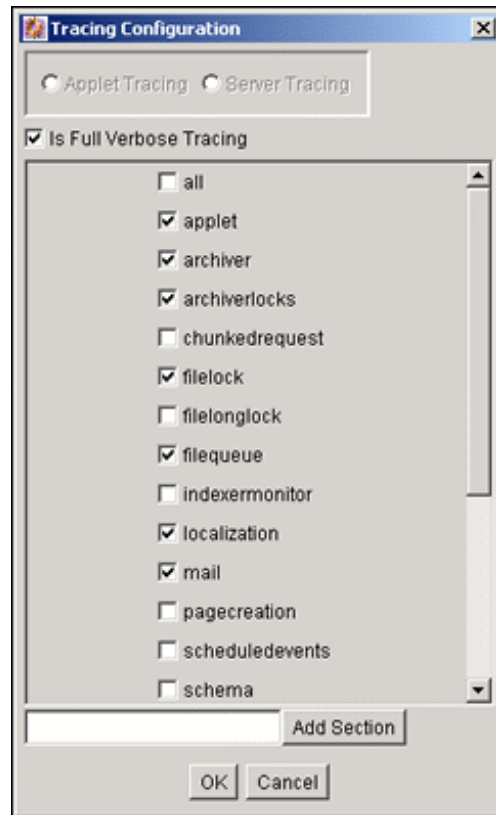
To facilitate international support, most tracing messages are in English and do not have translations.

C.2.1.2 Applet-Specific Tracing

For applet-specific tracing, the output goes to the browser Java console. To perform tracing by applet:

1. Start the administration applet to be traced.
2. Choose **Options**, then **Tracing**.
3. Make your selections, and click **OK**. The output is directed to the browser Java console.

Figure C-1 Applet-Specific Tracing



C.2.2 Using Stack Traces

The stack trace enables you to see what threads are currently running in the Content Server instance. It is a useful troubleshooting tool that provides information about the threads and enables you to monitor Content Server processing.

For instructions to initiate a current stack trace for the Content Server instance, see Oracle WebLogic Server documentation.

C.2.3 Using the Environment Packager

The Environment Packager is a diagnostic tool. It creates a zip file of the targeted state directories, log files, and other component and resource directories.

To create an environment zip file:

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Environment Packager**.
3. On the Environment Packager page, select which parts of the environment should be packaged.
4. When you are ready to create the environment zip file, click **Start Packaging**. A message is displayed while the zip file is being built, with a link to the zip file. The packaging process may take several minutes. The zip file link will not be available until the process has finished.

Note:

The packaged zip is named `server_environment_*.zip`. While the Content Server instance builds the packaged zip file, it will be located in `IntradocDir/vault/~temp`. When the build of the zip file is complete, it is moved to `IntradocDir/weblayout/groups/secure/logs/env`.

C.2.4 Using the Content Server Analyzer

The Content Server Analyzer application enables you to confirm the integrity of the Content Server repository components, including the file system, database, and search index. It can also assist system administrators in repairing some problems that are detected in the repository components.

Using the Content Server Analyzer, system administrators can do the following:

- Confirm the accuracy of synchronization between three important Content Server database tables (Revisions, Documents, and DocMeta).
- Confirm that the `dRevClassID` and `dDocName` fields are consistent across all revisions of content items.
- Determine if the file system (native and web-viewable file repositories) contains any duplicate or missing files.
- Ensure the accuracy of synchronization between the search index and the file system.
- Ensure the accuracy of synchronization between the search index and the Revisions database table.
- Ensure that the file system contains all necessary files.
- Remove duplicate files from the Content Server repository either permanently or provisionally by moving them in to the `logs/` directory.
- Produce a general report on the state of content items in the Content Server repository.

The method to start the Content Server Analyzer depends on the operating system:

- Windows: Choose **Start**, then **Oracle Content Server**, then *instance*, then **Content Server Analyzer**.
- UNIX: Navigate to the *DomainHome/ucm/cs/bin/* directory and run the Content Server Analyzer program.

These sections describe Content Server Analyzer tasks:

- [Accessing the Content Server Analyzer](#)
- [Specifying a Custom Analyzer Log Directory](#)
- [Invoking the Analysis Process](#)
- [Analyzing the Content Server Database](#)
- [Analyzing the Content Server Search Index](#)
- [Viewing the Analysis Progress and Results](#)
- [Generating a Status Report](#)
- [Canceling the Status Report](#)

C.2.4.1 Accessing the Content Server Analyzer

To display the Content Server Analyzer, use one of the following methods:

- Windows: Choose **Start**, then **Programs**, then **Content Server**, then *instance*, then **Utilities**, then **Content Server Analyzer**.
- UNIX: Change to the *DomainHome/ucm/cs/bin/* directory, type `./IdcAnalyze` in a shell window, and press the RETURN key on your keyboard.

The Content Server Analyzer application is displayed.

C.2.4.2 Specifying a Custom Analyzer Log Directory

The `logs/` directory is the default logging directory for the Content Server Analyzer. Analysis output files are written to this directory and extra files detected during a file system analysis process can be transferred here as well. Optionally, the default `logs/` directory name and path can be changed as desired.

To customize the Analyzer log directory name and path:

1. On the Content Server Analyzer: Configuration tab, place the cursor in the **Analyzer log dir** field.
2. Enter the desired directory path. During the next analysis process, the Content Server Analyzer automatically creates the specified directory or directories in the *DomainHome/ucm/cs/bin/* directory hierarchy.

C.2.4.3 Invoking the Analysis Process

To invoke the analysis process:

1. On the Content Server Analyzer: Configuration tab, select and activate the desired options (checking the corresponding check boxes).
2. Click **Start Analysis**.

 **Note:**

If this is the very first time the Content Server Analyzer has been run, the output files in the `logs/` directory are automatically created. On subsequent analysis processes, a confirmation message is displayed asking to overwrite the existing log file.

3. Click **Yes** to overwrite the existing log file. The Content Server Analyzer: Progress tab automatically opens. A completion message opens when all of the selected analysis processes are finalized.

 **Note:**

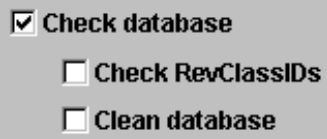
If you click **No**, the analysis process is terminated and you are prompted to manually remove files from the `logs/` directory before running the Content Server Analyzer again.

4. Click **OK**.

The results are displayed in the console area on the Progress tab.

C.2.4.4 Analyzing the Content Server Database

The **Check RevClassIDs** and **Clean database** options are used to check the integrity of the database columns. The available options enable users to examine the three tables that are used to store content item revision information (DocMeta, Documents, and Revisions). The DocMeta file is examined for extra entries that are not found in the Revisions table. Similarly, the Documents table is examined to verify that there are sufficient entries to correspond to the entries in the Revisions table.



Check database
 Check RevClassIDs
 Clean database

 **Note:**

The **Check RevClassIDs** and **Clean database** options are activated and selectable only when the **Check database** option is selected.

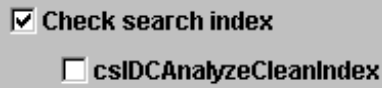
To analyze the Content Server database:

1. On the Content Server Analyzer: Configuration tab, select the applicable options.
2. Click **Start Analysis**.

The results are displayed in the console area on the Content Server Analyzer: Progress tab. For information about the analysis procedure, see [Invoking the Analysis Process](#).

C.2.4.5 Analyzing the Content Server Search Index

The **Check search index** and **csIDCAnalyzeCleanIndex** options are used to check the entries in the Revisions table to ensure that all of the documents that belong in the index are properly listed. Additionally, a check can be performed to ensure that there are no duplicate entries in the search index.



Check search index
 csIDCAnalyzeCleanIndex

Note:

The **csIDCAnalyzeCleanIndex** option is activated and selectable only when the **Check search index** option is selected.

To analyze the Content Server search index:

1. On the Content Server Analyzer: Configuration tab, select the applicable options.
2. Click the **Start Analysis** button (for information about the analysis procedure, see [Invoking the Analysis Process](#)).

The results are displayed in the console area on the Content Server Analyzer: Progress tab.

C.2.4.6 Viewing the Analysis Progress and Results

The Content Server Analyzer: Progress tab is displayed automatically when the **Start Analysis** button is clicked. The progress bars show when the Content Server Analyzer has completed processing the selected analysis options. The following image shows a partially finished analysis:

When the analysis process is complete, the results are displayed in the console area of the Progress tab. The results depend on what analysis options were selected. The following image of the console area shows the results from selecting database, search index, and file system options:

Note:

The Generate report option was not selected for this example. For an example of the generated status report, see [Generating a Status Report](#).

Figure C-2 Example Console Display of Results

```

Analyzing tables...
Error Count: 0.
Analyzing Index
Error Count: 0.
Checking filesystem.
Error Count: 0.
Finding Extra Files
Scanning c:/stellent/weblayout/groups/
Scanning c:/stellent/weblayout/groups/secure/
Scanning c:/stellent/weblayout/groups/public/
Scanning c:/stellent/weblayout/groups/public/documents/
Scanning c:/stellent/weblayout/groups/public/documents/adacct/
Scanning c:/stellent/weblayout/groups/public/documents/adeng/
Scanning c:/stellent/vault/
Scanning c:/stellent/vault/adacct/
Scanning c:/stellent/vault/adeng/
24 items found.
Ignored file: c:/stellent/weblayout/groups/secure/logs.
Ignored file: c:/stellent/weblayout/groups/secure/pages.
Ignored file: c:/stellent/weblayout/groups/public/pages.
Ignored file: c:/stellent/vault/~temp.
Error Count: 0.
    
```

C.2.4.7 Generating a Status Report

The status report generated by the Content Server Analyzer provides statistics about the content items in the repository. The status report output is displayed in the console area of the Progress tab.

To generate a status report:

1. On the Content Server Analyzer: Configuration tab, select **Generate report**.
2. Click **Start Analysis**.

When the analysis process is complete, the status report information is displayed immediately following the standard analysis results in the console area of the Content server Analyzer: Progress tab.

C.2.4.8 Canceling the Status Report

The report generation feature can be suppressed after the analysis process has already started. To cancel the content item status report during the analysis process:

1. During the analysis process, click **Cancel** on the Content Server Analyzer Application. You will be prompted about canceling after the current task is finished.
2. Click **Yes** to suppress the status report.

The status report is not included with the analysis results that are displayed in the console area of the Progress tab.

C.2.5 Using Debug Configuration Variables

The Content Server instance provides the debugging configuration variable `IsDevelopmentEnvironment`, which when set contributes applicable diagnostic information. This variable is set in the Content Server instance's configuration file (`IntradocDir/config/config.cfg`) during installation and when the Content Server instance is updated. `IsDevelopmentEnvironment` does the following:

- Defines whether the Content Server instance should run in debug mode.

- Enables a trace of script errors. If used as a parameter to a service call, script error information can be added to the bottom of the displayed page.

The debugging configuration variable `AlwaysReportErrorPageStackTrace`, also set in the Content Server instance's configuration file (`IntradocDir/config/config.cfg`), specifies that whenever an error occurs the stack trace is reported on the browser showing the Content Server interface.



Note:

See Configuration Variables in *Configuration Reference for Oracle WebCenter Content*.

C.2.6 Analyzing HDA Files

WebCenter Content administrators may need to analyze `.hda` (HDA) files in the process of troubleshooting Content Server issues. A HyperData File (HDA) is used to define properties and tabular data in a simple, structured ASCII file format. It is a text file (which can be identified by the suffix `.hda` in a file name) that is used by Content Server to determine which components are enabled and disabled and where to find the definition files for that component. The HDA file format is useful for data that changes frequently because the compact size and simple format make data communication faster and easier for Content Server. Details about HDA structure and use are available in HDA Files in *Developing with Oracle WebCenter Content*.

One option for reading a HDA is to add the `IsPageDebug=1` option to a page URL. When `IsPageDebug=1` is used, you can see a small gray tab at the bottom right-hand part of the browser window. When you click the tab, it expands and you can choose several pieces of information to display.

- **idocscript trace:** Displays the nested includes you previously could view with the `ScriptDebugTrace=1` variable in the 10gR1 release of Oracle Universal Content Management.
- **initial binder:** Displays the local data and result sets coming back from the service, just as you would by adding the `&IsJava=1` option to a page URL. In this display, it formats the results in easy-to-read tables instead of raw HDA format.
- **final binder:** Displays all of the local data and result sets after executing all of the includes for the display of the page (not just from the Service call).
- **javascript log:** Reports on the javascript functions and times being executed on the page.

For more information, see the Oracle Web page "What do you mean you don't read HDA?" at <http://www.ateam-oracle.com/what-do-you-mean-you-dont-read-hda/>.

C.3 Troubleshooting Oracle WebCenter Content Archiving

This section provides solutions to several common archiving issues for Content Server. Please attempt the recommended solutions before contacting Support.

This chapter covers the following topics:

- [Importing Issues](#)
- [Exporting Issues](#)

- [Transfer Issues](#)
- [Replication Issues](#)
- [Oracle Database Issues](#)
- [Miscellaneous Issues](#)

C.3.1 Importing Issues

This section covers the following topics:

- [File Extension Errors on Import System](#)
- [Selecting Specific Batch Files for Import](#)
- [Import Maps Do Not Work After Archive Import](#)
- [Identifying Imported Content Items From Archive](#)
- [Duplicate Content Items in Content Server](#)
- [Importing Archived Content to Proxied Server Fails](#)
- [No Importing Errors But Documents Are Missing](#)
- [Errors About Invalid Choice List Values](#)
- [Import Fails Due to Missing Required Field](#)
- [Changed Metadata Field Makes the Archiver Freeze During an Import](#)

C.3.1.1 File Extension Errors on Import System

Symptom

I am receiving errors on the importing system indicating that there are transfer and file extension problems with the documents.

Problem

The following errors were issued to the Archiver log:

```
Error: Event generated by user <user_name> at host <host_name>. File I/O error. Saving to file collection.hda. Write error.  
Error: Import error for archive <archive_name> in collection <collection_name>:  
Content item <item_name> was not successfully checked in. The primary and alternate files must have different extensions.
```

Recommendation

The I/O error on the export side probably corrupted the batch file and is, in turn, causing the file extension error on the import side. Possible solutions include:

- Open the batch file in a text editor and check for invalid data. Try deleting the exported `collection.hda` file and manually re-run the export/import function.
- In the exporting server, open the applicable `collection.hda` file and look for the lines associated with the content items that caused the file extension error. Some of the revisions of these content items may have the native file in the vault location listed in the alternate file location. There might also be a format entry for the alternate file. Delete these lines and re-import the files.

- Add an alternate extensions configuration setting to the Content Server configuration `config.cfg` file (`IntradocDir/config/config.cfg`) on the importing server:
 1. Open the `IntradocDir/Config/config.cfg` file in a text editor.
 2. Locate the **General Option Variables** section.
 3. Enter the following configuration setting:

```
AllowSamePrimaryAlternateExtensions=true
```

This configuration setting allows checked in content items to use identical document extensions for both the alternate and primary files.
 4. Save and close the `config.cfg` file.

 **Note:**

Although it probably is not necessary to add this configuration setting to the Content Server `config.cfg` file on the exporting server, it may be worthwhile to do so for general preventative measures.

5. Restart the Content Server instance.

C.3.1.2 Selecting Specific Batch Files for Import

Question

How can I select and re-run specific batch files from the General tab of the Archiver utility without deleting the remaining files that are required for backup purposes?

Recommendation

The most efficient method would be to create a new collection, copy the desired archives to the new collection, and run the import from there.

C.3.1.3 Import Maps Do Not Work After Archive Import

Symptom

I configured a value map to change metadata values during the import on an archive collection. But after the transfer, the import maps do not work.

Problem

The metadata values didn't reflect the configured metadata value changes.

Recommendation

To ensure that metadata value changes are retained when the files are exported into an archive and then later imported from that archive, the value maps must be configured on both sides of the transfer process. This means that the same value map must be configured on both the source (exporting) server as well as the target (importing) server.

C.3.1.4 Identifying Imported Content Items From Archive

Question

Due to a system crash, I need to import content from the old archive into a new archive without changing the content information (metadata) of the documents. How can I preface each content item using a letter or number to indicate that all the documents with this designation are new imports (but actually originated from the old archive)?

Recommendation

The archived documents can be re-imported and appropriately marked to distinguish them from other imported content items by applying an import map using the Content ID metadata field. An import map allows you to configure how values are copied from one metadata field to another during import. To set up the import `mapm`, complete the following steps:

1. On the **Import Maps** tab of the Archiver utility, click **Edit** in the **Field Maps** section.
2. On the Edit Value Maps page, select **All** (leave the **Input Value** field blank).
3. Select **Content ID** from the Field list.
4. Enter **X<\$dDocName\$>** in the **Output Value** field.

Where 'X' is the letter or number used to distinguish the re-imported content items and 'dDocName' is the database table field value for the document Content ID.

5. Click **OK**.

After you re-import the archive, the letter or number used for 'X' should be added to the content ID of each content item. Be sure to configure the same value map on both the source (exporting) server and the target (importing) server. This ensures that the metadata value changes are retained when the files are imported from the archive.

C.3.1.5 Duplicate Content Items in Content Server

Symptom

When I try to check in or import a content item, the following error message is issued:

```
Content item already exists.
```

Recommendation

This error is issued when archiving is done between contribution servers that are using the same autonumbering scheme for content IDs. For example:

- *Content ID 003* is checked in to Content Server instance A and later archived to Content Server instance B. If a file is checked in to Content Server instance B and the next auto-generated number happens to be 003, the error occurs.
- *Content ID 005* is checked in to both Content Server instance A and Content Server instance B. If this same content item is archived from Content Server instance A to Content Server instance B, the error occurs.

Possible solutions include:

- Set up an import value map that will add a prefix to the content ID of the imported files. For details, see [Identifying Imported Content Items From Archive](#).

- In each Content Server instance, use the System Properties utility to set up an automatic numbering prefix for checked-in content items:
 1. Start the System Properties utility.
 2. Open the Options tab.
 3. Select **Automatically assign a Content ID on check in**.
 4. Enter the desired prefix in the **Auto Name Prefix** field.
 5. Click **OK**.
 6. Restart the Content Server instance.

C.3.1.6 Importing Archived Content to Proxied Server Fails

Symptom

I am trying to import content from an exported archive to my proxied Content Server instance, but the import fails.

Recommendation

For more information about Archiver problems, open and view the Archiver logs (accessible from the Content Server instance's Administration page). These logs provide the type of message along with more descriptive information about the logged messages.

For example, if the Archiver log indicates that an import problem involves a metadata field option value that is unavailable, information about configured option lists for metadata fields can be found on the **Information Fields** tab of the Configuration Manager utility (accessible from the Administration page).

Using this information, compare the option list for the problem metadata field on both the exporting and importing servers. If there are any differences, corrections in one of the servers will make both option lists identical. This would resolve the unavailable option discrepancy.

C.3.1.7 No Importing Errors But Documents Are Missing

Symptom

When I run the import function, no errors are issued, but not all of the documents are being imported.

Problem

I exported 428 documents from the development server along with the configuration information (the metadata fields). Then, I transferred the archive to the main production server and ran the import. No errors were issued, so I thought everything had gone well. Unfortunately, when I searched the documents, I discovered that only 198 of the original 428 were actually imported.

Recommendation

Suggestions to resolve this problem include:

- Make sure that all Microsoft Word documents are included in the search index.

Particular versions of the search component do not include Microsoft Word documents with embedded links in the search index. Thus, these files will not be found in search queries.

You can remove all embedded links from the affected documents or add the following configuration setting to the *IntradocDir/config/config.cfg* file:

```
CheckMkvdkDocCount=true
```

This configuration setting ensures that all Word files are included in the search index. However, only the metadata is included, not the full text.

- Try exporting the original set of documents and ensure that the source files are deleted. Then re-import the archive that was just exported.

C.3.1.8 Errors About Invalid Choice List Values

Symptom

My imports are failing.

Problem

The system issues error messages indicating that there are invalid choice list values. I am currently using an option list in the Dependent Choice List applet to configure and control the values.

Recommendation

Apparently a specific metadata taxonomy has been established for your option lists such that there are probably fields that are dependent on each other. In this case, certain values in option lists are available based on what values have been selected in a previous option list. Unfortunately, when using the Archiver, the dependencies in your option lists are obviously conflicting with the Content Server instance's capacity to work with custom metadata fields.

A workaround for the conflict involves using the Content Server instance's Configuration Manager utility rather than the Dependent Choice List applet. This necessitates that you enter the metadata fields and corresponding option list values on the **Information Fields** tab of Configuration Manager:

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Configuration Manager**.
3. In the Configuration Manager window, select the **Information Fields** tab.
4. Click the **Add** button and enter one of your metadata field names in the Add Custom Info Field dialog.
5. Click **OK**.
6. In the Add Custom Info Field window, complete the fields as appropriate.
7. In the **Option List Type** field, choose the **Select List Not Validated** option.
8. This option ensures that content whose specified value does not match one currently entered in the **Use Option List** field are nevertheless checked in with the specified value. The **Use Option List** field lists the name for the list of values a user may choose from for the specified field.
9. Click **OK**.
10. Click **Update Database Design**.
11. Click **Rebuild Search Index**.

Use this method for the duration of your import process.

C.3.1.9 Import Fails Due to Missing Required Field

Symptom

I used the Archiver to export documents. Now, I'm trying to import them and the process fails.

Problem

When I try to import the previously exported documents, the Content Server issues an error indicating that the 'Company' metadata file is required.

Recommendation

You will need to use the Content Server instance's Configuration Manager utility to edit the *Company* field and make it a non-required field.

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Configuration Manager**.
3. In the Configuration Manager window, select the **Information Fields** tab.
4. Select the **Company** metadata field from the **Field Info** list.
5. Click **Edit**.
6. In the Edit Custom Info Field window, deselect **Require Value**.
7. Click **OK**.
8. Click **Update Database Design**.
9. Click **Rebuild Search Index**.

You should now be able to successfully re-import the archive.

C.3.1.10 Changed Metadata Field Makes the Archiver Freeze During an Import

Symptom

Some of our product names have changed and we need to update one of the metadata fields in the affected documents. After exporting all the documents with the old product name metadata field, I then attempt to import the documents using the new product name metadata field. But, every time I try this, the Archiver processes only a portion of the total archiving task and then stops.

Problem

Once the Archiver freezes, I am unable to navigate the Content Server user interface and I must shut down all of the open browsers. Also, during the next five minutes after shutting down the browsers, I have no connectivity to the Content Server instance at all. After this five-minute interval, I can access the Content Server instance again.

In addition to this freezing problem, the following error message is issued:

```
Stream error (299) - SKIPPING
```

Recommendation

One or more processes seem to be interrupting the import. Some possible problem solutions could be any of the following:

- [Checking the Metadata Field Properties](#)
- [Checking the Indexing Automatic Update Cycle](#)

C.3.1.10.1 Checking the Metadata Field Properties

The product name metadata field may not have been properly updated in Configuration Manager. Depending on the type of metadata field that the 'product name' is, changing the value could be the reason for the lock-up problem. Is the product name metadata field a (long) text field only or also an option list? If it is an option list, make sure that the new name value is a selection on the corresponding list.

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Configuration Manager**.
3. In the Configuration Manager window, select the **Information Fields** tab.
4. Select the product name metadata field from the **Field Info** list.
5. Click **Edit**.
6. In the Edit Custom Info Field window, if the **Field Type** value is *Text* or *Long Text* *and* **Enable Option List** is deselected, click **OK** or **Cancel** (this should not cause the lock-up problem).

Otherwise,

If **Enable Option List** is selected, then make sure that the new product name metadata field value is included as a selection on the corresponding list:

- a. Locate the **Use Option List** field and click **Edit**.
 - b. Enter the new product name metadata field value in the Option List dialog.
 - c. Click **OK**.
7. Click **OK** again (on the Edit Custom Info Field window).
 8. Click **Update Database Design**.
 9. Click **Rebuild Search Index**.

C.3.1.10.2 Checking the Indexing Automatic Update Cycle

The lock-up problem may be due to the indexer's automatic update cycle. The error message indicates that the indexer is failing because it loses connectivity. Every five minutes, the indexer executes an automatic update cycle and could somehow be grabbing the index file and locking it. If so, it might be useful to disable the indexer's automatic update cycle while you run the import.

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Repository Manager**.
3. In the Repository Manager window, select the **Indexer** tab.
4. Click the **Configure** button in the Automatic Update Cycle section of the tab.
5. In the Automatic Update Cycle window, deselect **Indexer Auto Updates**.
6. Click **OK**.

 **Note:**

Be sure to reactivate the automatic update cycle after completing the import. Otherwise, the server will no longer automatically update the index database, which could adversely impact future search results.

C.3.2 Exporting Issues

This section covers the following topics:

- [Total Export Possible with Blank Export Query](#)
- [New Check-Ins and Batch File Transfers](#)
- [Exporting User Attributes](#)
- [Folder Archive Export Doesn't Work If Collections Table Has Many Records](#)

C.3.2.1 Total Export Possible with Blank Export Query

Question

If I do not create an export query to define the content items to export, will the entire contents of my Content Server be exported?

Recommendation

Yes, test exports have confirmed that leaving the Export Query section blank (not defining an export query) will ensure that the Content Server contents are completely exported.

C.3.2.2 New Check-Ins and Batch File Transfers

Question

If I check some documents in to the Content Server after I have initiated a large export (but before it completes), will these documents be included in the export? Or, does the Archiver read the timestamp information and determine that the new files are more recent than those originally allocated for the export and not include them? Also, what happens to the archive export if the connection between the servers is interrupted or lost during the export?

Recommendation

When the export is initiated, Archiver runs a query on the system to build a list of the documents that are to be exported. This information is cached and used to build the export archive. Therefore, any new documents that are checked in during the export process will not be included even if they match the export query definition.

If the connection between servers is disrupted, the export process on the source server continues but the transfer to the target server stops. The source server accumulates a number of batch files. While waiting to transfer these files, the source server continues to ping the target server for a connection at regular interval. When the connection is reestablished, the accumulated batch files are transferred to the target server.

If you have used an automated (replicated) transfer, the batch files and their associated content files are removed from the source Content Server. If you have used a manual transfer, the batch files and their associated content files remain in the source Content Server.

C.3.2.3 Exporting User Attributes

Question

How can I export users in an archive?

Recommendation

You can export a `users.hda` file, which contains the user attributes from the Users database table, as follows:

1. Log in to the Content Server instance as an administrator.
2. Choose **Administration**, then **Archiver**.
3. In the Archiver window, select the **Export Data** tab.
4. Click **Edit** in the Additional Data section.
5. In the Edit Additional Data dialog, select **Export User Configuration Information**.
6. Click **OK**.

C.3.2.4 Folder Archive Export Doesn't Work If Collections Table Has Many Records

Symptom

I use the folder archive export feature to move my website hierarchy created by Site Studio. Initially, I can export folders by using the Virtual Folder Administration Configuration page without any problem. However, as my website grows, this function does not work anymore. The following errors are issued during the export procedure:

```
Error <timestamp> Event generated by user '<user>' at host '<host_name>'. Referred to by http://<host>/intradoc-cgi/nph-idc_cgi.exe?IdcService= COLLECTION_GET_ADMIN_CONFIG. Unable to retrieve content. Unable to execute service method 'loadCollectionArchive'. (System Error: Unknown error.)
Error <timestamp> IdcAdmin: Event generated by user '<user>' at host '<host>'. Unable to obtain the console output. Unable to execute the service 'GET_SERVER_OUTPUT' on Content Server 'contribution'. Unable to receive request. Response from host has been interrupted. Read timed out.
```

There is also an out-of-memory error in the Content Server output console:

```
<timestamp> SystemDatabase#Thread-13: SELECT * FROM Collections, ColMeta WHERE Collections.dCollectionID=ColMeta.dCollectionID AND dParentCollectionID=564
java.lang.OutOfMemoryError
Reporting error on thread Thread-13 occurring at <timestamp>.
java.lang.OutOfMemoryError
java.lang.OutOfMemoryError
```

Problem

Depending on the size of the folder hierarchy that is being exported as an archive file, the default heap size value for the Java Virtual Machine (JVM) may not be adequate.

Recommendation

Modify the heap size setting in the application server to provide more heap memory for Content Server. For details, see the appropriate application server documentation.

After restarting the Content Server instance, the archive export function should work correctly again.

C.3.3 Transfer Issues

This section covers the following topics:

- [Transfer Stopped When Target Locked Up](#)
- [Aborting/Deleting a Running Transfer](#)
- [Verifying the Integrity of Transferred Files](#)
- [Transfer Process Is Not Working](#)

C.3.3.1 Transfer Stopped When Target Locked Up

Symptom

The automated transfer function stopped when the target server locked up.

Problem

After restarting the target server, the log file listed an error message stating that there was a problem with a security group and that this prevented the import on the target server.

Recommendation

In this case, obviously the security group problem on the target server must be corrected before the transfer can proceed. Two additional procedures to perform that can help include:

- [Verifying and Testing the Outgoing Provider](#)
- [Restarting the Content Server](#)

C.3.3.1.1 Verifying and Testing the Outgoing Provider

Verifying and testing the outgoing provider ensures that it is set up and working properly:

1. Log in to the source Content Server instance as an administrator.
2. Go to the Administration page and click the **Providers** link.
3. Click the **Info** link of the appropriate outgoing provider.
4. Verify the information on the Outgoing Provider Information page.
5. Return to the Providers page and click the **Test** link corresponding to the outgoing provider.

C.3.3.1.2 Restarting the Content Server

In some cases, after problems have been corrected on either the source or the target server, the source server may stop transferring or possibly the automation function no longer works. In either case, restarting the Content Server instance should resolve the problem.

C.3.3.2 Aborting/Deleting a Running Transfer

Question

I accidentally started transferring an excessively large file to the production Content Server instance. What is the most efficient way to stop the transfer process while it is running?

Recommendation

There are several methods to abort or delete a transfer, including:

- [Disabling the Outgoing Provider](#)
- [Deleting a Transfer from the Transfer To Tab](#)
- [Deleting an Automated Transfer](#)

C.3.3.2.1 Disabling the Outgoing Provider

The fastest method to abort a running transfer is to disable the source server's outgoing provider:

1. Log in to the source Content Server instance as an administrator.
2. Go to the Administration page and click the **Providers** link.
3. Click the **Info** link of the appropriate outgoing provider on the Providers page.
4. In the Outgoing Provider Information page, click the **Disable** button.

C.3.3.2.2 Deleting a Transfer from the Transfer To Tab

To delete a transfer from the Transfer To tab, complete the following steps:

1. Log in to the source Content Server instance as an administrator.
2. Choose **Administration**, then **Archiver**. The Archiver utility starts.
3. Select **Options**, then **Open Archive Collection**.
4. Select the applicable collection from the list.
5. Click **Open**.
6. In the Archiver window, select the source archive in the Current Archives list.
7. Open the **Transfer To** tab.
8. Click **Remove** in the Transfer Destination section.
9. You are prompted to confirm the action.
10. Click **Yes**.

C.3.3.2.3 Deleting an Automated Transfer

To delete an automated transfer from the Automation for *Instance* page:

1. Log in to the source Content Server instance as an administrator.
2. Choose **Administration**, then **Archiver**. The Archiver utility starts.
3. Choose **Options**, then **View Automation For Instance**.
4. In the Automation For *Instance* window, open the **Transfers** tab.

5. Select the automated transfer to delete.
6. Click **Remove**. The automated transfer is removed from the list.

C.3.3.3 Verifying the Integrity of Transferred Files

Question

What is the best approach to verify the integrity of the files that have been transferred between two servers? Obviously, the documents in the target Content Server instance should be identical to those in the source instance. I need to ensure that all documents were in fact transferred and if some were not transferred, I must determine which ones failed to transfer.

Recommendation

To ensure that the transferred documents are identical to those on the source server, two items can easily be checked.

- **The Revisions table:**
Specifically, match the contents of the dDocName and dRevLabel columns on both instances and verify the accuracy or discrepancies between them.
- **The file system:**
Check the native file repository:
(DomainHome/ucm/cs/vault/content_type)
and web-viewable file repository:
(DomainHome/ucm/cs/weblayout/groups/public/documents/content_type)
on each server and verify the accuracy or discrepancies between them.

C.3.3.4 Transfer Process Is Not Working

Symptom

The transfer process is not setting up properly.

Recommendation

If the transfer process is not functioning correctly, check the outgoing provider on the source server and ensure that the information is correct. In particular, make sure that the server host name is correct and matches the HTTP server address.

To verify the server host name on the source server:

1. Start the System Properties utility:
`./SystemProperties`
2. Open the Internet tab.
3. Note the HTTP server address setting.
4. Go to the Administration page and click **Providers**.
5. Click the **Info** link for the appropriate outgoing provider on the Providers page.
6. In the Outgoing Provider Information page, check the server host name and make sure it corresponds exactly to the HTTP server address setting in System Properties.

7. If the server host name setting is different than the HTTP server address, click the **Edit** button.
8. Modify the **Server Host Name** setting as necessary.
9. Click **Update**.
10. Restart the Content Server instance.

C.3.4 Replication Issues

This section covers the following topic:

- [Stopping the Automatic Import Function](#)

C.3.4.1 Stopping the Automatic Import Function

Question

How can I stop the automatic import function?

Recommendation

When content meets the specified criteria, the automatic importer is, by default, configured to automatically perform an import every five minutes. However, there are two ways to disable the automatic import function:

- [Unregistering an Importer from the Replication Tab](#)
- [Deleting a Registered Importer from the Automation for Instance Page](#)

C.3.4.1.1 Unregistering an Importer from the Replication Tab

To unregister an importer from the Replication tab:

1. Log in to the source Content Server instance as an administrator.
2. Choose **Administration**, then **Archiver**.
The Archiver utility starts.
3. Select the archive in the Current Archives list.
4. Select the **Replication** tab.
5. Click **Unregister**.

The automatic import function is disabled from the selected archive.

C.3.4.1.2 Deleting a Registered Importer from the Automation for *Instance* Page

To delete a registered importer from the Automation for the *Instance* page:

1. Log in to the source Content Server instance as an administrator.
2. Choose **Administration**, then **Archiver**. The Archiver utility starts.
3. Choose **Options**, then **View Automation For Instance**.
4. In the Automation For Instance window, open the **Importers** tab.
5. Select the registered importer to delete.
6. Click **Remove**.

The registered importer is removed from the list.

C.3.5 Oracle Database Issues

This section covers the following topic:

- [Allotted Tablespace Exceeded](#)
- [Slow Oracle WebCenter Content Performance with Oracle Database](#)

C.3.5.1 Allotted Tablespace Exceeded

Symptom

I cannot transfer files. Every time I try to transfer files, I get 'max extents' error messages.

Problem

The following error messages (or similar) are issued:

```
IdcApp: Unable to execute query '<query_name>'. Error: ORA-01631: max # extents (50)
reached in table <table_name>.
ORA-01631 max # extents (<text_string>) reached in table <table_name>.
```

Recommendation

When the Content Server instance creates its database tablespace, it only allocates 50 extents. As the database grows and is re-indexed, it uses more space (extents). Eventually, the 50 extents limit is exceeded. At some point in the transfer, one of your files tried to extend past the 'max extents' limit. In this case, try implementing one or more of the following solutions:

- Look for weblayout queries that are excessively large, eliminate them, and retry your transfer.
- Perhaps a Content Server user does not have the right permission grants (resource and connect) to the Content Server schema. That user must have the temporary tablespace and default tablespace set to the Content Server defaults.
- If the system 'max extents' limit is less than the system maximum, you must increase the number of extents that are available. Refer to your Oracle Database documentation or ask your database administrator for the appropriate Oracle SQL command to increase the tablespace extents.
- You can optionally choose to re-create the database using larger initial, next or percent to grow parameters for the tablespaces. In this case, it is advisable to set the initial extents and next extents to 1Mb. Set the percent to grow parameter (PCTINCREASE) to 0% to allow the tables to automatically grow on an as-needed basis.

C.3.5.2 Slow Oracle WebCenter Content Performance with Oracle Database

Symptom

My Oracle WebCenter Content instance is running slow. I checked the memory and CPU usage of the application server and it has plenty of resources. What could be going wrong?

Recommendation

An Oracle WebCenter Content instance runs on an application server and relies on a database server on the back end. If your application server tier is running fine, chances are that your database server tier may host the root of the problem. While many things could cause

performance problems, on active Enterprise Content Management systems, keeping database statistics updated is extremely important.

Oracle Database has a set of built-in optimizer utilities that can help make database queries more efficient. It is strongly recommended to update or re-create the statistics about the physical characteristics of a table and the associated indexes in order to maximize the efficiency of optimizers. For more information, see:

<http://www.ateam-oracle.com/gathering-statistics-for-an-oracle-webcenter-content-database/>

C.3.6 Miscellaneous Issues

This section covers the following topics:

- [Archiving Does Not Work With Shared File System](#)
- [Archiving Does Not Work Over Outgoing Provider](#)

C.3.6.1 Archiving Does Not Work With Shared File System

Symptom

I am trying to transfer between two Content Server instances with access to a shared file system but it is not working.

Recommendation

When transferring between Content Server instances on a shared file system, the mapped or mounted drive must be available to both Content Server instances. This means that the computers must be on and logged in as a user who has system access to both Content Server instances. Make sure that all of the following conditions are met:

- Both computers are turned on.
- Both computers are logged in as a user with system access to both Content Server file systems.
- The shared drive has been properly mapped or mounted so the Content Server instance can 'see' it. Having network access to the computer is not sufficient.

C.3.6.2 Archiving Does Not Work Over Outgoing Provider

Symptom

I am trying to transfer between two Content Server instances over an outgoing provider but it is not working.

Recommendation

The Content Server instance that has an outgoing provider set up is considered the 'local' server, and the target Content Server instance for the outgoing provider is considered the 'proxied' server. Files are always transferred in the direction of the outgoing provider, from the local (source) instance to the proxied (target) instance.

It is possible that when the outgoing provider was added and defined for the source Content Server instance, the Proxied check box was selected. However, because the relative web root is the same for both Content Server instances, the outgoing provider is confused. The Proxied check box should be selected only if the target Content Server instance was installed as an

actual proxy of the local (master) Content Server instance. This server option should not be selected if the relative web root is the same for both Content Server instances.

C.4 Using My Oracle Support for Additional Troubleshooting Information

You can use My Oracle Support (formerly MetaLink) to help resolve Oracle Fusion Middleware problems. My Oracle Support contains several useful troubleshooting resources, such as:

- Knowledge base articles
- Community forums and discussions
- Patches and upgrades
- Certification information

 **Note:**

You can also use My Oracle Support to log a service request.

You can access My Oracle Support at <https://support.oracle.com>.