

## OpenText™ Documentum™ Content Management

### **Server Administration and Configuration Guide**

Manage repositories, connection broker, users and groups, storage areas, and security using the Documentum Server Manager utility or the command line interface.

EDCCS250400-AGD-EN-02

---

## **OpenText™ Documentum™ Content Management Server Administration and Configuration Guide**

EDCCS250400-AGD-EN-02

Rev.: 2026-Feb-04

This documentation has been created for OpenText™ Documentum™ Content Management CE 25.4.  
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product,  
on an OpenText website, or by any other means.

### **Open Text Corporation**

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111

Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440

Fax: +1-519-888-0677

Support: <https://support.opentext.com>

For more information, visit <https://www.opentext.com>

### **© 2026 Open Text**

Patents may cover this product, see <https://www.opentext.com/patents>.

### **Disclaimer**

#### **No Warranties and Limitation of Liability**

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However,  
Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the  
accuracy of this publication.

---

# Table of Contents

<b>1</b>	<b>Administration and configuration tools .....</b>	<b>11</b>
1.1	Introduction .....	11
1.2	Documentum Administrator .....	12
1.3	Documentum Server Manager .....	12
1.4	Tool suite .....	13
<b>2</b>	<b>Managing connection brokers .....</b>	<b>17</b>
2.1	Connection brokers .....	17
2.2	Connection broker initialization file .....	18
2.3	Connection broker projection targets .....	21
2.4	Server proximity .....	22
2.5	Restarting a connection broker .....	22
2.6	Adding a connection broker for one session .....	24
2.7	Implementing connection broker failover .....	24
2.8	Starting additional connection brokers .....	24
2.9	Shutting down connection brokers .....	26
2.10	Requesting connection broker information .....	27
<b>3</b>	<b>Managing Documentum CM Servers .....</b>	<b>29</b>
3.1	Documentum CM Servers .....	29
3.2	Starting a server .....	29
3.3	Managing Documentum CM Servers .....	30
3.4	server.ini file .....	44
3.5	Managing additional Documentum CM Servers .....	71
3.6	Managing Documentum CM Server in a virtual deployment .....	72
3.7	Server load balancing and failover .....	85
3.8	Shutting down a server .....	86
3.9	Clearing the server common area .....	87
3.10	Managing Tomcat .....	88
3.11	Server log files .....	89
3.12	dm_error utility .....	89
3.13	Improving performance on Oracle and PostgreSQL databases .....	90
<b>4</b>	<b>Managing repositories .....</b>	<b>91</b>
4.1	Repositories .....	91
4.2	Managing repositories .....	91
4.3	Adding repositories .....	117
4.4	Federations .....	118
<b>5</b>	<b>Managing sessions .....</b>	<b>121</b>
5.1	dfc.properties file .....	121

5.2	Managing connection requests .....	122
5.3	Defining the secure connection default for connection requests .....	123
5.4	Modifying the connection request queue size .....	124
5.5	Stopping a session server .....	124
<b>6</b>	<b>Managing Java Method Servers .....</b>	<b>125</b>
6.1	Java Method Servers .....	125
6.2	Java methods .....	130
6.3	Recording Java method output .....	131
6.4	Deploying Java methods .....	131
6.5	Adding additional servlets to Java Method Server .....	132
<b>7</b>	<b>Managing LDAP servers .....</b>	<b>133</b>
7.1	LDAP servers .....	133
7.2	LDAP certificate database management .....	149
<b>8</b>	<b>Managing MSA for OpenText Documentum CM services .</b>	<b>151</b>
8.1	Windows .....	151
8.2	Linux .....	155
<b>9</b>	<b>Managing OTDS authentication license server .....</b>	<b>157</b>
9.1	Overview .....	157
9.2	Configuring OTDS authentication in license server .....	157
9.3	Additional information .....	159
<b>10</b>	<b>OpenText Directory Services integration with Documentum CM Server .....</b>	<b>161</b>
10.1	Overview .....	161
10.2	Configuring OTDS integration with Documentum CM Server .....	161
10.3	Supported functions .....	162
10.4	Configuring OTDS authentication in Documentum CM Server .....	164
10.5	Authenticating OTDS users .....	165
10.6	Configuring OTDS as SAML service provider .....	165
10.7	Configuring OTDS for Kerberos SSO .....	165
10.8	Migrating LDAP users and groups as OTDS users and groups .....	166
10.9	Additional information .....	167
<b>11</b>	<b>Integration with Content Aviator services .....</b>	<b>169</b>
11.1	Overview .....	169
11.2	Content Aviator integration solution view .....	169
11.3	Prerequisites .....	170
11.4	Deploying and configuring Content Aviator components .....	171
11.5	Logging and tracing .....	175
11.6	Uninstalling Content Aviator components .....	176

<b>12</b>	<b>Distributed Content configuration .....</b>	<b>177</b>
12.1	Network locations .....	177
12.2	Accelerated Content Services servers .....	180
12.3	Branch Office Caching Services servers .....	187
12.4	Configuring distributed transfer settings .....	192
12.5	Messaging server configuration .....	192
<b>13</b>	<b>User management .....</b>	<b>195</b>
13.1	Administering users, groups, roles, and sessions .....	195
13.2	Users .....	196
13.3	Groups .....	211
13.4	Roles .....	218
13.5	Modules roles .....	221
13.6	Sessions .....	223
<b>14</b>	<b>Security and authentication .....</b>	<b>227</b>
14.1	Object permissions .....	227
14.2	Changing default operating system permits on public directories and files (Linux only) .....	230
14.3	Folder security .....	230
14.4	Additional access control entries .....	231
14.5	Default alias sets .....	232
14.6	Access evaluation process .....	232
14.7	Permission sets .....	234
14.8	Authenticating in domains .....	234
14.9	Principal authentication .....	235
14.10	Privileged clients .....	238
14.11	Administrator access sets .....	241
14.12	Managing authentication plug-ins, signatures, and encryption keys ..	245
14.13	Configuring two-man oversite .....	273
<b>15</b>	<b>Logging and tracing .....</b>	<b>275</b>
15.1	Introduction .....	275
15.2	Documentum CM Server logging and tracing .....	275
15.3	Foundation Java API logging .....	279
15.4	Foundation Java API tracing .....	279
<b>16</b>	<b>Audit management .....</b>	<b>291</b>
16.1	Auditing .....	291
16.2	Tracking external user transactions .....	292
16.3	Audit events .....	293
16.4	Audit trails .....	293
16.5	Audit properties .....	294

16.6	Events audited by default .....	294
16.7	Auditing by object type .....	296
16.8	Auditing by object instance .....	298
16.9	Auditing by events selected for all objects in the repository .....	299
16.10	Search audit .....	299
16.11	Audit policies .....	300
16.12	Registering audits .....	302
16.13	Adding, modifying, or removing audits .....	303
16.14	Verifying or purging audit trails .....	303
16.15	Interpreting audit trails of Foundation Java API method, workflow, and lifecycle events .....	303
16.16	Interpreting ACL and group audit trails .....	319
<b>17</b>	<b>Methods and jobs .....</b>	<b>323</b>
17.1	Methods .....	323
17.2	Method execution agents .....	328
17.3	Administration methods .....	329
17.4	Jobs .....	352
<b>18</b>	<b>Alias sets .....</b>	<b>451</b>
18.1	Alias sets and aliases .....	451
18.2	Creating or modifying alias sets .....	451
18.3	Viewing or removing aliases .....	452
18.4	Adding or modifying aliases .....	452
18.5	Deleting alias sets .....	453
<b>19</b>	<b>Formats .....</b>	<b>455</b>
19.1	Formats .....	455
19.2	Viewing, creating, or modifying formats .....	455
19.3	Deleting formats .....	457
<b>20</b>	<b>Types .....</b>	<b>459</b>
20.1	Object type categories and properties .....	459
20.2	Managing types .....	460
20.3	Creating or modifying types .....	461
20.4	Selecting a type .....	465
20.5	Deleting types .....	465
20.6	Viewing assignment policies .....	465
20.7	Converting types to shareable object types .....	466
20.8	Converting types to lightweight object types .....	466
20.9	Converting types to shareable and lightweight object types .....	466
<b>21</b>	<b>Storage management .....</b>	<b>467</b>
21.1	Storage management areas .....	467

21.2	Storage .....	467
21.3	Assignment policies .....	516
21.4	Migration policies .....	521
21.5	Orphaned content objects and files .....	526
21.6	Archiving and restoring documents .....	533
<b>22</b>	<b>InfoArchive integration with OpenText Documentum CM .</b>	<b>535</b>
22.1	Prerequisites .....	535
22.2	Setting up OpenText Documentum CM connector .....	536
22.3	Running archive job using Documentum Administrator .....	541
22.4	Cleaning archived objects .....	542
<b>23</b>	<b>Content delivery .....</b>	<b>543</b>
23.1	Content delivery services .....	543
23.2	Locating content delivery configurations .....	543
23.3	Creating or modifying content delivery configurations .....	544
23.4	Configuring the advanced properties of a content delivery configuration .....	546
23.5	Configuring replication properties for a content delivery configuration .....	549
23.6	Configuring extra arguments for a content delivery configuration .....	551
23.7	Deleting content delivery configurations .....	567
23.8	Testing content delivery configurations .....	567
23.9	Duplicating a content delivery configuration .....	567
23.10	Deactivating a content delivery configuration .....	568
23.11	Publishing objects .....	568
23.12	Content delivery configuration results .....	568
23.13	Content delivery logs .....	568
23.14	Effective labels .....	569
<b>24</b>	<b>Indexing management .....</b>	<b>571</b>
24.1	Indexing .....	571
24.2	Index agents and xPlore .....	571
24.3	Starting and stopping index agents .....	572
24.4	Disabling index agents .....	572
24.5	Enabling index agents .....	573
24.6	Verifying indexing actions .....	573
24.7	Viewing or modifying index agent properties .....	573
24.8	Managing index queue items .....	573
<b>25</b>	<b>OpenText Documentum Content Management (CM) Transformation Services management .....</b>	<b>577</b>
<b>26</b>	<b>Analytics management .....</b>	<b>579</b>

<b>27</b>	<b>Resource management .....</b>	<b>581</b>
27.1	Understanding resource management .....	581
27.2	Managing resource agents .....	581
27.3	Managing resource properties .....	582
<b>28</b>	<b>Cabinets, files, and virtual documents .....</b>	<b>585</b>
<b>29</b>	<b>API and DQL .....</b>	<b>587</b>
29.1	API and DQL .....	587
29.2	DQL editor .....	587
29.3	API tester .....	587
<b>30</b>	<b>Search .....</b>	<b>589</b>
30.1	Searches .....	589
30.2	Setting search preferences .....	589
30.3	Search guidelines .....	589
30.4	Running a simple search .....	590
30.5	Running an advanced search .....	593
30.6	Search results .....	593
30.7	Additional configuration options .....	593
30.8	Saved searches .....	594
30.9	Creating a search template .....	594
<b>31</b>	<b>Inbox .....</b>	<b>595</b>
<b>32</b>	<b>Workflows, work queues, and lifecycles .....</b>	<b>597</b>
32.1	Workflows .....	597
32.2	Work queue management .....	600
32.3	Lifecycles .....	601
32.4	References .....	601
<b>33</b>	<b>Performance and tuning .....</b>	<b>603</b>
33.1	Common problems with Documentum CM Server performance .....	603
33.2	Type caching .....	605
33.3	LDAP synchronization .....	606
33.4	Intelligent session management .....	611
33.5	Multiple workflows in Linux .....	613
<b>34</b>	<b>System events .....</b>	<b>615</b>
34.1	dm_default_set event .....	615
34.2	Foundation Java API events .....	615
34.3	Workflow events .....	622
34.4	Lifecycle events .....	625
34.5	Events sent to the fulltext user .....	626

34.6	Events related to jobs .....	626
<b>35</b>	<b>Populating and publishing the data dictionary .....</b>	<b>627</b>
35.1	Populating the data dictionary .....	627
35.2	Data dictionary population script .....	628
35.3	Publishing the data dictionary information .....	641
<b>36</b>	<b>High-availability support scripts .....</b>	<b>643</b>
36.1	Monitoring scripts .....	643
36.2	Processes not requiring a script .....	646
<b>37</b>	<b>Consistency checks .....</b>	<b>647</b>
37.1	General information .....	647
37.2	User and group checks .....	647
37.3	ACL checks .....	648
37.4	SysObject checks .....	649
37.5	Folder and cabinet checks .....	650
37.6	Document checks .....	651
37.7	Content object checks .....	651
37.8	Workflow checks .....	652
37.9	Object type checks .....	652
37.10	Data dictionary checks .....	653
37.11	Lifecycle checks .....	654
37.12	Object type index checks .....	654
37.13	Method object consistency checks .....	655
<b>38</b>	<b>Plug-in library functions for external stores .....</b>	<b>657</b>
38.1	General recommendations .....	657
38.2	dm_close_all .....	657
38.3	dm_close_content .....	658
38.4	dm_deinit_content .....	658
38.5	dm_init_content .....	658
38.6	dm_open_content .....	659
38.7	dm_plugin_version .....	660
38.8	dm_read_content .....	661
<b>39</b>	<b>Usage tracking .....</b>	<b>663</b>
39.1	Usage tracking .....	663



# Chapter 1

## Administration and configuration tools

### 1.1 Introduction

This guide contains administration and configuration information for OpenText™ Documentum™ Content Management Server. This guide is intended for system and repository administrators. The system administrator installs and owns the OpenText Documentum Content Management (CM) Server installation. The repository administrators owns and are responsible for one or more repositories. Readers should be familiar with the general principles of client/server architecture and networking. In addition, they should know and understand the Windows and Linux operating systems.

Documentum CM Server software manages the repository and provides content management capabilities. The repository consists of three main components: a file store containing the content assets, attribute tables within a relational database, and full-text indexes.

After Documentum CM Server is installed and running, typical system administration and configuration tasks include:

- Creating new repositories and maintaining existing repositories, including object types, methods, jobs, and alias sets
- Configuring, starting, and shutting down servers
- Maintaining connection brokers
- Managing content storage areas and content files
- Administering full-text indexes
- Managing users and groups
- Managing security
- Changing session configurations

The two main tools for administering and configuring Documentum CM Server are Documentum Administrator and Documentum Server Manager. Documentum Administrator is not included with Documentum CM Server.

Most administration and configuration tasks are typically done using Documentum Administrator. Some tasks have to be performed using Documentum Server Manager or the command line.

This guide provides instructions to administer and configure Documentum CM Server using the Documentum Server Manager or command line. For instructions to administer and configure Documentum CM Server using the Documentum

Administrator, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

## 1.2 Documentum Administrator

Documentum Administrator is the primary user interface for administration tasks. Documentum Administrator is a web-based interface for monitoring, administering, configuring, and maintaining OpenText Documentum Content Management (CM) repositories from any system running a web browser.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the information and instructions on the following:

- Logging in to Documentum Administrator
- Using the **System Information** page
- Determining the Documentum Administrator version
- Using the **Preferences** menu in Documentum Administrator

## 1.3 Documentum Server Manager

Documentum Server Manager is an administration tool added to the Windows Start menu during server installation on Windows. Documentum Server Manager is typically used to:

- Edit the `server.ini` file to change the Documentum CM Server configuration
- Uninstall a repository
- Start the Interactive Documentum Query Language (IDQL) utility
- Modify connection brokers
- Display connection broker log files
- Invoke the Documentum CM Server setup program to add or remove server components
- Invoke the Microsoft Performance Monitor tool
- Create a configuration summary report

### 1.3.1 Starting Documentum Server Manager

Documentum Server Manager is a Documentum CM Server administration tool only available on Windows.

**To start Documentum Server Manager:**

1. Log in to the Windows machine that is running Documentum CM Server.
2. Select Start > Documentum Server Manager.

## 1.4 Tool suite

Documentum CM Server includes various tools that automate regular administration tasks, such as files, monitoring storage space and database tables. The tools are implemented as jobs and most are installed in an inactive state. Documentum Administrator provides a graphical interface for defining, modifying, and monitoring the tools and their associated jobs.

The following table briefly describes the tools that are available:

**Table 1-1: OpenText Documentum CM tool suite**

Tool	Description
Archive	Automates archive and restore operations between content areas.
Audit Management	Deletes audit trail objects.
Consistency Checker	Checks the repository for consistency across a variety of object types.
Content Replication	Automates replication of document content for distributed file stores.
Content Storage Warning	Monitors disk space on the devices used to store content and index files. Queues a warning message when a disk used for content and index storage reaches a user-defined percentage of capacity.
Data Dictionary Publisher	Publishes data dictionary information to make it visible to users and applications.
Database Space Warning	Monitors the relational database management system (RDBMS). Queues a warning message when the RDBMS reaches a user-defined percentage of capacity.
	 <b>Note:</b> This tool is not installed for installations running against Microsoft SQL Server.

Tool	Description
Dm_LDAPSynchronization	Determines all changes in the Lightweight Directory Access Protocol (LDAP) directory server information and propagates the changes to the repository.
Dmclean	Automates the dmclean utility, which removes orphaned content objects, notes, ACLs, and SendToDistribution workflow templates from a repository.
Dmfilescan	Automates the dmfilescan utility, which removes orphaned content files from a specified storage area of a repository.
Dmextfilescan	Removes orphaned content files from S3 and S3-compatible stores. For more information about the dmextfilescan utility, see <a href="#">"dmextfilescan utility" on page 532</a> .
Distributed Operations	Performs the distributed operations necessary to manage reference links. This is an internal job that is installed as part of the tool suite. For more information about the job, see <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> .
File Report Utility	Provides a report to help restore deleted or archived document content using file system backups. This method only applies to distributed storage areas.
Group Rename	Renames a group in the repository.
Index Agent Startup	Starts the index agent.
Log Purge	Deletes log files for the server, session, connection broker, and agent and the trace log files resulting from method and job executions.
Queue Management	Deletes dequeued objects in the dmi_queue_item tables.
Remove Expired Retention Objects	Removes objects with an expired retention date, if they are stored in a Centera storage area.
Rendition Management	Removes of unwanted document renditions.
State of the Repository Report	Provides information about the repository status.
Swap Info	Reports on swap space availability and usage.
ToolSetup	Installs system administration tools.

Tool	Description
Update Stats	Updates stored statistics on the underlying RDBMS tables, to aid in query performance.
User Chg Home Db	Changes the user home repository.
User Rename	Changes a user name in the repository.
Version Management	Removes of unwanted document versions.

For more information, see “[Jobs](#)” on page 352.



## Chapter 2

# Managing connection brokers

## 2.1 Connection brokers

The connection broker is a process that provides client sessions with connection information, such as IP addresses and port numbers. The connection brokers that handle a client connection request are defined in the dfc.properties file of the client. By default, each Documentum CM Server installation must have one connection broker. The first connection broker is started as part of the installation process.

When a client contacts the connection broker, the connection broker sends back the IP address and port number of the server host. If there are multiple servers for the repository, the connection broker returns connection information for all of them. The client session then uses that information to choose a server and open the connection. Clients can request a connection through a particular server, any server on a particular host, or a particular server on a specified host.

The dfc.properties file contains most of the configuration parameters for handling sessions. For example, the file contains keys that identify which connection brokers are used to obtain a session, specify how many sessions are allowed for one user, and enable persistent client caching. Many keys have default values, but an administrator or application must explicitly set some of the keys. For more information, see “[dfc.properties file](#)” on page 121.

The standard connection broker that comes with a Documentum CM Server installation can be customized to meet more specific requirements, such as:

- Protection against being shut down by an unauthorized person
- A list of servers that can access the connection broker
- IP listening addresses to run multiple connection brokers
- Connection requests from outside a firewall

These options are configured in the connection broker initialization file. Both, the dfc.properties file and the connection broker initialization file cannot be modified using Documentum Administrator.

When Documentum CM Server is started, it automatically broadcasts information about itself. Each connection broker that receives the broadcast adds the server to its registry, or list of known servers. Documentum CM Server sends the first broadcast before it is fully initialized, and the connection broker sets the server status to *starting*. As soon as Documentum CM Server is fully initialized and ready to service clients, it broadcasts a checkpoint message. The receiving connection brokers update the server status to *open*.

Documentum CM Server broadcasts a checkpoint message at regular intervals. By default, the checkpoint interval is five minutes. If the connection broker does not receive a checkpoint message, it modifies the server status to *presumed down*. A connection broker keeps the entry for a non-broadcasting server for a specified time, called the `keep_retry` interval. Both, the checkpoint interval and the `keep_retry` interval are specified in the server configuration object, as described in “[General server configuration properties](#)” on page 33.

A connection broker deletes a Documentum CM Server from its list of known servers when:

- A server sends a delete me message as a result of a manual shutdown using the shutdown method.
- A server fails to broadcast a checkpoint message within the expected `keep_entry` interval.

For example, a server is not active as a result of a shutdown without a delete me message, a crash, or when the network between the server and connection broker fails.

- A server is reinitialized after a change to the projection targets in the server configuration object that deletes the connection broker from the targets.

## 2.2 Connection broker initialization file

The connection broker initialization file is an optional connection broker configuration file. The initialization file can have any valid file name. You can store the file in any location, but the most convenient place is the same directory in which the `dm_launch_docbroker` script is stored.

The initialization file is a plain text file and has the following format:

```
[SECURITY]
password = string_value
allow_hosts=host_name_list|deny_hosts=host_name_list

[DOCBROKER_CONFIGURATION]
host = host_name|IP_address_string
service = service_name
port = port_number
keystore_file=broker.p12
keystore_pwd_file=broker.pwd
cipherlist=AES128-SHA
secure_connect_mode=native or secure or dual

[TRANSLATION]port=["]outside_firewall_port=inside_firewall_port
{,outside_firewall_port=inside_firewall_port}["]
host=["]outside_firewall_ip=inside_firewall_ip
{,outside_firewall_ip=inside_firewall_ip}["]
```



**Note:** The password key in the [SECURITY] section is only valid on Linux. Connection brokers on Windows do not use the security password. The port translation strings are enclosed in double quotes when multiple ports or hosts are specified.

If the initialization file includes a valid service name, the connection broker is started with the service name. If the initialization file does not provide a service name, but a

valid port number, the connection broker is started using the port number. If a service name or a port number is not included, the connection broker is started on port 1489.

### 2.2.1 Invoking the initialization file

When you start a connection broker, the initialization file is not automatically invoked. To invoke the file, include the `-init_file` argument on the startup command line.

For Windows, the syntax is:

```
<drive>:\documentum\product\<version_number>\bin\dmdbroker.exe  
-init_file <filename>
```

If the connection broker is running as a service, edit the service entry to include the argument on the command line. You can use the Documentum Server Manager to edit the service entry.

For Linux, the syntax is:

```
% dm_launch_docbroker -init_file <filename>
```

If there are other arguments on the command line in addition to the initialization file argument, the `-init_file` argument must appear first or it is ignored.

### 2.2.2 Configuring shutdown security (Linux only)

Defining a security password for a connection broker ensures that only a user who knows the password can stop the connection broker. Define a password in the [SECURITY] section with the password key:

```
[SECURITY]  
password=<string_value>
```

### 2.2.3 Restricting server access

By default, a connection broker accepts broadcasts from any server. However, you can configure a connection broker to either:

- Accept broadcasts only from specified servers
- Reject broadcasts from specified servers

To define accepted servers, use the following format in the initialization file:

```
[SECURITY]  
...  
allow_hosts=<host_name_list>
```

To define rejected servers, use the following format:

```
[SECURITY]  
...  
deny_hosts=<host_name_list>
```

<host\_name\_list> is a list of the host machines on which the servers reside. Separate multiple host names using commas. For example:

```
[SECURITY]
...
deny_hosts=<bigdog,fatcat,mouse>
```

The options are mutually exclusive. For each connection broker, you can configure either the accepted servers or the rejected servers, but not both.

## 2.2.4 Certificate-based SSL configuration

Use these parameters to enable certificate-based Secure Sockets Layer (SSL):

- keystore\_file: Keystore containing the connection broker certificate and private key
- keystore\_pwd\_file: File containing the plain-text or encrypted keystore password
- Cipherlist: List of ciphers separated using ":"

For more information about certificate-based SSL configuration, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

## 2.2.5 Supported connection broker connection modes

This section lists the supported connection modes for connection broker.

- Native: Connections are in the raw remote procedure call (RPC) format without any encryption
- Secure: SSL mode is:
  - used with anonymous ciphers (ADH:DEFAULT)
  - used with certificates
- Dual: Connections are both in the raw RPC format without any encryption and SSL mode is used with anonymous ciphers (ADH:DEFAULT) and certificates

## 2.2.6 Translating IP addresses

For security reasons, many enterprises set up firewalls to prevent outside users from accessing enterprise repositories and file systems.

To allow a user or client application outside the firewall to connect to a repository inside the firewall, the connection broker initialization file includes a [TRANSLATION] section. This section redirects a request to a safe IP address and port name. The section has the following format:

```
[TRANSLATION]port=["outside_firewall_port=inside_firewall_port
{,outside_firewall_port=inside_firewall_port}"]
host=["outside_firewall_ip=inside_firewall_ip
{,outside_firewall_ip=inside_firewall_ip}"]
```

where

<outside\_firewall\_port> and <inside\_firewall\_port> are port numbers.

<outside\_firewall\_ip> and <inside\_firewall\_ip> are IP addresses.

For example, suppose repository A is inside a firewall and that application B, outside the firewall, wants to connect to repository A. Also suppose the connection broker that receives the request has the following TRANSLATION section in its initialization file:

```
[TRANSLATION]
port=2231=4532
host=2.18.13.211=172.18.23.257
```

When the connection broker receives the request, it translates 4532 to 2231 and 172.18.23.257 to 2.18.13.211. It sends the values 2231 and 2.18.13.211 back to application B, which uses them to establish the connection.

If you specify multiple ports or hosts for translation, enclose the translation string in double quotes. For example:

```
[TRANSLATION]
port= "2253=6452,2254=6754 "
```

#### To use a [TRANSLATION] section:

1. Define the IP address translation rules in the firewall.
2. Enter the rules in the [TRANSLATION] section of the connection broker initialization file.
3. Restart the connection broker, specifying the initialization file on the command line.

## 2.3 Connection broker projection targets

Active Documentum CM Servers must regularly broadcast, or project, connection information to at least one connection broker. Server broadcasts are called *checkpoints*. The connection brokers receiving the checkpoints are called *connection broker projection targets*.

Connection broker projection targets are defined in the server configuration object. The Documentum CM Server installation procedure defines one connection broker projection target in the server.ini file. The target is the connection broker that is specified during the installation procedure. When the installation procedure is complete, the target definition can be moved to the server configuration object.

For more information, see “[Creating or modifying connection broker projections](#)” on page 39.

## 2.4 Server proximity

Documentum CM Servers send a proximity value to each connection broker projection target. The proximity value represents physical proximity of the server to the connection broker. By default, clients connect to the server with the smallest proximity value since that server is the closest available server. If two or more servers have the same proximity value, the client makes a random choice between the servers.

The proximity values should reflect the topology of a Documentum CM Server installation. For example, an installation with three servers and one connection broker, the server closest to the connection broker projects the lowest proximity value. The server farthest from the connection broker projects the highest proximity value.

The server proximity value is specified in the network location section of the server configuration object, as described in “[Creating or modifying network locations](#)” [on page 39](#).

An individual server that has multiple connection broker projection targets can project a different proximity value to each target. Guidelines for setting proximity values are:

- Proximity values should have a value of 1 to 999, unless the Documentum CM Servers are in a distributed configuration.
- Any server with a proximity value of 9000 to 9999 is considered a Documentum CM Server and typically only handles content requests.
- For values from 1001 through 8999, the first digit is ignored and only the last three digits are used as the proximity value. For example, if for a proximity value of 8245, clients ignore the 8 and only consider 245 the proximity value.
- On Windows, proximity values of 10,000 and more represent servers in another domain. Users who want to connect to such servers must specify the server by name in the Connect command line.

## 2.5 Restarting a connection broker

On Windows, a connection broker can either be started as a service or from the command line. On Linux, a connection broker is always started from the command line.

## 2.5.1 Restarting a connection broker running as a Windows service

Double-click **Start connection broker** in the OpenText Documentum CM group.



**Note:** The syntax of the connection broker service name is Documentum Docbroker Service <connection\_broker\_name> where <connection\_broker\_name> is the name of the connection broker. The default service name is Documentum Docbroker Service Docbroker.

## 2.5.2 Restarting a connection broker that is not running as a Windows service

At the operating system prompt, enter the startup command line.

The syntax for the startup command is:

```
dmdocbroker.exe [-init_file <filename>] -host <host_name>  
-service <service_name> -> port <port_number>
```

For example:

```
d:\document\product\6.0\bin\dmdocbroker.exe  
-init_file DocBrok.ini -host engr -service engr_01
```

## 2.5.3 Restarting a connection broker on Linux

1. Log in to the machine on which to start the connection broker.
2. Change to the \$DOCUMENTUM/dba directory:

```
% cd $DOCUMENTUM/dba
```

3. At the operating system prompt, type the command line for the dm\_launch\_docbroker utility. The command-line syntax is:

```
dm_launch_docbroker [-init_file <file_name>] [-host <host_name>] [-service  
<service_name>] [-port <port_number>]
```

Include the host name and a service name or port number to identify the connection broker. Otherwise specify an initialization file that includes a [DOCBROKER\_CONFIGURATION] section to identify the connection broker.

## 2.6 Adding a connection broker for one session

Documentum Administrator obtains connection information from the connection broker referenced in the dfc.properties file of the Documentum Administrator installation. You cannot modify the dfc.properties file using Documentum Administrator. If you have system administrator or superuser privileges, you can add connection brokers for an active session by storing connection broker information in a cookie. However, the repositories of that connection broker can only be accessed during the current session.

For more information about adding a connection broker for a session, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

## 2.7 Implementing connection broker failover

Failover for connection information requests from a client is implemented by listing multiple connection brokers in the dfc.properties file. In addition, the value of the dfc.docbroker.auto\_request\_forward key in the dfc.properties file must be set to T.

By default, the first connection broker listed in the file handles the connection request. If that connection broker does not respond within 15 seconds or less, the request is forwarded to the next connection broker that is listed in the dfc.properties file. The request is forwarded sequentially until a connection broker responds successfully or until all connection brokers defined in the file have been tried. If there is no successful response, the connection request fails.

## 2.8 Starting additional connection brokers

A repository can have multiple connection brokers. The connection brokers can run on separate machines or on the same machine. With multiple connection brokers on the same machine, each connection broker on the machine must use a separate port or a separate network card.

Configuring a connection broker to use a separate port, requires defining a services file entry that identifies the service name for the connection broker. The service name for the connection broker must be unique among the service names.

Alternatively, you can create an initialization file that identifies the service. For example:

```
[DOCBROKER_CONFIGURATION]
host=<host_machine_name>
service=<service_name>
```

or

```
[DOCBROKER_CONFIGURATION]
host=<host_machine_name>
port=<port_number>
```

where <port\_number> is the port identified in the new service.

To configure a connection broker to use a separate network card, create an initialization file for the connection broker. The file must include a

[DOCBROKER\_CONFIGURATION] section to identify the IP address of the network card. Use the following format:

```
[DOCBROKER_CONFIGURATION]
host=<IP_address_string>
service=<service_name>
port=<port_number>
```

<IP\_address\_string> must be in the dotted decimal format (for example, 143.23.125.65).

The service name is the connection broker service name, defined in the host machine services file. The port number is the port defined in the service. For more information about setting up service names, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*. If you include a service name, the connection broker is started using that service. Otherwise, if you include a port number, the connection broker is started using that port. If you do not include a service name or a port number, the connection broker uses port number 1489.

### To start additional connection brokers:

1. Start the connection broker from the operating system prompt.

- On Windows:

```
d:\documentum\product\<version>\bin\dmdbroker.exe
[-init_file <filename>] -host <host_name> -service <service_name>
```

- On Linux:

```
dm_launch_docbroker [-init_file <filename>] -host <host_name>
-service <service_name>
```

Include the host name and a service name or port number to identify the connection broker. Otherwise, specify an initialization file that includes a [DOCBROKER\_CONFIGURATION] section to identify the connection broker.

2. Modify the projection properties in the server configuration object to add the new connection broker as a server projection target.
3. Optionally, modify the server.ini file to add the new connection broker as a server projection target.
4. Reinitialize the server.

## 2.9 Shutting down connection brokers

The connection broker shutdown procedure varies, depending on whether the connection broker runs on Windows or Linux. The shutdown procedure also depends on whether the connection broker was started as a service or from the command line.

If the connection broker was configured with shutdown security, supply the correct password to shut down the connection broker.

### 2.9.1 To stop a connection broker running as a service on Windows

1. Click **Start > Program Files > Documentum > Server Manager**.
2. Select the connection broker tab.
3. Select the correct connection broker.
4. Click **Stop**.

### 2.9.2 To stop a connection broker started from the Windows command line

Close the window in which the connection broker is running.

### 2.9.3 To stop a connection broker on Linux

Execute the dm\_stop\_docbroker utility on the command line:

```
% dm_stop_docbroker [-P<password>] [-B[atch]]  
[-N<port_number>] [-S<service_name>]
```

The utility stops the connection broker that is running on the host specified in the dmshutdown script. That connection broker was specified during the initial server installation. If you are executing the dm\_stop\_docbroker utility in interactive mode (without the -B flag), the utility displays which connection broker it intends to stop and prompts for a confirmation. If you include the -B flag, the utility does not prompt for confirmation or display which connection broker it is stopping. The default for the -B flag is FALSE.

If you have multiple connection brokers on one machine, you can include the -N and -S arguments to identify a particular connection broker to shut down.

The <password> is the password specified in the connection broker initialization file. For more information about connection broker security, see “[Configuring shutdown security \(Linux only\)](#)” on page 19. If the connection broker initialization file contains a password, supply this password to stop the connection broker.

If you cannot use the dm\_stop\_docbroker utility, you can use the Linux kill command to stop the connection broker if it was started without security. If you do

not know the process ID for the connection broker, you can obtain it using the Linux ps command. You cannot use the Linux kill command to stop a connection broker that was started with security. Only the Linux kill -9 command stops a secured connection broker.

### 2.9.3.1 Stopping multiple connection brokers on Linux

If you have multiple connection brokers, stop two or more by editing the dm\_stop\_docbroker script before running the dm\_stop\_docbroker utility. The script resides in the \$DOCUMENTUM/dba directory. The last line in this script contains the connection broker host name that is stopped when the dm\_stop\_docbroker utility runs:

```
./dmshutdown docbroker -Tlapdog -P$password $@  
# lapdog is the host name
```

To stop multiple connection brokers, add a line one for each host on which a connection broker resides to the script. For example, connection brokers are running on hosts named lapdog, fatcat, and mouse. To stop all three connection brokers, edit dm\_stop\_docbroker to include these three lines:

```
./dmshutdown docbroker -Tlapdog -P$password $@  
#lapdog is the host name  
  
./dmshutdown docbroker -Tfatcat -P$password $@  
#fatcat is the host name  
  
./dmshutdown docbroker -Tmouse -P$password $@  
#mouse is the host name
```

If all connection brokers use the same password, the dm\_stop\_docbroker utility substitutes the password specified on the command line for \$password in the script. If each connection broker requires a different password, add the password for each connection broker in the script:

```
./dmshutdown docbroker -Tlapdog -Pbigbark $@  
#lapdog is the host name  
  
./dmshutdown docbroker -Tfatcat -Pmeowmeow $@  
#fatcat is the host name  
  
./dmshutdown docbroker -Tmouse -Psqueak $@  
#mouse is the host name
```

## 2.10 Requesting connection broker information

To obtain information about servers or repositories associated with a particular connection broker, or which connection broker a client can access, use the following methods:

- `getServermap`: Returns information about associated servers for a particular connection broker.

The `IDfDocbrokerClient.getServerMap` method returns the non-persistent server locator object. The server information appears at corresponding index positions in the repeating properties of the object. For example, the name of the host machine for the server named in `r_server_name[0]` is specified in `r_host_name[0]`.

The process ID is specified in `r_process_id[0]`, and the status is specified in `r_last_status[0]`.

For more information about the server locator object, see *OpenText Documentum Content Management - Server System Object Reference Guide* (EDCCS250400-ORD).

- `getDocbaseMap`: Returns information about associated repositories for a particular connection broker.

The `IDfDocbrokerClient.getDocbaseMap` method returns the non-persistent repository locator object. The repository information appears at corresponding index positions in the repeating properties. For example, the name of the repository whose ID is in `r_docbase_id[3]` is found in `r_docbase_name[3]` and its description is found in `r_docbase_description[3]`.

For more information about the repository locator object, see *OpenText Documentum Content Management - Server System Object Reference Guide* (EDCCS250400-ORD).

- `getDocbrokerMap`: Returns a list of connection brokers a client can access.

The `IDfTypedObject.getDocbrokerMap` method returns the non-persistent docbroker locator object.

The information for a single connection broker appears at corresponding index positions in the repeating properties. For example, the values at `network_protocol[2]`, `host_name[2]`, `port_number[2]`, and `time_out[2]` describe one connection broker.

The method is also useful when sending a `getDocbaseMap` or `getServerMap` method to a particular connection broker to find the protocol, host name, and port number values for the connection broker.

For more information about the docbroker locator object, see *OpenText Documentum Content Management - Server System Object Reference Guide* (EDCCS250400-ORD).

- Query the client config object.

Each client session references a non-persistent client config object for configuration information. The client object properties are populated from the keys of the `dfc.properties` file. Any key value specified in the file is reflected in the client config object.

The keys in the `dfc.docbroker` category contain information about the connection brokers in the properties file is contained in the keys with the category `dfc.docbroker`. For example, a `dfc.docbroker.host` key identifies a connection broker host and a `dfc.docbroker.port` key identifies a connection broker port.

The repeating properties of the client config object use the same names as the keys in the `dfc.properties` file. For example, connection broker hosts are found in the `dfc.docbroker.host` property.

## Chapter 3

# Managing Documentum CM Servers

## 3.1 Documentum CM Servers

A Documentum CM Server is a process that provides client access to the repository. Documentum CM Servers receive queries from clients in the form of OpenText™ Documentum™ Content Management Foundation Java API methods or Documentum Query Language (DQL) statements and make the actual call to the underlying RDBMS or the file directories. Every repository must have at least one active Documentum CM Server. If a repository does not have an active server, users cannot access that repository.

The default Documentum CM Server installation starts one Documentum CM Server for a repository. However, a repository can have more than one Documentum CM Server. If a repository is very active, serving many users, or its users are widely spread geographically, multiple servers can provide load balancing and enhance performance. For more information, see [“Adding or modifying Documentum CM Servers” on page 31](#).

Repositories are comprised of object type tables, type indexes, and content files. The type tables and type indexes are tables in an underlying relational database. The content files are typically stored in directories on disks in a given installation. However, content files can also be stored in the database, in a retention storage system such as Centera or NetApp SnapLock, or on external storage devices.

A full-text index is associated with a particular repository or, in a consolidated deployment, with all repositories indexed by a xPlore installation. Full-text indexes enable rapid searching for designated values or strings in content files and property values.

## 3.2 Starting a server

Documentum CM Server can only be started or restarted using Documentum Server Manager or a startup script.

### To restart a server using Documentum Server Manager (Windows):

1. Log into the machine where Documentum CM Server is installed as the OpenText Documentum CM installation owner.
2. Navigate to **Start > Programs > Documentum > Documentum Server Manager**.
3. Click the **DocBroker** tab, select a connection broker, then click **Start**.
4. Click the **Repository** tab, select a repository, then click **Start** to start Documentum CM Server.

5. Click **Start > Programs > Administrative Tools > Services**.
6. Right-click **Documentum Java Method Server** in the Services list, then click **Start** to start the Java Method Server.

**To restart a server using the startup script (Linux):**

1. Log into the machine where Documentum CM Server is installed as the OpenText Documentum CM installation owner.
2. Run the \$Documentum/dba/dm\_launch/<docbrokerName> script to start the connection broker, where <docbrokerName> is the name of the connection broker.  
Change to the \$DOCUMENTUM/dba directory.
3. Run the dm\_start\_<repositoryname> script that references the server to start.  
The dm\_start\_<repositoryname> script checks that a log directory is defined for the installation, copies any existing log file to a new location, and starts the server. The script has an optional argument, -oclean, that removes the files in the server common area if the argument is included it in the command line.
4. Navigate to the %DM\_JMS\_HOME%\bin\startMethodServer.cmd and run the startMethodServer.sh script to start the application server.

### 3.3 Managing Documentum CM Servers

The default Documentum CM Server installation creates a repository with one server. In Documentum Administrator, administrators can configure additional servers to run against a particular repository.

Each Documentum CM Server is associated with a server configuration object. A server configuration object is a template for a Documentum CM Server. A server configuration is defined by the properties in the associated server configuration object and the parameters in the server.ini file that is read during server startup. At startup, a server always reads the CURRENT version of its server configuration object.

All server configuration objects for the current repository are listed on the Documentum CM Server configuration page in Documentum Administrator, as described in “[Server configuration object information](#)” on page 31.

Server configuration objects are stored in the repository System cabinet. You can add Documentum CM Servers by creating multiple server configuration objects, as long as they are uniquely named. You can also modify a server configuration object and save it as a new object.



**Note:** For more information about creating, starting, and stopping a remote Content Server, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

**Table 3-1: Server configuration object information**

<b>Column</b>	<b>Description</b>
<b>Name</b>	The name of the server configuration object.
<b>Host</b>	The name of the host on which the Documentum CM Server associated with the server configuration object is running.
<b>Operational Status</b>	<p>The current running status and dormancy status separated by a comma of the Documentum CM Server. Valid values are:</p> <p>Running Status:</p> <ul style="list-style-type: none"> <li>• <b>Running</b></li> <li>• <b>Unknown</b></li> </ul> <p>Dormancy Status:</p> <ul style="list-style-type: none"> <li>• <b>Dormancy Requested</b></li> <li>• <b>Projected Dormancy</b></li> <li>• <b>Dormant</b></li> <li>• <b>Active</b></li> <li>• <b>Invalid</b></li> </ul> <p> <b>Note:</b> The Operational Status column will display only the current running status for Documentum CM Server versions prior to 7.0.</p>
<b>Version</b>	The version of the server configuration object.

### 3.3.1 Adding or modifying Documentum CM Servers

The **Server Configuration list** page in Documentum Administrator lists the server configuration objects of all Documentum CM Servers for the current repository. Each Documentum CM Server has a server configuration object in the repository.

**Table 3-2: Server configuration properties tabs**

<b>Tab</b>	<b>Description</b>
<b>Info</b>	Select the <b>Info</b> tab to view or modify information on the server host, the operating system on which the server is running, code pages and locales, and other general information.
<b>Connection Brokers</b>	Select the <b>Connection Brokers</b> tab to view or modify connection broker projections.

Tab	Description
<b>Network Locations</b>	Select the <b>Network Locations</b> tab to view or modify the proximity values for the associated network locations.
<b>App Servers</b>	Select the <b>App Servers</b> tab to add an application server for Java method execution.
<b>Cached Types</b>	Select the <b>Cached Types</b> tab to specify which user-defined types are to be cached at server startup.
<b>Locations</b>	Select the <b>Locations</b> tab to view the locations of certain files, objects, and programs that exist on the server host file system, including the assume user program, change password program, log file.
<b>Far Stores</b>	Select the <b>Far Stores</b> tab to view accessible storage areas and to designate far stores. A server cannot store content in a far store. For more information about far stores, see <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> .

For more information about adding or modifying Documentum CM Servers, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.2 Duplicating a server configuration object

You can create a server configuration object using an existing server configuration object as a template. Create a server configuration object when you run additional servers against a repository, whether on the same host or a different host.

For more information about duplicating a server configuration object, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.3 Modifying general server configuration information

You can create or modify the general server information, such as the server host, the operating system on which the server is running, code pages and locales.

**Table 3-3: General server configuration properties**

<b>Field</b>	<b>Value</b>
<b>Name</b>	The name of the initial server configuration object created. By default, the server configuration object has the same name as the repository. When you create a new server configuration object, you assign it a new name.
<b>Host Name</b>	The name of the host on which the server is installed. Read-only.
<b>Server Version</b>	The version, operating system, and database of the server defined by the server configuration object. Read-only.
<b>Process ID</b>	The process ID of server on its host. Read-only.
<b>Install Owner</b>	The OpenText Documentum CM installation owner. Read-only.
<b>Install Domain</b>	On Windows, the domain in which the server is installed and running. Read-only.
<b>Trusted Mode</b>	Indicates if OpenText™ Documentum™ Content Management Trusted Content Services is available. Read-only.
<b>Dormancy Status</b>	Indicates the dormancy status of Documentum CM Server.   <b>Note:</b> The Dormancy Status label is only visible for 7.0 and later versions of Documentum CM Server.
<b>Update Configuration Changes</b>	
<b>Re-Initialize Server</b>	Select to reinitialize the server after the server configuration object is saved.
<b>Configuration Changes</b>	
<b>Web Server Location</b>	The name of the web server host and its domain. Used by client applications for creating DRLs.
<b>Web Server Port</b>	Identifies the port the web server uses. The default is 80.

Field	Value
<b>Agent Launcher</b>	<p>Defines the method that launches the agent exec process. The default value is agent_exec_method.</p> <p>The agent_exec_method is created when you install Documentum CM Server. Its name is stored in the agent_launcher property of the server configuration object. It polls jobs that contain scheduling information for methods. Jobs are launched by the agent_exec process.</p> <p>To disable all job execution, leave this field empty.</p> <p>Click the <b>Select Agent Launcher Method</b> link to access the Choose a method page.</p>
<b>Operator Name</b>	<p>The name for the repository operator if the repository operator is not explicitly named on the dmarchive.bat command line or in the Archive or Request method. This must be manually configured. The default is the owner of the server configuration object (the repository owner).</p> <p>The repository operator is the user whose Inbox receives all archive and restore requests.</p> <p>Click the <b>Select Operator</b> link to access the Choose a user page.</p>
<b>Server Cache Size</b>	The maximum number of objects allowed in the server cache. The default is 200.
<b>Client Cache Size</b>	The maximum permitted size of the client cache, expressed as the number of objects. The default is 50.
<b>Network File Share</b>	Indicates whether the server is using Network File Share for file sharing.
<b>Checkpoint Interval</b>	Defines the interval at which the server broadcasts service information to connection brokers. The unit of measurement is seconds. The default is 300 seconds.
<b>Keep Entry Interval</b>	<p>Specifies how long each connection broker keeps a server entry if the connection broker does not receive checkpoint broadcasts from the server. This time limit is included in the broadcast information of server.</p> <p>By default, the value is 1,440 minutes (24 hours).</p>

Field	Value
<b>Locale Name</b>	<p>Indicates the server locale.</p> <p>The value is determined during server installation.</p>
<b>Default Client Codepage</b>	<p>The default codepage for clients. The value is determined programmatically and is set during server installation. In general, it does not need to be changed.</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>• UTF-8</li> <li>• ISO_8859-1</li> <li>• Shift_JIS</li> <li>• EUC-JP</li> <li>• EUC-KR</li> <li>• US-ASCII</li> <li>• ISO_10646-UCS-2</li> <li>• IBM850</li> <li>• ISO-8859-8</li> </ul>
<b>Server OS Codepage</b>	<p>The code page used by the operating system of the machine on which the server resides. The value is determined programmatically and is set during server installation. In general, this value is not changed.</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>• UTF-8</li> <li>• ISO_8859-1</li> <li>• Shift_JIS</li> <li>• EUC-JP</li> <li>• EUC-KR</li> <li>• US-ASCII</li> <li>• ISO_10646-UCS-2</li> <li>• IBM850</li> <li>• ISO-8859-8</li> </ul>
<b>Turbo Backing Store</b>	<p>The name of the file store storage area where the server puts renditions generated by indexing blob and turbo content. The default is filestore_01.</p>
<b>Rendition Backing Store</b>	<p>The name of the file store storage area where the server will store renditions generated by full-text indexing operations.</p>

Field	Value
<b>Modifications Comments</b>	Remarks on changes made to the server configuration object in this version.
<b>SMTP Server</b>	<p>The name of the computer hosting the SMTP Server that provides mail services to Documentum CM Server.</p> <p>The value is provided during the Documentum CM Server installation.</p> <p> <b>Note:</b> From the 22.4 release, Documentum CM Server provides SMTP config object that can be modified only using IAPI/IDQL or OpenText Documentum Content Management (CM) Foundation Java API and not using Documentum Administrator. For more information about SMTP configuration, see <i>OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)</i>.</p>
<b>Workflow Agent Worker Threads</b>	The number of workflow agent worker sessions. The maximum value is 1000. The default value is 3. Setting this to 0 disables the workflow agent.
<b>Secure Connect Mode</b>	<p>Specifies whether type of connection the server accepts. Options are:</p> <ul style="list-style-type: none"> <li>• Dual: Uses encrypted and non-encrypted connections.</li> <li>• Native: Uses non-encrypted connections only.</li> <li>• Secure: Uses encrypted connections only.</li> </ul> <p>If you change the mode, you must restart the server. Re-initializing the server does not suffice.</p>
<b>Maximum Content Migration Threads</b>	<p>Defines a valid value range for the argument PARALLEL_DEGREE for parallel content migration when running MIGRATE_CONTENT administration method or setting up a migration policy rule. Valid values are between 1 and 128.</p> <p>This option requires Content Storage Services on Documentum CM Server.</p>

Field	Value
<b>System Shutdown Timeout</b>	<p>The time in seconds that the workflow agent attempts to shut down work items gracefully after receiving a shutdown command. The default value is 120 seconds.</p> <p>When the timeout value expires, the server takes over and shuts down the workflow agent. This feature is only applicable for repositories that use multiple Documentum CM Servers.</p> <p>If the timeout period is exceeded (or is set to zero), Documentum CM Server takes over and shuts down the workflow agent immediately.</p> <p>If the timeout period is a negative value, Documentum CM Server waits for the workflow agent threads to complete the automatic tasks held by workflow agent workers before shutting down gracefully.</p>
<b>Authorization Settings</b>	
<b>Inherit Permission Set From</b>	<p>The permission set the server uses for new objects if a user fails to specify a permission set for an object or fails to specify that no default permission set is wanted. Options are:</p> <p>A User permission set is defined for a user when a system administrator, superuser, or repository owner creates a user. This permission set can be used as the permission set for any object created by the user. Because user objects are not subtypes of SysObject, the permission set is not used to enforce any kind of security on the user. A User permission set can only be used as a default permission set.</p> <p>A Type permission set is associated with the type definition for a SysObject or SysObject subtype. A Type permission set can only be used as a default permission set.</p> <p>A Folder permission set is associated with a folder or cabinet. If a user wants to change the properties of a folder or cabinet, modify the folder or cabinet object itself, or move, copy, or link an object to the folder, the server uses the permissions in the associated permission set to determine whether the user can perform the requested operation.</p>

Field	Value
<b>Default Alias Set</b>	The default alias set for new objects. Click the Select Alias Set link to access the Choose an alias set page.
<b>Enabled LDAP Servers</b>	The LDAP configuration objects for LDAP servers used for user authentication and synchronization.  Click the Select link to access the Choose LDAP Server Configurations page to add LDAP servers.
<b>Maximum Login Ticket Expiration Time</b>	The maximum length of time, in minutes, that a login ticket generated by the current server can remain valid. The minimum value is 1 minute. The maximum value is 43200 minutes (30 days). The default value at server installation is 43200.
<b>Default Login Ticket Expiration Time</b>	The default length of time, in minutes, that a login ticket generated by the current server can remain valid. The value must always be less than or equal to the maximum login ticket expiration time. The default value is 5 minutes.
<b>Application Access</b>	Application access control (AAC) tokens are encoded strings that may accompany connection requests from applications. The information in a token defines constraints on the connection request. If selected, a connection request received by this server from a non-superuser must be accompanied by a valid application access control token and the connection request must comply with the constraints in the token.
<b>Superuser Access</b>	When selected, a user with superuser privileges cannot connect to the server using a global login ticket.

For more information about modifying general server configuration information, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.4 Creating or modifying connection broker projections

The connection broker is the intermediary between a client and the server when the client wants a repository connection. If a server is not known to at least one connection broker, no clients can connect to the repository associated with the server. Each server broadcasts information to connection brokers at regular intervals. The broadcast contains the information maintained by connection brokers about the server and the repository accessed by the server.

When a client requests a connection to a repository, the connection broker sends the client the connection information for each server associated with the repository. The client can then choose which server to use.

For more information about creating or modifying connection broker projections, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

### 3.3.5 Creating or modifying network locations

A network location identifies locations from which end users connect to OpenText Documentum CM web clients. Network locations define specific IP address ranges. Documentum CM Servers use network locations to determine the content storage location from which a content file is provided to web client users.

For more information about creating or modifying network locations, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

### 3.3.6 Creating or modifying application servers

Documentum CM Server supports application servers in the server configuration object. The server configuration object specifies the name and the URI of the associated application servers.

Documentum CM Server supports a wide variety of network-accessible application, personalization, portal, and e-commerce servers from enterprise vendors such as Microsoft, IBM, Oracle, SAP, and so on. The *Release Notes* documents of various OpenText Documentum CM products contain the information about the supported application server. The vendor documentation of the application server contains more information on how to deploy an application server.

For more information about creating or modifying application servers, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

### 3.3.7 Creating or modifying cached types

Cached types specify which user-defined types are to be cached at server startup. By default, no user-defined objects are cached.

For more information about creating or modifying cached types, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.8 Creating or modifying locations

The **Location** tab lets you view and modify the locations of files, objects, and programs on the server hosts file system, including the assume user program, change password program, and log file.

**Table 3-4: Locations page properties**

Field	Value
<b>Assume User</b>	The location of the directory containing the assume user program. The default is assume_user.
<b>Change Password</b>	The location of the directory containing the change password program. The default is change_password.
<b>Common</b>	The location of the common directory. The default is common.
<b>Events</b>	The location of the events directory. The default is events.
<b>Log</b>	The location of the logs directory. The default is temp.
<b>Nls</b>	The location of the NLS directory. The default is a single blank.
<b>Secure Writer</b>	The location of the directory containing the secure writer program. The default is secure_common_area_writer.
<b>System Converter</b>	The location of the directory containing the convert.tbl file and the system-supplied transformation scripts. There is no default for this field.
<b>Temp</b>	The location of the temp directory.
<b>User Converter</b>	The full path for the user-defined transformation scripts. The default is convert.
<b>User Validation</b>	The full path to the user validation program. The default is validate_user.

Field	Value
<b>Verity</b>	5.3 and later repositories, contains a dummy value for compatibility with Webtop 5.2.x. The default value is verity_location.
<b>Signature Check</b>	The location of the directory that contains the signature validation program. The default is validate_signature.
<b>Authentication Plugin</b>	The location of an authentication plug-in, if used. The default is auth_plugin in \$Documentum/dba/auth.

For more information about creating or modifying locations, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.9 Creating or modifying far stores

In a Distributed Content environment, a far store is a storage area remote or inaccessible from the current Documentum CM Server, in which the server cannot store content. For more information about Distributed Content environments, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

For more information about creating or modifying far stores, *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.10 Moving a server to dormant and active states

This section describes how to move a server to a dormant state and back to an active state.

A Documentum CM Server can be moved to a dormant state only from an active state. To perform this operation, you should be a member of the dm\_datacenter\_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of Documentum CM Server.

A Documentum CM Server can be moved back to an active state only from a dormant state. To perform this operation, you should be a member of the dm\_datacenter\_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of Documentum CM Server.

For more information about moving a server to dormant and active states, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.11 Enabling or disabling save operation for a Documentum CM Server in dormant state

You can perform the enable or disable save operation for a Documentum CM Server if you are a member of the dm\_datacenter\_managers, a privileged group whose membership is maintained by superusers. When you enable save operation for a Documentum CM Server which is in dormant state, you can perform create and update operations. By default, save operation is disabled. This feature is only applicable for 7.0 and later versions of Documentum CM Server.



#### Caution

To perform any of the view, create, update, or delete operations for a Documentum CM Server which is in dormant state, you as a member of the dm\_datacenter\_managers group should execute the action **Enable Save Operation**, else view, create, update, or delete operations will fail.

For more information about enabling or disabling save operation for a Documentum CM Server in dormant state, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.12 Projecting active or dormant state of Documentum CM Server to connection broker

The dormancy status of Documentum CM Server can be projected to the connection broker. To perform this operation, you should be a member of the dm\_datacenter\_managers, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of Documentum CM Server.



#### Notes

- The **Project Dormant Status to Connection Broker** and **Project Active Status to Connection Broker** menu options are available only for Documentum CM Servers which is in active state. These options will not be available for Documentum CM Servers which is in dormant state. Therefore, you always can perform the Project Dormant Status to Connection Broker operation first followed by Project Active Status to Connection Broker operation.
- For a WDK application to login to a repository in a dormant state, dmc\_wdk\_presets\_owner, dmc\_wdk\_preferences\_owner, and dm\_bof\_registry users should be a member of dm\_datacenter\_managers.

For more information about projecting active or dormant state of Documentum CM Server to connection broker, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

### 3.3.13 Viewing server and connection broker log files

The server log file records server activities. Server logs provide valuable information for troubleshooting server or repository problems.

Connection broker logs record information about connection brokers, which provide connection information to clients.



**Note:** If you are connected to a secondary server, you see only the server and connection broker logs for that server.

For more information about viewing server and connection broker log files, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

### 3.3.14 Deleting a server configuration object

Do not delete the CURRENT version of the server configuration object of an active server. You can safely delete the CURRENT version of the server configuration object of a server that is shut down, or old configuration object versions of an active server. To display old versions of server configuration objects, select the **All Versions** filter from the list box on the server configuration object page.

For more information about deleting a server configuration object, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

#### 3.3.14.1 Confirming object deletion

When you delete certain objects from a repository, you must confirm that you want to delete the object.

For more information about confirming object deletion, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

### 3.3.15 Configuring a server as a process engine

If the Business Process Manager application is installed in a repository and you have process engine, you can configure a server as a process engine.

For more information about configuring a server as a process engine, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

### 3.3.16 Disabling a process engine server

You can disable a server as a process engine.

**To disable a server as a process engine:**

1. Using any client, connect to the repository whose server you are disabling as a process engine.
2. Navigate to the /System/Workflow/Process Engine folder.
3. Make sure that all objects in the folder are displayed.  
For example, in Documentum Administrator, select **Show All Objects and Versions** from the list box.
4. Delete the object corresponding to the name of the server that is configured as a process engine.

### 3.3.17 Changing ACL or groups in a high-availability setup

In a distributed setup, having several Documentum CM Servers in high-availability setup, any changes to access control list (ACL) or groups and so on takes some time to reflect the changes in all the servers. This time depends on the change checker interval. While doing sensitive operation such as deleting a user from a repository, you need to be aware of this to prevent unauthorized operations during this interval.

## 3.4 server.ini file

The server configuration is defined by the server.ini file and the server configuration object. The server installation procedure creates both files automatically and the files are called when the server is started.

The properties in the server configuration object provide operating parameters and a map to the files and directories that the server can access. At startup, a Documentum CM Server always reads the CURRENT version of server configuration object.

The server.ini file contains information you provide during the installation process, including the repository name and the repository ID. That information allows the server to access the repository and contact the RDBMS server. The server.ini file also contains the name of the server configuration object.

You can use Documentum Administrator to modify the server configuration object, as described in [“Adding or modifying Documentum CM Servers” on page 31](#). However, the server configuration object pages in Documentum Administrator do not contain all of the default and optional properties that are defined in the server.ini file. Some those properties can only be modified in the server.ini file using the Documentum Server Manager. Typically, only the installation owner can modify the server.ini file.

### 3.4.1 Modifying the server.ini file

The server.ini file contains configuration information for the server. The file is stored in the %DOCUMENTUM%\dba\config\<repository> directory (\$DOCUMENTUM/dba/config/<repository>) and is called when the server is started.

The server.ini file has the following format:

```
[ SERVER_STARTUP ]
<key>=<value>

[ DOCBROKER_PROJECTION_TARGET ]
<key>=<value>

[ DOCBROKER_PROJECTION_TARGET_<n> ] #<n> can be 0-49
<key>=<value>

[ FUNCTION_EXTENT_SIZE ]      #Oracle only
<key>=<value>

[ TYPE_EXTENT_SIZE ]          #Oracle only
<key>=<value>
```

Only the [SERVER\_STARTUP] section is required. The other sections are optional.

Changes to the server.ini file take effect only after the server is stopped and restarted.



**Note:** To receive a verbose description of the server.ini file, type the following command at the operating system prompt:

```
documentum -h
```

If you want to add a comment to the file, use a semicolon (;) as the comment character.

To change the server.ini file, you must have appropriate access privileges for the %DOCUMENTUM%\dba\config\<repository> (\$DOCUMENTUM/dba/config/<repository>) directory in which the file resides. Typically, only the installation owner can access this directory.

#### To modify the server.ini file:

1. Open the server.ini file:

On Linux, use the text editor of your choice.

On Windows:

- a. Navigate to **Start > Programs > Documentum > Documentum Server Manager**.
- b. Select the **Repository** tab.
- c. Select the repository associated with the server.ini file.
- d. Click **Edit Server.ini**.

2. Edit the properties that you want to change.

3. Save the file.
4. Stop and restart the server to make the changes take effect.

### 3.4.2 SERVER\_STARTUP section keys

The keys in the [SERVER\_STARTUP] section provide repository and the database access information as well as default operating parameters. The default and optional keys can be modified using Documentum Server Manager.

[“Keys in the SERVER\\_STARTUP section” on page 46](#), describes the keys in the server startup section in alphabetical order.

**Table 3-5: Keys in the SERVER\_STARTUP section**

Key	Data type	Description
acl_update_threshold	integer	Optional key. Improves performance when the dm_world permission in an ACL is updated.  If the key is not specified, Documentum CM Server updates the entire dmr_content object type table. If the key value is larger than the number of affected rows, only the affected rows are updated. Otherwise, Documentum CM Server updates the entire table.
check_user_interval	integer	Optional key. The interval, in seconds, in which Documentum CM Server checks the login status of a user. The default value is 0, meaning that the status is only checked when the user logs in.
cipherlist	string	Optional key. Used for certificate-based SSL communication. Specifies the list of ciphers.

Key	Data type	Description
client_session_timeout	integer	Optional key. Specifies, in minutes, how long the server waits for a communication from a client session before disconnecting the session.  The default value is 5 minutes.
concurrent_sessions	integer	Optional key. Specifies the number of connections the Documentum CM Server can handle concurrently. The default is 100. For more information, see <a href="#">“concurrent_sessions” on page 67</a> .
crypto_keyname	string	Specifies the name of the Application Encryption Key (AEK) key. This can be used in hosts which have consolidated repositories using different AEK keys.
crypto_keystore	string	Keystore value. Valid values are: <ul style="list-style-type: none"><li>• Local: For password-based AEK</li><li>• Remote_Vault: For Vault-based AEK key</li></ul>
crypto_mode	string	Mode based on the algorithm used to generate the AEK key. Valid values are: <ul style="list-style-type: none"><li>• AES128_RSA2048_SHA3_384</li><li>• AES192_RSA2048_SHA3_384</li><li>• AES256_RSA2048_SHA3_384</li><li>• 3DES_RSA2048_SHA3_384</li></ul>

Key	Data type	Description
database_auth_type	integer	<p>Optional key. Used for authenticating with or without using password between the Documentum CM Server and database. Valid values are:</p> <ul style="list-style-type: none"> <li>• 0: For authentication using password</li> <li>• 1: For authentication without using password</li> </ul>
database_conn	string	The database connection string, which is used by the server to connect with the RDBMS server. This key is specified during Documentum CM Server installation and is only required for Oracle databases.
database_name	string	The tablespace or database in the RDBMS. This key is specified during Documentum CM Server installation and only required by SQL Server databases.
database_owner	string	The RDBMS login name of the repository owner. This key is specified during Documentum CM Server installation.
database_password_file	string	The name of the file that contains database passwords.
database_user	string	<p>The RDBMS login name of the normal database user with restricted privileges used during operation mode.</p> <p>For more information about the normal database user with restricted privileges, see <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i>.</p>

Key	Data type	Description
deferred_update_queue_size	integer	<p>Optional key. Controls the size of the deferred object update record queue. The default queue size is 1000, the valid range for this parameter is 256 to 4096.</p> <p>Increase the queue size, if repository operations generate a large number of deferred object updates. If the queue fills up, the deferred updates are performed immediately, which can impact application performance.</p>
distinct_query_results	Boolean	<p>Optional key. Specifies whether duplicate rows are included in query results. Valid values are:</p> <ul style="list-style-type: none"> <li>• FALSE: The default value. Duplicate rows are included in query results.</li> <li>• TRUE: Only distinct rows are returned in query results.</li> </ul> <p>The NOFTDQL hint returns only unique results. If the identical query is executed in FTDQL, the key is ignored and all results of the query are returned, including duplicate results.</p>

Key	Data type	Description
dm_group_list_limit_temp_table	Boolean	<p>Optional key. Specifies whether Documentum CM Server creates a temporary table that contains the names of all groups to which a session user belongs. Valid values are:</p> <ul style="list-style-type: none"><li>• TRUE: The SQL generated for every DQL query contains a LEFT OUTER JOIN on the temporary table. This operation improves performance when you execute multiple queries in the same session.</li><li>• FALSE: The default value. The SQL generated for every DQL query contains a subquery that fetches the names of all the groups to which a session user belongs. However, if the user is part of many groups this subquery becomes inefficient.</li></ul> <p> <b>Note:</b> This is supported only in administration mode.</p>

Key	Data type	Description
dm_left_outer_join_for_acl	Boolean	<p>Improves performance levels for session users without superuser privileges who belong to large number of groups.</p> <p>When you set this variable, it composes a LEFT OUTER JOIN from the dm_sysobject_s table to the dm_acl_s table on the FROM clause of the converted SQL statement. The LEFT OUTER JOIN returns all entries from the left table even though an entry does not have a matching entry on the right table. It uses the left table as a driving table to find the corresponding entries on the right table, which guides the database optimizer to a better execution plan, thus improving performance on SQL Server.</p>
dm_use_temporary_tablespace	Boolean	<p>When you set this variable to T, OpenText Documentum CM creates the temporary tables on the temporary database instead of creating in your repository database.</p> <p> <b>Note:</b> To use this, you must have a provisioned temporary database. OpenText does not recommend to use this key. However, you can use this ONLY when you have any concerns about the multiple read/write operations in your repository database.</p>
docbase_id	integer	The repository ID. The repository ID must be unique among all the repositories installed on the system. This key is specified during Documentum CM Server installation.

<b>Key</b>	<b>Data type</b>	<b>Description</b>
docbase_name	string	The repository name. This key is specified during Documentum CM Server installation.
db_oracle_dop	integer	Optional key. Indicates the degree of parallelism to be used by the underlying Oracle database. The index creation runs faster depending on the number of CPUs, table partitioning and disk fragmentation of the database. This key is specified prior to the Documentum CM Server upgrade. The value should be greater than or equal to 2.
db_oracle_index_nologging	Boolean	Optional key. Helps in faster insertion and index creation. Improves performance by bypassing the writing of the redo log. This key is specified prior to the Documentum CM Server upgrade. Valid values are TRUE and FALSE. The default is TRUE.
db_oracle_online_index	Boolean	Optional key. Indicates whether the index is being created online. During an online index rebuild, Oracle takes a snapshot log on the target table to hold DML activity, read the table in a full-table scan (read consistent), build the new index and then apply the changes from the snapshot log after the index has been rebuilt. During a regular index rebuild, an exclusive lock occurs as the existing index is read. This key is designed for scheduled downtime periods where there is no DML activity. This key is specified prior to the Documentum CM Server upgrade. The default is FALSE.

Key	Data type	Description
dsis_daemon_token	integer	Optional key. Documentum Secret Integration Service (DSIS) authentication token.
dsis_url	string	Optional key. DSIS URL.
enable_database_partition	Boolean	Optional key. This key is used to enable the partitioning of the repository.
enforce_four_digit_year	Boolean	<p>Optional key. Specifies whether Documentum CM Server displays dates using four digits. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The default value. Documentum CM Server displays the year date using four digits if the user does not specify a date format.</li> <li>• FALSE: Documentum CM Server does not display the year in four digits by default.</li> </ul>
gethostbyaddr	Boolean	<p>Optional key. Specifies whether the Documentum CM Server calls the <code>gethostbyaddr()</code> function during connection requests to obtain the host name of the machine on which a client application resides. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The default value. Documentum CM Server uses the <code>gethostbyaddr()</code> function to obtain the host name.</li> <li>• FALSE: Documentum CM Server skips the <code>gethostbyaddr ()</code> calls during connection requests and uses host addresses instead.</li> </ul> <p>If a large number of client machines do not have names, set the key to FALSE to skip to achieve better performance.</p>

Key	Data type	Description
history_cutoff	integer	<p>Optional key. Specifies a cut-off time for historical sessions in minutes. For example, if the history_cutoff value is 15, the server does not return any historical session older than 15 minutes, even if the maximum number of sessions defined in history_sessions has not been reached.</p> <p>The default value for history_cutoff is 240 minutes.</p>
history_sessions	integer	<p>Optional key. Specifies the number of maximum timed-out sessions returned by the SHOW_SESSIONS function. Use the apply method or the EXECUTE statement to run SHOW_SESSIONS. For more information about history_sessions, see <i>OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)</i>.</p>
host	string	<p>The IP address on which the server listens. The host key value is specified during Documentum CM Server installation.</p> <p>Some host machines have multiple network cards. If you want Documentum CM Server to use a particular network card on the host machine, specify the IP address of the card in this key before starting the server.</p>

Key	Data type	Description
ignore_client_domain	Boolean	<p>Optional key. Specifies whether the Documentum CM Server ignores the domain passed by the client during a connection request. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The Documentum CM Server ignores the client domain and uses the domain specified in user_auth_target attribute for all user authentications.</li> <li>• FALSE: The default value. The Documentum CM Server uses the client domain passed in a connection request.</li> </ul>
incremental_jms_wait_time_on_failure	integer	<p>Optional key. Used for Documentum CM Server to determine the time it should retry to POST to a previously failed Java Method Server. By default, the incremental time interval is set to 30 seconds. This key is specified in configuring Java Method Server for high-availability only.</p> <p> <b>Note:</b> This key is not applicable in configuring Java Method Server for high-availability in the 7.3 and later releases.</p>
install_owner	string	This key is not used. The value in the server configuration object is used instead.
isDSISEnabled	Boolean	<p>Optional key. Indicates if Vault is enabled. Valid values are:</p> <ul style="list-style-type: none"> <li>• T: Store the passwords and secrets in Vault.</li> <li>• F: Passwords and secrets are not stored in Vault.</li> </ul>

Key	Data type	Description
jms_max_wait_time_on_failures	integer	<p>Optional key. Used as a cap on wait time so as not to wait for a long time for the next retry time. This key is specified in configuring Java Method Server for high-availability only. The default value for jms_max_wait_time_on_failures is 1 hr (3600 seconds).</p> <p> <b>Note:</b> This key is not applicable in configuring Java Method Server for high-availability in the 7.3 and later releases.</p>
keystore_file	string	Optional key. Used for Certificate-based SSL communication. Specifies the connection broker certificate and private key.
keystore_pwd_file	string	Optional key. Used for Certificate-based SSL communication. Specifies the plain-text or encrypted keystore password.
ip_mode	string	<p>Optional key. Specifies whether Documentum CM Server supports IP addresses in the IPv6 format. Valid values are:</p> <ul style="list-style-type: none"> <li>• DUALSTACK: The default value. Documentum CM Server accepts both the IPv4 and IPv6 addresses.</li> <li>• V4ONLY: Documentum CM Server only accepts the IPv4 addresses.</li> </ul> <p> <b>Note:</b> IPv6 addresses should not start with f.</p>

Key	Data type	Description
listener_queue_length	integer	<p>Optional key. Specifies the queue for connection requests. This key is only used on Windows.</p> <p>Documentum CM Server creates a socket listener for incoming connection requests. By default, the maximum backlog queue value is 200. The key must be a positive integer value. Documentum CM Server passes the specified value to the listen () Windows Sockets call.</p>
mail_notification	Boolean	<p>Optional key. Specifies whether email messages are sent when a work item or an event is queued. Valid values are</p> <ul style="list-style-type: none"> <li>• TRUE: The default value. Email messages are sent.</li> <li>• FALSE: Users are not notified.</li> </ul> <p>If no mail server is set for Documentum CM Server, OpenText recommends you to turn off email sending by setting this key to FALSE.</p>
max_nqa_string	integer	<p>Optional key. Defines the maximum length of a non-qualifiable string property, in bytes.</p> <p>The default is 2000.</p> <p>If the key is not specified, the default is the maximum length allowed by the underlying relational database.</p>

Key	Data type	Description
max_ftacl_cache_size	integer	<p>Optional key. Limits the number of elements cached per session to process FTDQL-compliant full-text queries. Documentum CM Server caches ACL information on objects to evaluate security on the results returned by full-text queries.</p> <p>The default value is -1 (no limit). If the value is 0, no security information is cached. The key can have any integer value greater than -1. However, OpenText recommends that you do not change the default value.</p>
max_session_heap_size	integer	<p>Optional key. Specifies, in bytes, how much memory a session can use. The default value is -1, which means that the heap grows as necessary to whatever size the server machine resources allow, up to the server addressing memory limit of 2 GByte.</p>
max_storage_info_count	integer	<p>Optional key. Defines the maximum number of storage areas for which Documentum CM Server maintains information in shared memory. The default is 100. Valid values are positive integers from 100 to 65535.</p> <p>The value does not limit the number of storage areas. For example, if the key value is 150, it is possible to create additional storage areas, but information for the additional storage areas is not maintained in memory. In a multiserver environment, all Documentum CM Servers must use the same max_storage_info_count value.</p>

Key	Data type	Description
maxtypes_in_from_clause	integer	Optional key. Defines the maximum number of types in FROM clause increased to the specified number. If the key is not specified, the default value is 50.
method_server_enabled	Boolean	Optional key. Specifies whether the Documentum CM Server or the Java method server is used to execute dm_method objects. Valid values are: <ul style="list-style-type: none"> <li>• TRUE: The default value. The Java method server executes dm_method objects that are configured to run on the Java method server. If the methods are not configured correctly, Documentum CM Server executes the method instead.</li> <li>• FALSE: Documentum CM Server executes dm_method objects.</li> </ul>
method_server_threads	integer	Optional key. Specifies the maximum number of method server worker processes that are available to execute method objects. The default (and minimum) value is 5. The maximum value for this key is the value set in the concurrent_sessions property of the server configuration object. <p>The method_server_threads values are for the <i>dmbasic method server</i> only and do not have any impact on the Java method server.</p>

Key	Data type	Description
owner_xpermit_default	string	<p>Optional key. Specifies whether object owners are assigned extended permissions for an object by default or have the permissions that are explicitly assigned to them. Valid values are:</p> <ul style="list-style-type: none"> <li>• ACL: Object owners have only the extended permissions that are assigned explicitly and are not granted extended permissions by default. The key value is case-sensitive and must be specified in capital letters.</li> <li>• ALL or No value set: Object owners are assigned all extended permissions by default. Only the following sysobjects are secured by default: dm_job, dm_job_request, dm_jms_config, dm_procedure, dm_client_rights, and dmc_module</li> </ul> <p>This feature is governed using the DM_OWNER_CHANGE_ALLOWED environment variable. If you set the value to 0 (for backward compatibility), users who does not have the sysadmin privileges can still change the ownership.</p>

Key	Data type	Description
preserve_existing_types	Boolean	<p>Optional key. Specifies whether Documentum CM Server queries the RDBMS at startup to determine if the object type tables are present for all defined object types. Valid values are:</p> <ul style="list-style-type: none"><li>• TRUE: The default value. Documentum CM Server preserves existing types and does not dynamically destroy and recreate object type tables for types that are reported missing by the RDBMS.</li><li>• FALSE: Documentum CM Server dynamically destroys and recreates object type tables for types that are reported missing by the RDBMS.</li></ul>

Key	Data type	Description
rdbms_connect_retry_timeout	integer	<p>Optional key.</p> <ul style="list-style-type: none"> <li>• Server startup: Specifies how long the server tries to connect to the RDBMS. The server attempts to connect every 30 seconds until it is successful or the time-out limit is reached. Also note that the server process sleeps for 30 seconds before every retry operation. The remaining time is taken to connect to RDBMS and so in actual it takes up 1 minute.</li> <li>• Server already running: If the server is already running and if the RDBMS connection is lost, there might be many internal server sessions started already and whenever each of them tries to connect to RDBMS, it fails and retries for 1 second. If the retry operation fails, then the server does not stop as other sessions might be operating and server does not know if the RDBMS failure is intermittent or not. So, the server does not give back RDBMS session for this particular call while for others it continues. If the server.ini value is not set, then for each session, it will retry for 10 times (default timeout value is 5 minutes) before failing.</li> </ul>

Key	Data type	Description
saveasnew_retain_source_group	Boolean	<p>Optional key. Specifies which default group is assigned to a new object created by a <code>IDfSysObject.saveAsNew</code> method. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The new object is assigned to the default group of the original (source) object.</li> <li>• FALSE: The default value. The new object is assigned to the default group of the user who issues the <code>saveAsNew</code> method.</li> </ul>
server_codepage	string	UTF-8 is the only allowed value.
server_config_name	string	<p>Specifies which server configuration object is used to start Documentum CM Server. The Documentum CM Server installation procedure assigns the name of the repository to the server configuration object generated for the server.</p> <p>The default value is the name of the repository.</p>
server_login_ticket_version	integer	Specifies the format of the generated login ticket, for backwards compatibility.
server_startup_sleep_time	integer	<p>Specifies the amount of time, in seconds, that Documentum CM Server waits before trying to connect to the RDBMS. The time delay allows the underlying RDBMS to start before Documentum CM Server attempts to connect.</p> <p>The default value is 0.</p>

Key	Data type	Description
service	string	The TCP/IP service name for Documentum CM Server. This key is configured during Documentum CM Server installation. The value is the service name that appears in services file of the Documentum CM Server host machine. If a repository has multiple Documentum CM Servers, this name must be unique for each Documentum CM Server.
start_index_agents	Boolean	Specifies whether Documentum CM Server starts configured index agent instances at Documentum CM Server startup.  The default value is TRUE.
ticket_multiplier	integer	Specifies the number of login tickets with server scope allocated in shared memory. The number of tickets allocated by the server is computed as follows:  $\text{#tickets} = \text{concurrent_sessions} * \text{ticket_multiplier}$  The default value is 10.
truststore_file	string	Optional key. Used for Certificate-based SSL communication. Specifies the trusted connection broker certificates.
umask	string(4)	Optional key. Modifies the default operating system permissions assigned to public directories and files created by Documentum CM Server in the server or repository installation on Linux. For more information, see “umask” on page 68.

Key	Data type	Description
update_access_date	Boolean	<p>Specifies whether the r_access_date property is updated in the deferred update process. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The default value. Documentum CM Server updates the r_access_date property as part of the deferred update process.</li> <li>• FALSE: Documentum CM Server does not update the r_access_date property.</li> </ul>
upd_last_chg_time_from_db	Boolean	<p>Optional key. Specifies that all Documentum CM Servers in a clustered environment have timely access to all changes in group membership. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: Should only be used for environments with multiple Documentum CM Servers. The value should be set to TRUE for all running Documentum CM Servers.</li> <li>• FALSE: The default value.</li> </ul>
use_estimate_search	Boolean	<p>Specifies whether users can execute the ESTIMATE_SEARCH administration method. The administration method is used to fine-tune SEARCH conditions for queries. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The default value. Users can execute the method.</li> <li>• FALSE: The method does not execute.</li> </ul>

Key	Data type	Description
use_group_address	integer	<p>Specifies who receives email notifications when an event is queued to a group. Valid values are:</p> <ul style="list-style-type: none"> <li>• 0: The default value. Documentum CM Server sends email to each group member.</li> <li>• 1: Documentum CM Server sends email to the groups address. If the group has no email address, the server sends notifications to each group member.</li> <li>• 2: Documentum CM Server sends email to each group member and to the group address.</li> </ul> <p>To reduce the number of emails sent, OpenText recommends that you set use_group_address to 1. This results in lesser load on the method server.</p>
user_auth_case	string	<p>Specifies the case Documentum CM Server converts the user name of the client before authenticating the user. Valid values are:</p> <ul style="list-style-type: none"> <li>• upper: The user name is converted to upper case.</li> <li>• lower: The user name is converted to lower case.</li> <li>• insensitive: The user name is converted to allow case-insensitive login.</li> <li>• NULL: The default value. The name is authenticated using the case in which it was entered by the user.</li> </ul>

Key	Data type	Description
user_auth_target	string	<p>Specifies the domain that Documentum CM Server uses to authenticate client user names and passwords only on Windows.</p> <p>The default is the domain in which the server resides.</p>
validate_database_user	Boolean	<p>Specifies whether Documentum CM Server validates that the user identified in the database_owner key in the server.ini file has a valid operating system user account. Valid values are:</p> <ul style="list-style-type: none"> <li>• TRUE: The default value. Documentum CM Server validates the operating system user account.</li> <li>• FALSE: Documentum CM Server does not validate the operating system user account.</li> </ul>
wait_for_connect_timeout	integer	<p>Specifies how long Documentum CM Server waits for a connection request before starting to process other work, such as deferred updates.</p> <p>The default value is 10 seconds.</p>

### 3.4.2.1 concurrent\_sessions

The concurrent\_sessions key controls the number of connections the server can handle concurrently. This number must take into account not only the number of users who are using the repository concurrently, but also the operations those users are executing. Some operations require a separate connection to complete the operation. For example:

- Issuing an IDfQuery.execute method with the readquery flag set to FALSE causes an internal connection request.
- Executing an apply method or an EXECUTE DQL statement starts another connection.
- When the agent exec executes a job, it generally requires two additional connections.

- Issuing a full-text query requires an additional connection.

The default value is 100. Consider the number of active concurrent users you expect, the operations they are performing, and the number of methods or jobs you execute regularly, and then modify this value accordingly.

The maximum number of concurrent sessions is dependent on the operating system of the server host machine. The limit is:

- 3275 for Windows
- 1020 for Linux

### 3.4.2.2 **database\_refresh\_interval**

The database\_refresh\_interval key defines how often the main server thread (parent server) reads the repository to refresh its global caches. You can raise this value but it cannot be lowered.

The default value is 1 minute.

### 3.4.2.3 **umask**

On Linux, permissions can be expressed as a 3-digit octal number, representing the permission level for the owner, group owner, and others. For example, a file created with permissions 700 grants the owner read, write and execute permission, but the group owner and others get no permissions at all. Permissions of 644 grants the owner read and write permission, but the group owner and others only have read permission. Similarly, 640 gives the owner read and write permission, the group owner read only permission and others get no permissions.

The umask is also expressed as an octal number and is used to further restrict (or mask) the permissions when a directory or file is created. For example, if the requested permissions are 766 and the umask is 22, the actual permissions applied is 744. A bit set in the umask turns off the corresponding bit in the requested permissions.

Documentum CM Server uses a umask key in the server.ini file that is separate from the Linux per-process umask, but applies it in a similar fashion. The Documentum CM Server internally refers to permissions with the symbolic names dmOSFSAP\_Public, dmOSFSAP\_Private, dmOSFSAP\_Public ReadOnly, dmOSFSAP\_PrivateReadOnly, and dmOSFSAP\_PublicOpen. “[Documentum CM Server directory and file permissions on Linux](#)” on page 68 describes the associated permission values.

**Table 3-6: Documentum CM Server directory and file permissions on Linux**

Permission name	Directory value	File value
dmOSFSAP_Public	755	644
dmOSFSAP_Private	700	600

Permission name	Directory value	File value
dmOSFSAP_Public ReadOnly	555	444
dmOSFSAP_PrivateReadOnl y	500	400
dmOSFSAP_PublicOpen	777	666

 **Note:** The umask in the server.ini configuration file only modifies the values for the dmOSFSAP\_PublicOpen permissions. If the umask is not specified in the server.ini file, the default setting for the dmOSFSAP\_PublicOpen permissions is 777 for directories and 666 for files. Any directories or files that are publicly accessible outside the Documentum CM Server are created using this permission.

### 3.4.3 DOCBROKER\_PROJECTION\_TARGET section keys

The [DOCBROKER\_PROJECTION\_TARGET] and [DOCBROKER\_PROJECTION\_TARGET\_n] sections define the connection brokers to which Documentum CM Server sends connection information. The Documentum CM Server installation procedure creates one [DOCBROKER\_PROJECTION\_TARGET] section in the server.ini file, which contains access information the first broadcast to a connection broker. For the first broadcast, the connection broker name provided during the installation is used as the host key. The proximity key is assigned 1, the default value. When the Documentum CM Server is started at the end of the installation procedure, it projects the connection information to the connection broker specified in the host key.

Connection broker projection targets are also defined in a set of properties in the server configuration object. We recommend to use the server configuration properties to define additional projection targets, instead of the server.ini file. Modifying the server configuration object allows changing a target without restarting Documentum CM Server. If the same projection target is defined in both the server configuration properties and in the server.ini file, Documentum CM Server uses the values for the target in the server configuration properties.

The [DOCBROKER\_PROJECTION\_TARGET] section defines the first projection target. To define additional targets, use [DOCBROKER\_PROJECTION\_TARGET\_n] sections. The <n> can be any integer from 0 to 49.

[“server.ini DOCBROKER\\_PROJECTION\\_TARGET keys” on page 70](#) describes the keys.

**Table 3-7: server.ini DOCBROKER\_PROJECTION\_TARGET keys**

<b>Key</b>	<b>Datatype</b>	<b>Comments</b>
host	string	Name of connection broker host.   <b>Note:</b> If you specify the connection broker IP address instead of host name in <code>server.ini</code> , the same connection broker IP address is used for both the native and secure ports.
port	integer	Port number used by the connection broker.   <b>Note:</b> By default, the secure port is assigned by incrementing the configured native port by 1.
proximity	integer	User-defined value that represents distance of server from connection broker.

### 3.4.4 FUNCTION\_EXTENT\_SIZE and TYPE\_EXTENT\_SIZE sections

The [FUNCTION\_EXTENT\_SIZE] and [TYPE\_EXTENT\_SIZE] sections specify how much space is allocated in the RDBMS for the object type tables. They are available only for Oracle.

[“server.ini FUNCTION\\_EXTENT\\_SIZE keys” on page 70](#), lists the keys for the FUNCTION\_EXTENT\_SIZE section.

**Table 3-8: server.ini FUNCTION\_EXTENT\_SIZE keys**

<b>Key</b>	<b>Datatype</b>	<b>Description</b>
database_ini_ext_large	integer	Specifies the size of the initial extent allotted by default to object types categorized as large.
database_ini_ext_small	integer	Specifies the size of the initial extent allotted by default to object types categorized as small.

Key	Datatype	Description
database_ini_ext_default	integer	Specifies the size of the initial extent allotted by default to object types categorized as default.
database_next_ext_large	integer	Specifies the size of the second extent allotted by default to object types categorized as large.
database_next_ext_small	integer	Specifies the size of the second extent allotted by default to object types categorized as small.
database_next_ext_default	integer	Specifies the size of the second extent allotted by default to object types categorized as default.

[“server.ini TYPE\\_EXTENT\\_SIZE keys” on page 71](#), lists the keys for the TYPE\_EXTENT\_SIZE section.

**Table 3-9: server.ini TYPE\_EXTENT\_SIZE keys**

Key	Datatype	Comments
database_ini_ext_<typename>	integer	Replace <typename> with the name of the object type.
database_next_ext_<typename>	integer	Replace <typename> with the name of the object type.

## 3.5 Managing additional Documentum CM Servers

A repository can have more than one Documentum CM Server. For more information, see [“Adding or modifying Documentum CM Servers” on page 31](#).

Additional Documentum CM Servers serving a single repository require:

- Unique service names

The service name for each server must be unique within the network connecting the machines and that service name must be referenced in the service property of the server.ini file invoked for the server.

- The same trust level

Servers servicing one repository must be all non-trusted servers or all trusted servers. It is not possible to have trusted and non-trusted servers servicing one repository.

- Individual server configuration objects and server.ini files

On a Windows host, each server must have its own server configuration object and server.ini file.

On a Linux host, each server must have its own server configuration object and server.ini file, and start up script.

- On Windows hosts:

The primary installation account must be in the domain administrators group. The program SC.EXE must be installed in %SystemRoot%\System32\SC.EXE. SC.EXE is available on the Windows SDK CD. It is used to create and start services for Documentum CM Server.

- On Linux hosts:

- The installation account of the primary host must have sufficient privilege to execute remsh commands.
- The primary host must be able to resolve target machine names through the /etc/hosts file or DNS.
- Each target machine must be able to resolve the primary host name through the /etc/hosts file or DNS.

For more information about starting additional servers, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

## 3.6 Managing Documentum CM Server in a virtual deployment

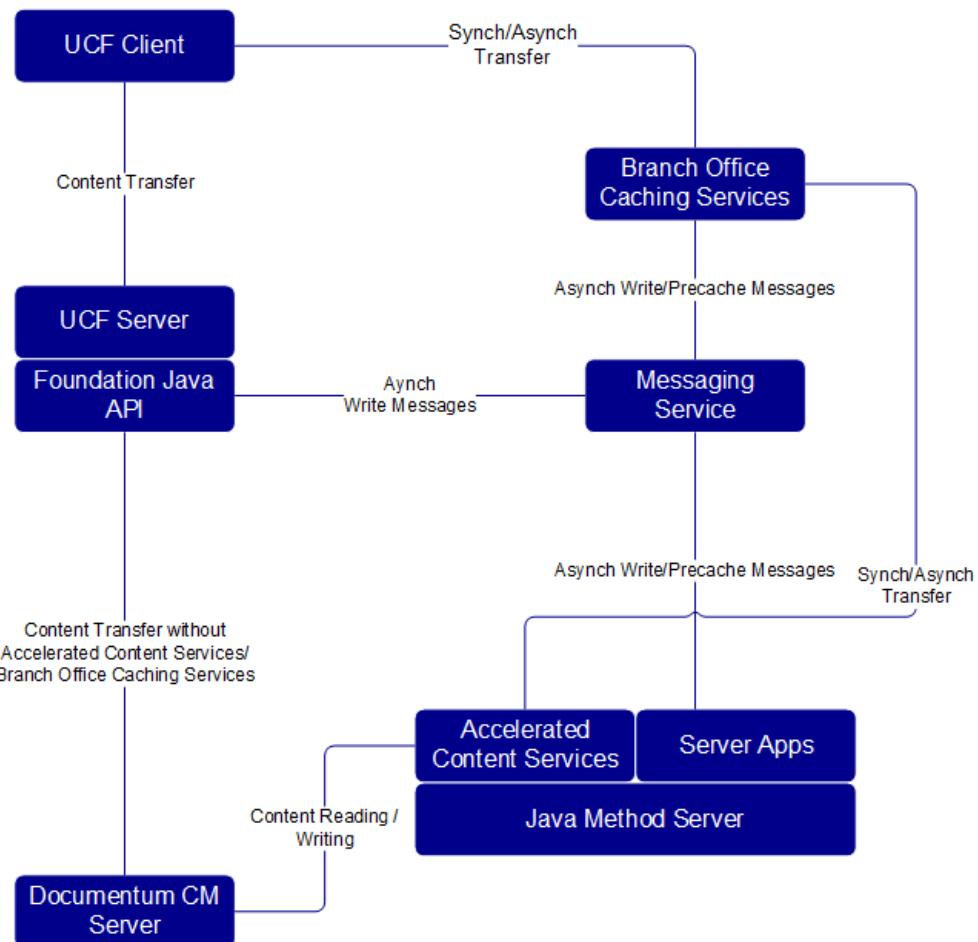
### 3.6.1 Overview

To run the Documentum CM Server effectively in a virtual environment, you must be able to automate the provisioning, management, and monitoring of Documentum CM Server. A virtual environment can be an environment in which virtualized servers, such as VMware vSphere, are deployed. Managing Documentum CM Server in a virtual environment involves programmatically scaling the system up and down to adjust and balance the system load. In addition, system components must automatically re-connect to one another when one or more of them are restarted. In a virtual deployment, Documentum CM Server can perform the following processes:

- Programmatically and gracefully start or restart the Documentum CM Server and all of its components in the correct sequence
- Programmatically and gracefully shut down the Documentum CM Server and all of its components in the correct sequence
- Programmatically and gracefully fail over the Documentum CM Server and all of its components in the correct sequence
- Monitor the performance of the Documentum CM Server and all of its components

The first three processes require that the operational status of Documentum CM Server and its components be able to be placed into a dormant state. A dormant state ensures that the transactions of Documentum CM Server that are in progress are completed but that no new transactions are started. The dormant state enables Documentum CM Server to be gracefully started, restarted, shut down, or complete failovers without transactions being lost or the state of Documentum CM Server becoming inconsistent.

**Figure 3-1** illustrates the interactions between the major OpenText Documentum CM components.



**Figure 3-1: OpenText Documentum CM components**

### 3.6.2 Operational status

When a Documentum CM Server is in a dormant or dormancy-requested state, the following occurs:

- No new connections are accepted.
- All existing connections are placed into a read-only mode.
- Its status is projected to its associated connection brokers, which prevent new connections from being made to it.

Connections can be pooled connections, previously timed-out but reconnected sessions, and scheduled jobs. When running transactions are completed, they are placed into a read-only mode. Because some users (such as datacenter administrators) must be able to perform actions on a dormant Documentum CM Server, they can be added to a privileged group. Users in the privileged group can perform any operations that are allowed with their existing privileges and permissions on a dormant Documentum CM Server.

The Java Method Server is never placed into a dormant state, because in a Java Method Server high-availability configuration multiple Documentum CM Server instances could be using the same Java Method Server.

[“Effects of operational status on Documentum CM Server components - Documentum CM Server” on page 74](#) describes the effects of the operational status of Documentum CM Server components.

For more information about making a Documentum CM Server instance or repository dormant, see [“Moving a server to dormant and active states” on page 41](#).

For more information about only projecting a Documentum CM Server instance as dormant or active, see [“Projecting active or dormant state of Documentum CM Server to connection broker” on page 42](#).

**Table 3-10: Effects of operational status on Documentum CM Server components - Documentum CM Server**

Operational status	Value	Documentum CM Server
ACTIVE	0	Normal operation. It can accept connections and process transactions.
DORMANCY_REQUESTED	2	Does not accept new connection. All existing connections are placed into a read-only mode. All currently running transactions are completed.

<b>Operational status</b>	<b>Value</b>	<b>Documentum CM Server</b>
DORMANT	1	Does not accept new connections. All running transactions have completed.
PROJECTED_DORMANT	N/A	Normal operation (including read/write transactions) continue for existing connections.

**Table 3-11: Effects of operational status on Documentum CM Server components - OpenText™ Documentum™ Content Management Accelerated Content Services**

<b>Operational status</b>	<b>Value</b>	<b>OpenText Documentum Content Management (CM) Accelerated Content Services</b>
ACTIVE	0	Normal operation. It can accept connections and process transactions.
DORMANCY_REQUESTED	2	N/A
DORMANT	1	Does not accept new connections. All running transactions have completed.
PROJECTED_DORMANT	N/A	Normal operation.

**Table 3-12: Effects of operational status on Documentum CM Server components - connection broker**

<b>Operational status</b>	<b>Value</b>	<b>Connection broker</b>
ACTIVE	0	Normal operation. It can accept connections and process transactions.
DORMANCY_REQUESTED	2	Does not accept projections from Documentum CM Server. Does not provide Documentum CM Server or repository maps.
DORMANT	1	Does not accept projections from Documentum CM Server and Accelerated Content Services. Does not provide Documentum CM Server or repository maps.

Operational status	Value	Connection broker
PROJECTED_DORMANT	N/A	Does not allow any new connections to the Documentum CM Server.

**Table 3-13: Effects of operational status on Documentum CM Server components - workflow agent**

Operational status	Value	Workflow agent
ACTIVE	0	Normal operation. It can accept connections and process transactions.
DORMANCY_REQUESTED	2	All currently running workflows are halted. Any running, automatic tasks are stopped and any of their acquired work items are placed into the paused state. However, dormant work items of an automatic task remain in the dormant state.
DORMANT	1	All workflows have been halted. Any running, automatic tasks have been stopped and any of their acquired work items have been placed into the paused state.
PROJECTED_DORMANT	N/A	Normal operation.

**Table 3-14: Effects of operational status on Documentum CM Server components - xPlore**

Operational status	Value	Index Agent [1]	xPlore deployment [1]	
			Single repository	Multiple repositories
ACTIVE	0	Normal operation.	Normal operation.	Normal operation.
DORMANCY_REQUESTED	2	Behavior is identical to that of the DORMANT operational status.	Behavior is identical to that of the DORMANT operational status.	Behavior is identical to that of the DORMANT operational status.

<b>Operational status</b>	<b>Value</b>	<b>Index Agent [1]</b>	<b>xPlore deployment [1]</b>	
			<b>Single repository</b>	<b>Multiple repositories</b>
DORMANT	1	<ul style="list-style-type: none"> <li>For a dormant Documentum CM Server: Only the index agents that are associated with that Documentum CM Server are shut down; whereas the index agents of other Documentum CM Servers associated with the same repository continue to operate normally.</li> <li>For a dormant repository: All index agents (for all Documentum CM Servers associated with that repository) are shut down.</li> </ul>	<p>For a dormant Documentum CM Server:</p> <ul style="list-style-type: none"> <li>One index agent: All xPlore instances in the xPlore deployment are placed into an off_line state.</li> <li>Multiple index agents: All xPlore instances in the xPlore deployment remain in normal operation</li> </ul> <p>For a dormant repository, all xPlore instances in an xPlore deployment are placed into an off_line state.</p>	<p>For a dormant Documentum CM Server or repository, the xPlore instances in the xPlore deployment remain in normal operation.</p> <p> <b>Note:</b> Even when all repositories are dormant, all xPlore instances in the xPlore deployment remain in normal operation.</p>
PROJECTED_DORMANT	N/A	Normal operation.	Normal operation.	Normal operation.

[1] Only xPlore version 1.3 or later can work with Documentum CM Server virtual deployment server.

“Behavior of dormant servers in various deployments” on page 78 describes the behavior of dormant servers in the various Documentum CM Server deployments.

**Table 3-15: Behavior of dormant servers in various deployments**

<b>Deployment</b>	<b>Dormant server instances</b>	<b>Behavior</b>
High Availability	Single	Using the other server instance, existing sessions can access the repository in a read/write mode and new sessions can be created.
	Both	Existing sessions can access the repository in a read-only mode. New sessions cannot be created.
Load Balanced	Multiple (at least one server instance is active)	Using the other server instances, existing sessions can access the repository in a read/write mode and new sessions can be created. New sessions are load-balanced across the active server instances
	All	Existing sessions can access the repository in a read-only mode. New sessions cannot be created.
remote Content Server	Local	Metadata requests are routed to the remote server. Content access for non-cached data might be affected.
	Remote	The remote server does not process content requests. Content access for non-cached data might be affected.
Federated	Member	Push replication as well as any federation operations that require the governing repository are impacted.
	Governing	Pull replication and any federation operations that require the governing repository are impacted.

### 3.6.2.1 Privileged group

The name of the privileged group is `dm_datacenter_managers`. All users in this privileged group are referred to as *privileged users*. When a repository is in a dormant state, all privileged users can connect to the repository in a new session (if required) and can enable read/write permissions for themselves. Enabling read/write permissions for privileged users do not allow any more permissions than their existing privileges and permissions. By default, privileged users are not enabled for read/write permissions when logging in to a dormant repository.



**Note:** Members of the `dm_datacenter_users` group can login in read-only mode to the system that is in a dormant state. However, if you want all the users to login in read-only mode to the system that is in a dormant state, set the environment variable `DM_DATACENTER_ALLOW_CONN` to `<1>`.

For more information about enabling and disabling read/write permission for privileged users, see “[Enabling or disabling save operation for a Documentum CM Server in dormant state](#)” on page 42.

### 3.6.3 Monitoring performance

To manage Documentum CM Server in a virtual environment effectively, you must be able to determine when the performance of any of its various components is unacceptable and then take corrective action. Performance is a measurement of an action over a specific time period. An example of a performance metric is when Documentum CM Server executes twenty transactions within a time period of thirty minutes.

You can retrieve the following performance metrics for Documentum CM Server and Java Method Server servers:

- RPCs
  - The total number of RPCs executed in the specified time period
  - These execution statistics for RPCs executed during the specified time period:
    - Execution time of the fastest RPC
    - Execution time of the slowest RPC
    - Average execution time of all RPCs
- Transactions
  - The total number of transactions executed in the specified time period
  - These execution statistics for transactions executed during the specified time period:
    - Execution time of the fastest transaction
    - Execution time of the slowest transaction

- Average execution time of all transactions
- Database (Documentum CM Server only)
  - Total size of the tablespace
  - Total size of the audit table
  - Total number of audit table rows



**Note:** Foundation Java API Javadocs contain more information on the performance metrics.

### 3.6.3.1 Using the Foundation Java API performance monitoring API

To implement a new application or add functionality to an existing application that monitors the performance of Documentum CM Server in a virtual environment, you use the methods specified in “[Performance monitoring tasks](#)” on page 80.



#### Notes

- After getting a session, you can call all of the performance monitoring methods, which are implemented in `IDfSession`.
- Only privileged users can call these methods.
- The Foundation Java API Javadocs contain more information and examples on implementing these methods.

**Table 3-16: Performance monitoring tasks**

Task	Description	Foundation Java API methods
Starting and stopping the time period during which to collect performance metrics	Starts the time period during which to collect performance metrics.	<code>startGatheringMetrics(java.util.List&lt;java.lang.String&gt;metricsToGather)</code>
	Stops the time period during which to collect performance metrics.	<code>stopGatheringMetrics(java.util.List&lt;java.lang.String&gt;metricsToStop)</code>
Retrieving performance metrics	Retrieves performance metrics that have been collected during the specified time period.	<code>collectMetrics(java.util.List&lt;java.lang.String&gt;metricsToCollect)</code>

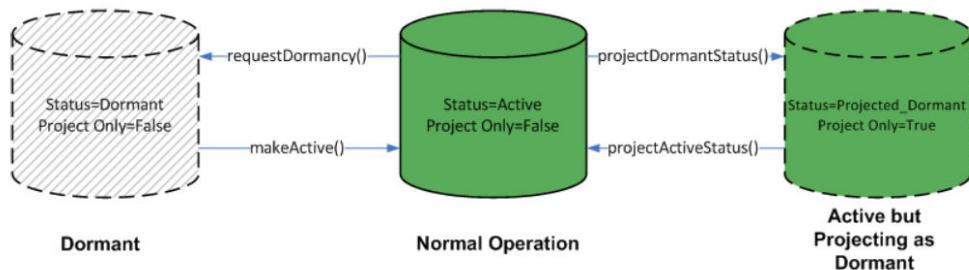
Task	Description	Foundation Java API methods
Retrieving the state of performance metrics	<p>Retrieves the execution state of each of the performance metrics as follows:</p> <ul style="list-style-type: none"> <li>INITIALIZED - the metric can be collected, but the server has not started to collect it yet</li> <li>STARTED - the server has started to collect this metric</li> <li>STOPPED - the server has stopped collecting this metric</li> </ul>	listMetricsState()
Resetting previously set performance metrics	Clears all of the values for existing performance metrics and frees all server memory associated with performance metrics.	resetMetrics()

### 3.6.4 Using the Foundation Java API operational status API

The Foundation Java API Javadocs contain more information and examples about implementing the operational status methods.

After getting a session, you can call all of the operational status methods, which are implemented in `IDfSession`. Before changing the operational status of a repository, Documentum CM Server, or Accelerated Content Services server, check their current operational status.

Figure 3-2 shows the Documentum CM Server state changes as a result of executing the different Foundation Java API methods.



**Figure 3-2: Documentum CM Server state changes**

### 3.6.5 Restarting Documentum CM Server components in virtual deployments

This section discusses how and in which order to reinstall Documentum CM Server components in the Windows and Linux virtual deployment environments.

#### 3.6.5.1 Overview

In a virtual deployment, you need to be able to restart applications if a Documentum CM Server is being replaced. When you restart applications in a Documentum CM Server deployment, restart the following components in the following order:

1. Connection brokers
2. Documentum CM Server and repositories
  - All workflow master and worker threads and processes
  - All dmbasic method threads and processes
3. The Java Method Server application server. Java Method Server and Accelerated Content Services reconnect.  
 **Note:** The Documentum CM Server repositories are projected to the connection brokers.
4. Index agents

Whenever an individual component is restarted:

- All transactions that were running at the time the component was stopped are restarted.
- No data loss or integrity issues occur.

#### 3.6.5.2 Restarting Documentum CM Server on Windows

##### 3.6.5.2.1 Start connection brokers

On the command line, run:

```
net start <service>
```

where <service> is the name of the connection broker service to start.

 **Example 3-1: Start connection brokers**

```
net start "Documentum Connection Broker Service docbroker2"
```



An exit status of zero (in %ERRORLEVEL%) indicates that the restart was successful; a nonzero result indicates that the restart was unsuccessful.

### 3.6.5.2.2 Start Documentum CM Server and repositories

On the command line, run:

```
net start <service>
```

where <service> is the name of the Documentum CM Server and repository Windows service to start.

#### ► Example 3-2: Start Documentum CM Server and repositories

```
net start "Documentum Repository Service <Repo2>"
```



An exit status of zero (in %ERRORLEVEL%) indicates that the restart was successful; a nonzero result indicates that the restart was unsuccessful.

### 3.6.5.2.3 Start the Java Method Server application server

On the command line, run:

```
net start <service>
```

where <service> is the name of the Java Method Server service to start. The default name is Documentum Java Method Server.

#### ► Example 3-3: Start the Java Method Server application server

```
net start "Documentum Java Method Server"
```

An exit status of zero (in %ERRORLEVEL%) indicates that the restart was successful; a nonzero result indicates that the restart was unsuccessful.



### 3.6.5.2.4 Start the index agents

Make sure that server-impl.jar (in which IndexAgentCtrl.class is contained) is included in CLASSPATH.

1. On the index agent host, start the application server.
2. On the Documentum CM Server host, on the command line, run:

```
Java IndexAgentCtrl -docbase_name <repository_name> -user_name <usser_name> -action start
```

where:

- <repository\_name> is the name of the repository that the index agent runs against.

- <usser\_name> is the name of a user that has administrator permissions.  
An exit status of zero (in %ERRORLEVEL%) indicates that the restart was successful; a nonzero result indicates that the restart was unsuccessful.

### 3.6.5.3 Restarting Documentum CM Server on Linux

#### 3.6.5.3.1 Start connection brokers

On the command line, run:

```
$DOCUMENTUM/dba/dm_launch_docbroker [-init_file file_name] [-host host_name]  
[-service service_name] [-port port_number]
```

Include the host name (<host\_name>) and a service name (<service\_name>) or port number (<port\_number>) to identify the connection broker. Otherwise specify an initialization file (<file\_name>) that includes a [DOCBROKER\_CONFIGURATION] section to identify the connection broker. An exit status of zero (in the \$? variable) indicates that the restart was successful; a nonzero result indicates that the restart was unsuccessful.

#### 3.6.5.3.2 Start Documentum CM Server and repositories

On the command line, run:

```
$DOCUMENTUM/dba/dm_start_<repository>
```

where <repository> is the name of the repository to start.

 **Example 3-4: Start Documentum CM Server and repositories**

```
$DOCUMENTUM/dba/dm_start_<Repo2>"
```



An exit status of zero (in %ERRORLEVEL%) indicates that the restart was successful; a nonzero result indicates that the restart was unsuccessful.

#### 3.6.5.3.3 Start the Java Method Server application server

On the command line, run:

```
$DM_HOME/tomcat/bin/startup.sh
```

#### 3.6.5.3.4 Start the index agents

Make sure that server-impl.jar (in which IndexAgentCtrl.class is contained) is included in CLASSPATH.

1. On the index agent host, start the application server.
2. On the Documentum CM Server host, on the command line, run:

```
Java IndexAgentCtrl -docbase_name <repository_name> -user_name <usser_name> -action start
```

where:

- <repository\_name> is the name of the repository that the index agent runs against.
- <usser\_name> is the name of a user that has administrator permissions.

An exit status of zero (in %ERRORLEVEL%) indicates that the restart was successful; a nonzero result indicates that the restart was unsuccessful.

## 3.7 Server load balancing and failover

When an installation has a large number of users or there is a lot of activity in the repository, multiple Documentum CM Servers can be used to balance the load. Starting multiple servers also allows graceful failover if a particular server stops for any reason.

The Documentum CM Servers used for load balancing must project identical proximity values to the connection broker. If the servers have identical proximity values, clients pick one of the servers randomly. If the proximity values are different, clients always choose the server with the lowest proximity value.

Sessions cannot fail over to a Documentum CM Server with a proximity of 9000 or greater. Documentum CM Servers with a proximity of 9000 or higher are called content-file servers. remote Content Server installed at remote, distributed sites are configured as content-file servers by default. A client session can only fail over to servers that are known to the connection broker used by that session. For a proper failover, make sure that Documentum CM Servers project to the appropriate connection brokers and with appropriate proximity values.

If a Documentum CM Server stops and additional servers are running against the repository with proximity values less than 9000, the client library gracefully reconnects any disconnected sessions unless one of the following exceptions occurs:

- If the client application is processing a collection when the disconnection occurs, the collection is closed and must be regenerated again when the connection is reestablished.
- If there is ongoing transfer between the client and server, the content transfer must be restarted from the beginning.
- If the client had an open explicit transaction when the disconnection occurred, the transaction is rolled back and must be restarted from the beginning.

- If the original connection was started with a single-use login ticket or a login ticket scoped to the original server, the session cannot be reconnected to a failover server because the login ticket cannot be reused.

## 3.8 Shutting down a server

On Windows, Documentum Server Manager can be used to shut down Documentum CM Server. On Linux, the dm\_shutdown\_<repository> script or the shutdown method shuts down Documentum CM Server. To make sure that Documentum CM Server shuts down properly, the Java Method Server should be stopped first, then stop the repository services and the connection broker.

You must have system administrator or superuser user privileges to stop a server.

### 3.8.1 Shutting down a server running on Windows

**To shut down a server:**

1. Navigate to **Start > Control Panel > Administrative Tools > Services**. Select the Java Method Server, then click **Stop**.
2. Navigate to **Start > Programs > Documentum > Documentum Server Manager**, click the **Repository** tab, select the repository, then click **Stop**.
3. Select the **DocBroker** tab, select the connection broker, then click **Stop**.



#### Caution

On Windows, OpenText does not recommend to use an IDfSession.shutdown method to shut down the server. The method does not necessarily shut down all relevant processes.

### 3.8.2 Shutting down a server running on Linux

On Linux, the dm\_shutdown\_<repository> script logs into the specified repository and issues a shutdown request. The script waits 90 seconds before exiting. If the repository shuts down more quickly, the script exits as soon as the server is down. This script is useful when you want to shut down the server as part of a program or application, without human intervention.

You must run the script on the machine where the server resides. To invoke the script, issue the command:

```
dm_shutdown_<repository> [-k]
```

where <repository> is the name of the repository. The -k flag instructs the script to issue an operating-system kill command to stop the server if the shutdown request has not been completed in 90 seconds.



**Note:** You must pass NO\_IMMEDIATE if you want the scripts to wait for open transactions to be closed before shutting down Documentum CM Server on Linux. The syntax format is:

```
shutdown,session[,immediate][,delete_entry]
```

For example: The `./dm_shutdown_testrepo NO_IMMEDIATE` command issues the shutdown operation after the open transactions are closed.

### 3.8.3 Creating a shut-down script

Use the instructions in this section to create a shut-down script for a Documentum CM Server running on a Linux host.

#### To create a script for a new server:

1. Make a copy of an existing `dm_shutdown_<repository>` script and save the copy with a new name.

`dm_shutdown_<repository>` scripts are found in `$DOCUMENTUM/dba`.

For example:

```
% cd $DOCUMENTUM/dba
% cp dm_shutdown_engrepository dm_shutdown_devrepository1
```

2. In the new copy, edit the line immediately preceding `shutdown,c,T` by replacing `<repository name>` with `<repository_name>.<server_config_name>`.

The line you want to edit is as shown:

```
./iapi <repository name> -U$DM_DMADMIN_USER -P -e << EOF
```

Use the name of the server configuration object that you created for the server.

For example:

```
./iapi devrepository2.server2 -U$DM_DMADMIN_USER -P -e << EOF
```

3. Save the file.

## 3.9 Clearing the server common area

Use the procedures in this section to remove files that are in the server common area.

#### To remove all files from the server common area:

1. Stop Documentum CM Server.
2. Do one of the following:
  - On Windows, edit the Documentum CM Server service to add `-oclean` to the end of the command line.
  - On Linux, add the `-oclean` argument in the `dm_start_<repositoryname>` command line.

3. Restart the server.

## 3.10 Managing Tomcat

The Tomcat binary is bundled with the Documentum CM Server installation suite. The application server is installed into the *<Tomcat\_directory>* subdirectory of the Documentum CM Server installation directory. The default Tomcat root directory is:

- \$DOCUMENTUM\Tomcat\_directory on Windows
- \$DOCUMENTUM\_SHARED\Tomcat\_directory on Linux

The Documentum CM Server installation creates a Tomcat server instance in the *<TomcatRoot>\server\<instance name>* directory. For example, C:\Documentum\Tomcat\_directory\server\DtcmServer\_MethodServer.

### 3.10.1 Starting and stopping the Tomcat application server

The Tomcat application server is started automatically after a Documentum CM Server installation. However, starting and stopping a Documentum CM Server does not automatically start or stop the Tomcat application server. The application server hosts one or more Java applications or processes, such as the method server, the Java Method Server, Accelerated Content Services server, and the DmMail application.

#### To start the application server:

On Windows:

1. Navigate to %DM\_JMS\_HOME%\bin.
2. Execute startMethodServer.cmd or start the Windows service for the server instance.

For the Java method server, and the server instance hosting the Java method server, the service name is Documentum Java Method Server. Starting that service is equivalent to executing startMethodServer.cmd.

On Linux:

1. Configure the \$DM\_JMS\_HOME environment variable manually. For example: \$DOCUMENTUM/tomcat.
2. Navigate to \$DM\_JMS\_HOME/bin.
3. Execute start MethodServer.sh.

#### To stop an instance server:

Stopping the server stops all applications running within it.

On Windows:

1. Navigate to %DM\_JMS\_HOME%\bin.
2. Execute stopMethodServer.cmd or stop the Windows service for the server instance.

For the Java method server, and the server instance hosting the Java method server, the service name is Documentum Java Method Server. Stopping that service is equivalent to executing stopMethodServer.cmd.

On Linux:

1. Configure the \$DM\_JMS\_HOME environment variable manually. For example: \$DOCUMENTUM/tomcat.
2. Navigate to \$DM\_JMS\_HOME/bin.
3. Execute stopMethodServer.sh.

## 3.11 Server log files

Each Documentum CM Server maintains a log file. By default, the <serverconfig\_name>.log log file is stored in the %DOCUMENTUM%\dba\log directory, where <serverconfig\_name> is the name of the server configuration object. The default location is defined in the log location object that is referenced by the log\_location property in the server configuration object.

Both, the name and the location of the file can be modified using the -logfile parameter on the server start-up command line. The server appends to the log file while the server is running. If the server is stopped and restarted, the file is saved and another log file started. The saved log files have the following format:

On Windows: <serverconfig\_name>.log.save.mm-dd-yy\_hh.mi.ss

On Linux: <serverconfig\_name>.log.save.mm.dd.yyyy.hh.mi.ss

## 3.12 dm\_error utility

The dm\_error utility returns information about Documentum CM Server errors. The utility is run from the command line: dm\_error <error\_code> Where <error\_code> is the abbreviated text that describes the error. For example, DM\_SERVER\_E\_NO\_MTHDSVR\_BINARY.

The utility output of the displays the cause of the error and possible solutions, as described in the following example:

```
[DM_SERVER_E_NO_MTHDSVR_BINARY]
"%s: Method server binary is not accessible."
CAUSE: The method server binary "mthdsrv" is not under
$DM_HOME/bin or it does not have the proper permission.
ACTION: Make sure method server binary "mthdsrv" is under
$DM_HOME/bin and set execution permission for it.
```

### 3.13 Improving performance on Oracle and PostgreSQL databases

The performance and throughput of Documentum CM Server depends to a certain extend on where the repository content is stored in the underlying database. When a repository is created, the Documentum CM Server creates object-type tables and indexes in the underlying RDBMS in the same tablespace by default. Oracle or PostgreSQL can be partitioned to store data in different tablespaces. For example, frequently used data could be stored in a designated tablespace. The size and number of the extents allotted for each table are determined by default configuration parameters in the server.ini file. For more information about improving performance, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

# Chapter 4

## Managing repositories

### 4.1 Repositories

Repositories are comprised of object type tables, type indexes, and content files. The type tables and type indexes are tables in an underlying relational database. The content files are typically stored in directories on local disks. Content files can also be stored in the database, in a retention storage system such as Centera or NetApp SnapLock, or on external storage devices.

A full-text index is associated with a particular repository or, in a consolidated deployment, with all repositories indexed by a particular index server installation. Full-text indexes enable rapid searching for designated values or strings in content files and property values.

Users access repositories through Documentum CM Servers. The Documentum CM Servers receive queries from clients in the form of Foundation Java API methods or Documentum Query Language statements and make the actual call to the underlying RDBMS or the file directories. Every repository must have at least one active Documentum CM Server. If a repository does not have an active server, users cannot access that repository.

Information about the repository is located in a server startup file. The startup file is executed whenever the Accelerated Content Services server is started. The information in the startup file binds the Documentum CM Server to the repository.

### 4.2 Managing repositories

The repository is configured on the **Administration > Basic Configuration > Repository** page in Documentum Administrator. A repository is represented by a repository configuration object that defines configuration parameters, such as the name of the underlying RDBMS, security levels for the repository, and other operating configuration parameters.

Only users with superuser privileges can view or modify the repository configuration object of a repository. It is not possible to use Documentum Administrator to create additional repositories or delete an existing repository. Adding another repository requires running the Documentum CM Server installer.

You can modify some, but not all, of the repository configuration values. The synchronization options control the behavior of OpenText Documentum CM Offline Client.

You must use Documentum Administrator for the following activities:

- Viewing or modifying the repository configuration
- Modifying repository synchronization
- Activating OpenText Documentum CM license

For more information, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

#### 4.2.1 Moving a repository to dormant and active states

This section describes how to move a repository to a dormant state and back to an active state.

A repository can be moved to a dormant state only from an active state. To perform this operation, you should be a member of the `dm_datacenter_managers`, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of repositories.



##### Notes

- When a repository is moved to a dormant state, the status of all the Documentum CM Servers and Accelerated Content Services servers for this repository will also be moved to a dormant state.
- In a multiple Documentum CM Server setup, moving a repository to a dormant state will move all the configured Documentum CM Servers to a dormant state. However, there will be delay in moving the non-connected servers to a dormant state. This delay is equal to the value of `database_refresh_interval` key as specified in `server.ini`. The `database_refresh_interval` key defines how often the main server thread (parent server) reads the repository to refresh its global caches. You can raise this value but it cannot be lowered. The default value is 1 minute.
- For a WDK application to login to a repository in a dormant state, `dmc_wdk_presets_owner`, `dmc_wdk_preferences_owner`, and `dm_bof_registry` users should be a member of `dm_datacenter_managers`.

A repository can be moved back to an active state only from a dormant state. To perform this operation, you should be a member of the `dm_datacenter_managers`, a privileged group whose membership is maintained by superusers. This feature is only applicable for 7.0 and later versions of repositories.



**Note:** When a repository is moved to an active state, the status of all the Documentum CM Servers and Accelerated Content Services servers for this repository will also be moved to an active state.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on the following:

- Moving a repository to a dormant state

- Moving a repository to an active state

### 4.2.2 Enabling a repository as a global registry

Enabling a repository as a global registry after configuration, requires activating the dm\_bof\_registry user. The global registry and user credentials can also be configured in the dfc.properties file.

For more information about enabling a repository as a global registry, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

During the Foundation Java API installation on client machines, such as the Documentum Administrator host, provide the user login name and password for the dm\_bof\_registry user. This action updates the dfc.properties file and enables the Foundation Java API installation to contact the global registry.

#### To modify the dfc.properties file manually:

1. On the Foundation Java API host, navigate to \$DOCUMENTUM/config (Linux) or %DOCUMENTUM%\config (Windows).
2. From a command prompt, execute the following command to generate the encrypted form of the global registry user's password:

```
java -cp dfc.jar com.documentum.fc.tools.RegistryPasswordUtils  
password_of_user
```

where password\_of\_user is the clear-text password of the global registry user.

3. Open the dfc.properties file in a text editor and modify the following attributes:

```
dfc.globalregistry.repository=global_registry_repository_name  
dfc.globalregistry.username=user_login_name  
dfc.globalregistry.password=encrypted_password_of_user
```

where encrypted\_password\_of\_user is the encrypted password you generated in step 2.

4. Save the dfc.properties file.

### 4.2.3 Repository content

The Documentum CM Server installation program and the scripts that run during repository configuration automatically create various objects, such as cabinets, configuration objects, users, and groups.

**“Default users created during repository configuration”** on page 94 lists the default users that are created during repository configuration.

**Table 4-1: Default users created during repository configuration**

User	User privileges	Extended user privileges
repository_owner	Superuser	None
installation_owner	Superuser	None
global registry user	None	None
dm_bpm_inbound_user	None	None
dm_autorender_win32	System Administrator	None
dm_autorender_mac	System Administrator	None
dm_mediaserver	System Administrator	None
dm_fulltext_index_user	Superuser	None

The configuration program creates a number of default groups. “[Default groups created during repository configuration](#)” on page 94 describes the default groups. In addition to the default groups, the configuration program also creates a set of privileged groups.

**Table 4-2: Default groups created during repository configuration**

Group	Members
admingroup	installation_owner, repository_owner
docu	repository_owner, installation_owner, dm_autorender_win32, dm_autorender_mac, dm_mediaserver
queue_admin	None.
queue_manager	queue_admin group
queue_processor	queue_manager group
process_report_admin	queue_admin

#### 4.2.4 Type indexes

Indexes on the object type tables in the RDBMS enhance the performance of repository queries. When a repository is configured, the Documentum CM Server creates various object type indexes. There are several administration methods for managing type indexes:

- **MAKE\_INDEX**  
For more information, see “[MAKE\\_INDEX](#)” on page 345.
- **MOVE\_INDEX**  
By default, type tables and indexes are stored in the same tablespace or segment. However, you can create a repository with separate tablespaces or segments for

each or you can move the indexes later, using the MOVE\_INDEX method. Indexes that you create can be placed in any directory. For more information, see ["MOVE\\_INDEX" on page 345](#).

For more information about creating a repository with separate tablespaces, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

- [DROP\\_INDEX](#)

Removes a user-defined index. OpenText strongly recommends that you do not remove any of the system-defined indexes. For more information, see ["DROP\\_INDEX" on page 341](#).

Each method can be executed through Documentum Administrator, an apply method, or the DQL EXECUTE statement.

## 4.2.5 Date values

By default, Documentum CM Server stores values as UTC (Coordinated Universal Time) time in new repositories (OpenText Documentum CM 6 and later), and as the local time in repositories that are upgraded from versions prior to 6.

The r\_normal\_tz property in the docbase config object controls how Documentum CM Server stores dates in the repository. If the property value is 0, all dates are stored in UTC time. Otherwise, dates are normalized using the local time of Documentum CM Server before being stored in the repository. Offset value is time zone offset from UTC time, expressed as seconds and it is set by Documentum CM Server during the upgrade of existing repositories (repositories upgraded from 5.x versions to later). For example, if the offset represents the Pacific Standard Time zone, the offset value is -8\*60\*60, or -28800 seconds. When the property is set to an offset value, Documentum CM Server stores all date values based on the time identified by the time zone offset.

In a OpenText Documentum CM 6 or later repository, r\_normal\_tz value is set to 0. In a repository upgraded from a release earlier than version 6, the r\_normal\_tz value is set to the offset that represents Documentum CM Server local time by Documentum CM Server and cannot be changed.

## 4.2.6 Moving or duplicating a repository

Moving or duplicating a repository requires dump and load operations. Dump and load operations can be used to:

- Move part of a repository from one location to another.
- Duplicate part of a repository.

Use dump and load operations to create a duplicated repository with a different name or repository ID than the source repository.

Dump or load operations require superuser privileges. A dump operation creates a binary file of objects dumped from a repository. If a dumped object has associated

content files, the content files are either referenced by full path or included directly in the dump file. The load operation loads the objects and content files into another repository.

Dump files are created by using the session code page. For example, if the session in which the dump file was created was using UTF-8, the dump file is a UTF-8 dump file. The repository into which the dump file is loaded must use the same code page as the source repository.

Dump and load operations can be performed manually using either IAPI, Docbasic scripts, or the IDfDumpRecord and IDfLoadRecord Foundation Java API interfaces.



**Note:** Dump and load operations require additional steps for repositories where Web Publisher is installed.

#### 4.2.6.1 Supporting object types

There are several object types that support dump and load operations:

- Dump Record (dm\_dump\_record)

A dump record object contains information about a specific dump execution. It has a property that contains the name of the file with the dumped information and properties whose values tell Documentum CM Server which objects to copy into the specified file.

- Dump Object Record (dmi\_dump\_object\_record)

A dump object record object contains information about one specific object that is copied out to the dump file. Dump object record objects are used internally.

- Load Record (dm\_load\_record)

A load record object contains information about a specific load operation. Its properties are used by Documentum CM Server to manage the loading process. It also has two properties that contain the starting and ending times of the load operation.

- Load Object Record (dmi\_load\_object\_record)

A load object record object contains information about one specific object that is loaded from the dump file into a repository. Load object record objects are used internally.

For more information about the properties of the preceding list of object types, see *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)*.

#### 4.2.6.2 Dumping objects under retention

If a dumped SysObject is associated with a retainer, the dump operation also dumps the retainer. Retainers record retention policy definitions.

If a retainer object is dumped directly, the object identified in the retainer\_root\_id property of the retainer is also dumped. That object can be a single SysObject or a container, such as a folder. If it is a container, the objects in that container are not dumped, only the container itself is dumped.

 **Note:** This information does not apply to dump and load operations that are used to execute object replication jobs.

#### 4.2.6.3 Aspects and dump operations

A dump operation does not dump aspects associated with a dumped object. If aspects are associated with specific instances of an object type, those aspects must be created in the target repository. Similarly, if default aspects are defined for an object type and instances of that type are dumped, the default aspects must be manually created in the target repository. The aspects must be created in the target repository before performing the load operation.

#### 4.2.6.4 Dumping an entire repository

Dumping the contents of an entire repository by setting the dump\_operation property of the dump record object to full\_docbase\_dump is currently not supported.

#### 4.2.6.5 Dumping specific objects

To dump only specific objects in a repository, set the type, predicate, and predicate2 repeating properties of the dump record object. The type property identifies the type of object you want to dump and the predicate and predicate2 properties define a qualification that determines which objects of that type are dumped. For more information about properties of a dump record object, see *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)*.

However, when you dump an object, the server includes any objects referenced by the dumped object. This process is recursive, so the resulting dump file can contain many more objects than the object specified in the type, predicate, and predicate2 repeating properties of the dump record object.

When dumping a type that has a null supertype, the server also dumps all the objects whose r\_object\_ids are listed in the ID field of the type.

The ACL associated with a dumped object is also dumped.

#### 4.2.6.5.1 Setting the type property

The type property is a repeating property. The object type specified at each index position is associated with the WHERE clause qualification defined in the predicate at the corresponding position.

The dump operation dumps objects of the specified type and any of its subtypes that meet the qualification specified in the predicate. Consequently, it is not necessary to specify each type by name in the type property. For example, if you specify the SysObject type, then Documentum CM Server dumps objects of any SysObject or SysObject subtype that meets the qualification.

Use the following guidelines when specifying object types and predicates:

- The object type must be identified by using its internal name, such as dm\_document or dmrContainment.

Object type definitions are only dumped if objects of that type are dumped or if objects that are a subtype of the type are dumped.

This means that if a subtype of a specified type has no objects in the repository or if no objects of the subtype are dumped, the dump process does not dump the definition of subtype. For example, suppose you have a subtype of documents called proposal, but there are no objects of that type in the repository yet. If you dump the repository and specify dm\_document as a type to dump, the type definition of the proposal subtype is not dumped.

This behavior is important to remember if you have user-defined subtypes in the repository and want to ensure that their definitions are loaded into the target repository.

- To dump subtype definitions for types that have no objects instances in the repository or whose objects are not dumped, you must explicitly specify the subtype in the dump script.
- If you have created user-defined types that have no supertype, be sure to explicitly include them in the dump script if you want to dump objects of those types. For example, the following commands will include all instances of *your\_type\_name*:

```
append,c,1,type  
your_type_nameappend,c,1,predicate  
1=1
```

- If you have system or private ACLs that are not currently associated with an object, they are not dumped unless you specify dm\_acl as a type in the dump script. For example, include the following lines in a dump script to dump all ACLs in the repository (including orphan ACLs):

```
append,c,1,type  
dm_acl  
append,c,1,predicate  
1=1
```

You may want to specify a qualification in the predicate to exclude orphaned internal ACLs.

- By default, storage area definitions are only included if content associated with the storage is dumped. If you want to dump the definitions of all storage areas, even though you may not dump content from some, include the storage type (file store, linked, and distributed) explicitly in the dump script.
- When you dump the dm\_registered object type, Documentum CM Server dumps only the object (dm\_registered) that corresponds to the registered table. The underlying RDBMS table is not dumped. Use the dump facilities of the underlying RDBMS to dump the underlying table.

#### 4.2.6.5.2 Setting the predicate properties

You must supply a predicate for each object type you define in the type property. If you fail to supply a predicate for a specified type, then no objects of that type are dumped.

To dump all instances of the type, specify a predicate that is true for all instances of the type, such as 1=1.

To dump a subset of the instances of the object type, define a WHERE clause qualification in the predicate properties. The qualification is imposed on the object type specified at the corresponding index level in the type property. That is, the qualification defined in predicate[0] is imposed on the type defined in type[0], the qualification defined in predicate[1] is imposed on the type defined in type[1], and so forth.

For example, if the value of type[1] is dm\_document and the value of predicate[1] is object\_name = 'foo', then only documents or document subtypes that have an object name of foo are dumped. The qualification can be any valid WHERE clause qualification. For more information about the description of a valid WHERE clause qualification, see *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)*.

The predicate property accepts a maximum of 255 characters. If the qualification exceeds 255 characters, place the remaining characters in the predicate2 property at the corresponding index level. For example, if the qualification defined for type[0] is 300 characters, you put the first 255 characters in predicate[0] and the remaining 45 in predicate2[0]. When the dump is executed, Documentum CM Server concatenates predicate[0] and predicate2[0]. The predicate2 property accepts a maximum of 255 characters also.

*Important:* If you use the predicate2 property at any index position, you must also set the predicate2 property at all index positions before the desired position. Documentum CM Server does not allow you to skip index positions when setting repeating properties. For example, if you set predicate2[2] and predicate2[4], you must also set predicate2[0], predicate2[1], and predicate2[3]. It is valid to set the values for these intervening index positions to a single blank.

#### 4.2.6.6 Content files and dumping

How the dump operation handles content depends on where the content is stored and how the include\_content parameter is set in the dump\_parameter argument of the dump object.

By default, if the content is stored in a file store, Centera storage area, or NetApp SnapLock storage area, the content is not included in the dump file. You can set the include\_content parameter to include such content. If you are dumping a repository that has encrypted file store storage areas, you must include the content in the dump file. Documentum CM Server decrypts the content before placing it into the dump file.

For more information about the default behavior and requirements for handling dump files without content, see “[Dumping without content](#)” on page 100. For more information about including content and the requirements for dump files with content, see “[Including content](#)” on page 101.

If the content is stored in a blob or turbo storage area, the content is automatically included in the dump file because the content is stored in the repository.

Content stored in external storage cannot be included in a dump file.

##### 4.2.6.6.1 Dumping without content

By default, a dump operation on content in file stores, Centera stores, or NetApp SnapLock stores does not include content. Instead, when an object with content is dumped, the operation places a reference to the content in the dump file. If the content is stored in a file system, the reference is a file system path. If the object is stored in a retention storage system, the reference is the address of content.

When the dump file is loaded into the target repository, any file systems referenced for content must be visible to the server at the target site. For content in retention storage, the ca\_store object at the target site must have an identical definition as the ca\_store object at the source repository and must point to the same storage system used by the source repository.

In the target repository, the storage objects for the newly loaded content must have the same name as the storage objects in the source repository but the filepaths for the storage locations must be different.

The owner of the target repository must have Read permission in the content storage areas of the dumped repository when the load operation is executed. The load operation uses the target repository owner account to read the files in the source repository and copy them into the target repository.

#### 4.2.6.6.2 Including content

To include content in a dump file, set the `include_content` property to T (TRUE) in the dump record object. If the property is true, when Documentum CM Server dumps an object with content, the content is copied into the dump file also. The content must be stored in a file store, Centera store, or NetApp SnapLock storage area. Documentum CM Server cannot copy content from external storage into a dump file.

In the target repository, the storage objects for the newly loaded content must have the same names as those in the source repository, but the actual directory location, or IP address for a retention store, can be different or the same.

Always include content if you are dumping a repository to make a backup copy, to archive a repository, or to move the content or if the repository includes an encrypted storage area.

#### 4.2.6.6.3 Compressing content

When you include content, you can create a compressed dump file to save space. To compress the content in the dump file, set the `dump_parameter` property to `compress_content = T`.

Documentum CM Server automatically decompresses a compressed dump file during a load operation.

#### 4.2.6.7 Setting the cache size

Documentum CM Server uses an in-memory cache to store the object IDs of dumped objects. Before dumping an object, Documentum CM Server checks the cache to see if the object has already been dumped.

You can improve the performance of a large dump operation by setting a larger cache size. If you do not specify a cache size, the server uses a default size of 1 MB, which can hold up to 43,690 object IDs.

To increase the cache size, set the `cache_size` argument of the `dump_parameter` property to a value between 1 and 100. The value is interpreted as megabytes and defines the maximum cache size. The memory used for the cache is allocated dynamically as the number of dumped objects increases.

Documentum CM Server ignores the cache setting when doing a full repository dump.

#### 4.2.6.8 Using non-restartable dump

You can also improve the performance of a dump operation by creating a non-restartable dump. However, if a non-restartable dump operation fails, you will not be able to restart the dump from the failure point. Instead, you must create a new dump record object to start the dump operation from the beginning.

A dump operation can only be non-restartable if it is a partial repository dump. Full repository dump operations are always restartable.

To create a non-restartable dump, set the dump\_parameter property to restartable=F.

#### 4.2.6.9 Using a script to create a dump file

For dump operations that you execute regularly, we recommend that you write a script that creates and saves the dump object and checks for errors after the execution. Using a script avoids re-creating the dump object manually each time you want to perform the task.

##### To use a script:

1. Write a script that creates the dump object, sets its properties, saves the object, and checks for errors.

If you do not set the file\_name property to a full path, Documentum CM Server assumes the path is relative to the root directory of the server. The filename must be unique within its directory. This means that after a successful load operation that uses the dump file, you must move the dump file to archival storage or destroy it so you can successfully execute the script later.

2. Use IAPI to execute the script. Use the following command-line syntax:

```
iapi source_db -Username -Ppassword < script_filename
```

where:

- *source\_db* is the name of the repository that you want to dump.
- *username* is the user name of the user who is executing the operation.
- *password* is the user password.
- *script\_filename* is the name of the file you created in step 1.

3. If the dump was successful, destroy the dump object. If the Save on the dump operation did not return OK, the dump was not successful.

Destruction of the dump object cleans up the repository and removes the dump object records and state information that are no longer needed.

#### 4.2.6.9.1 Sample script for a partial repository dump

 **Note:** There is a template for a sample script in %DM\_HOME%\install\DBA\dump\_template.bat (\$DM\_HOME/install/DBA/dump\_template.api ).

The script assumes that you want to dump all instances of the types, not just a subset. Consequently, the predicates are set as 1=1 (you cannot leave them blank). If you want to dump only some subset of objects or want to include all ACLs, type definitions, or storage area definitions, modify the script accordingly.

Here is the script:

```
create,c,dm_dump_record
set,c,1,file_name
dumpfile name# Supply your own file name.
# This must be a new file
append,c,1,type
dm_sysobject
append,c,1,predicate
1=1
append,c,1,type
dm_assembly
append,c,1,predicate
1=1
append,c,1,type
dm_format
append,c,1,predicate
1=1
append,c,1,type
dm_user
append,c,1,predicate
1=1
append,c,1,type
dm_group
append,c,1,predicate
1=1
append,c,1,type
dmi_queue_item
append,c,1,predicate
1=1
append,c,1,type
dmi_registry
append,c,1,predicate
1=1
append,c,1,type
dm_relation
append,c,1,predicate
1=1
append,c,1,type
dm_relation_type
append,c,1,predicate
1=1
append,c,1,type
dmr_containment
append,c,1,predicate
1=1
append,c,1,type
dmr_content
append,c,1,predicate
1=1
append,c,1,dump_parameter
cache_size=60 #set cache size
append,c,1,dump_parameter
restartable=F #non-restartable dump
append,c,1,predicate
1=1
```

```
save,c,1  
getmessage,c
```

The preceding script has the following characteristics:

- It does not copy content files into the dump file.
- It only dumps ACLs associated with a dumped object.
- It does not dump subtype definitions if there are no objects of that subtype.
- It does not dump storage area definitions if the dump does not include any content associated with the storage area.
- It does not dump user-defined subtypes that have no supertype.
- It does not dump job objects.
- It is not restartable.



### Notes

- In the append command line, the l is the lowercase letter L.
- If you do not set the file\_name property to a full path, Documentum CM Server assumes the path is relative to the root directory of the server. The filename must be unique within its directory. This means that after a successful load operation using the dump file, you must move the dump file to archival storage or destroy it so that you can successfully execute the script later.
- To dump user-defined types that have no supertype, add Append methods for each to the script:

```
append,c,1,type  
your_type_nameappend,c,1,predicate  
1=1
```

#### 4.2.6.10 If the server crashes during a dump operation

If Documentum CM Server crashes during a dump operation, there are two alternatives:

- Destroy the dump file (target file named in the script) if it exists and then re-execute the script.  
If the specified file already exists when you try to save a new dump record object, the save operation fails. Re-executing the script creates a new dump record object.
- If the dump operation is restartable, fetch the existing dump object from the source repository and save it again. Saving the object starts the dump operation. Documentum CM Server begins where it left off when the crash occurred.

#### 4.2.6.11 Moving the dump file

The dump file is a binary file. If you move a dump file from one machine to another electronically, be sure to use a binary transfer protocol.

If your operating system is configured to allow files larger than 2 GB, the dump file can exceed 2 GB in size. If you create a dump file larger than 2 GB, you cannot load it on a machine that does not support large file sizes or large file systems.

#### 4.2.6.12 Loading a repository

Loading a repository puts the objects stored in a dump file into the repository. The dump file header does not indicate the session code page in which the dump file was created. If you do not know the session code page in use when a dump file was created, do not load the dump file.

If the dump file does not include the actual content files associated with the objects you are loading, the operation reads the content from the storage areas of the dumped repository. This means that the owner of the repository that you are loading must have Read privileges at the operating system level for the storage areas in the source repository.

The load operation generates a dmi\_queue\_item for the dm\_save event for each object of type SysObject or a subtype that is loaded into the target repository. The event is queued to the dm\_fulltext\_index\_user user account. This ensures that the objects are added to the index of target repository. You can turn off this behavior. For more information, see [“Turning off save event generation during load operations” on page 106](#).

Loading a repository is accomplished by creating and saving a load record object. The act of saving the object starts the operation.



**Note:** The load operation performs periodic commits to the repository. Consequently, you cannot load a repository if you are in an explicit transaction. The Documentum CM Server does not allow you to save a load record object if you are in an explicit transaction. Similarly, you cannot perform a revert or destroy operation on a load record object if you are in an explicit transaction.

#### 4.2.6.12.1 Refreshing repository objects from a dump file

Generally, when you load objects into a repository, the operation does not overwrite any existing objects in the repository. However, in two situations overwriting an existing object is the desired behavior:

- When replicating content between distributed storage areas
- When restoring archived content

In both situations, the content object that you are loading into the repository could already exist. To accommodate these instances, the load record object has a relocate property. The relocate property is a Boolean property that controls whether the load operation assigns new object IDs to the objects it is loading.

The type and predicate properties are for internal use and cannot be used to load documents of a certain type.

#### 4.2.6.12.2 Loading job objects

If you dump and load job objects, the load operation automatically sets the job to inactive in the new repository. This ensures that the job is not unintentionally started before the load process is finished and it allows you the opportunity to modify the job object if needed. For example, to adjust the scheduling to coordinate with other jobs in the new repository.

The load operation sets jobs to inactive (`is_inactive=TRUE`) when it loads the jobs, and sets the `run_now` property of jobs to FALSE.

If the load operation finds an existing job in the target repository that has the same name as a job it is trying to load, it does not load the job from the dump file.

#### 4.2.6.12.3 Loading registered tables

When you load a registered table, the table permits defined for that table are carried over to the target repository.

#### 4.2.6.12.4 Turning off save event generation during load operations

During a load operation, every object of type `SysObject` or `SysObject` subtype loaded into the target repository generates a save event. The event is queued to the `dm_fulltext_index_user`. This behavior ensures that the object is added to the target index of the repository.

The behavior is controlled by the load parameter called `generate_event`. The parameter is T by default. If you do not want the load operation to queue save events to the `dm_fulltext_index_user`, set the parameter to F for the operation. The parameter is set in the `load_parameter` property as:

```
generate_event=F
```

#### 4.2.6.12.5 Loading a new repository

New repositories are not empty. They contain various cabinets and folders created by the installation process, such as:

- A user object for the repository owner
- A cabinet for the repository owner
- The docu group
- The System cabinet, which contains a number of subfolders
- The Temp cabinet

When you load a dump file into a new repository, these objects are not replaced by their counterparts in the dump file because they already exist in the new repository.

However, if you have changed any of these objects in the source repository (the source of the dump file), the changes are lost because these objects are not loaded. For example, if you have added any users to the docu group or if you have altered permissions on the System cabinet, those changes are lost.

To make sure that any changes you have made are not lost, fetch from the source repository any of the system objects that you have altered and then use the Dump method to get a record of the changes. For example, if the cabinet of repository owner was modified, use the following command sequence to obtain a listing of its property values:

```
fetch,c,cabinet_iddump,c,1
```

After the load operation, you can fetch and dump the objects from the new repository, compare the new dump results with the previous dump results, and make any necessary changes.

#### 4.2.6.12.6 preLoad utility

OpenText Documentum CM provides a utility that you can run on a dump file to tell you what objects that you must create in the new repository before you load the dump file. The utility can also create a DQL script that you can edit and then run to create the needed objects. The syntax for the preload utility is:

```
preload repository [-Username] -Ppassword -dump_file filename [-script_file name]
```

- *repository* is the name of the repository into which you are loading the dump file.
- *filename* is the name of the dump file.
- *name* defines a name for the output DQL script.

If you do not include a username, the current user is assumed.



**Note:** This utility does not report all storage areas in the source repository, but only those that have been copied into the dump file.

#### 4.2.6.12.7 Load procedure for new repositories

Use the procedure in this section to load a dump file into a new repository.



**Note:** You cannot perform this procedure in an explicit transaction because the load operation performs periodic commits to the repository. Documentum CM Server does not allow you to save the load record object to start the load operation if you are in an explicit transaction.

##### To load a dump file into a new repository:

1. Create the repository.



##### Notes

- If the repository shares any directories with the source repository, you must assign the repository an ID that differs from the source repository ID.
- If the old and new repositories have different owners, make sure that the new repository owner has Read privileges in the storage areas used by the old repository if the old repository was not dumped with the include\_content property set to TRUE.

2. Create the necessary storage objects and associated location objects in your new repository.

Each storage object in your source repository must have a storage object with the same name in the new repository. The filestore objects in the new repository must reference location objects that point to actual directories that differ from those referenced by the location objects in the source repository.

For example, suppose you have a file store object with the name storage\_1 in your source repository that points to the location object named engr\_store, which references the d:\documentum\data\enr (/u04/home/<installation\_owner>/data/enr) directory. In the new repository, you must create a file store object with the name storage\_1 that references a location object that points to a different directory.



**Note:** The location objects can be named with different names or they can have the same name. Either option is acceptable.

3. If your storage areas in the source repository had associated full-text indexes, create corresponding fulltext index objects and their location objects in the new repository. Note that these have the same naming requirements as the new storage objects described in “[Load procedure for new repositories](#)” on page 108.
4. Create and save the following script:

```
create,c,dm_load_record  
set,c,1,file_name  
full_path_of_dump_filesave,c,1  
getmessage,c
```

5. Log in as the owner of the installation and use IAPI to execute the script.

When you start IAPI, connect to the new repository as a user who has Sysadmin privileges in the repository.

6. After the load completes successfully, you can destroy the load object:

```
destroy,c,load_object_id
```



### Notes

- Destroying the load object cleans the load object record objects that are generated by the loading process and old state information.
- If you created the dump file by using a script, move the dump file to archival storage or destroy it after you successfully load the file. You cannot successfully execute the script again if you leave the dump file in the location where the script created it. Documentum CM Server does not overwrite an existing dump file with another dump file of the same name.
- If Documentum CM Server crashes during a load, you can fetch the Load Object and save it again, to restart the process. Documentum CM Server begins where it left off when the crash occurred.

#### 4.2.6.12.8 DocApps

DocApps are not dumped when you dump a repository. Consequently, after you load a new repository, install and run the DocApp installer to reinstall the DocApps in the newly loaded repository.

#### 4.2.6.13 Generating dump and load trace messages

You can activate tracing during dump and load operations to generate trace messages in the Documentum CM Server session log.

To activate tracing, use a setServerTraceLevel method.

The trace information includes:

- Whether Documentum CM Server fails to dump or load an object
- The query used to search for matching objects for a dump or load operation
- The current progress and status of a dump or load operation

## 4.2.7 Repository maintenance

Repositories should be cleaned up regularly as part of a maintenance schedule. Cleaning a repository involves removal of:

- Orphaned content files

When users delete a document, or any object that has a content file associated with it, the system deletes the object and marks the content as an orphan. The system does not delete the actual content file. This must be done using the dmclean utility.

- Unwanted document versions and renditions
- Orphaned annotations and internal ACLs

An annotation is orphaned when it is detached from all documents or other objects to which it was attached.

An internal ACL is orphaned when it is no longer referenced by any object.

- Aborted workflows

A workflow that has been stopped by the execution of an Abort method is an aborted workflow.

- Old log files

### To clean a repository:

1. Perform a complete backup of the repository.
2. Delete unwanted versions of documents.

You can delete only versions created before a certain date or by a certain author or delete all but the CURRENT version from one or more version trees.

- To delete selected versions of documents, use the DELETE...OBJECT statement.

Identify the documents to delete by their creation date, modification date, or some other criteria that you choose. For example, the following statement deletes all documents that have not been changed since January 1, 2000:

```
DELETE "dm_document" OBJECTS  
WHERE "r_modify_date" < DATE('01/01/2000')
```

- To delete versions from a version tree, use a IDfSysObject.prune method.  
  
Prune deletes all unwanted versions on a specified tree or branch of a tree. An unwanted version is any version that has no symbolic label and that does not belong to a virtual document. The Javadocs contains information for the usage of the method.
- 3. Delete unused renditions.  
  
A rendition is represented in the repository by a content object that points to the source document and by a content file.

To delete a rendition (without deleting its source document, first update the content object for the rendition to remove its reference to the source document.

For example, the following UPDATE...OBJECT statement updates all server- and user-generated renditions created before January 1, 2000:

```
UPDATE "dmr_content" OBJECTS
SET "parent_count" = 0,
TRUNCATE "parent_id",
TRUNCATE "page"
WHERE "rendition" != 0 AND "set_time" < DATE('01/01/2000')
```

The updates in the preceding example statement detach the affected renditions from their source documents, effectively deleting them from the repository.

4. Clean the temp directory by deleting the temporary files in that location.

You can determine the location of the temp directory with the following query:

```
SELECT "file_system_path" FROM "dm_location"
WHERE "object_name" = 'temp'
```

5. Delete any unwanted dmi\_queue\_item objects.

Every time an object is placed in the inbox of a user, a dmi\_queue\_item object is created. When the object is removed, the queue item object is not destroyed, but it is marked in the repository as dequeued. Use the DELETE...OBJECT statement to remove dmi\_queue\_item objects.

For example, the following statement removes all queue items objects that were dequeued before January 1, 2000:

```
DELETE "dmi_queue_item" OBJECTS
WHERE "dequeued_date" < DATE('01/01/2000')
AND "delete_flag"=true
```

6. Run the dmclean utility to remove orphaned content files, orphaned annotations and ACLs, and aborted workflows. You can execute the Dmclean administration tool or run the dmclean utility manually. For more information about the utility, see “[Dmclean](#)” on page 372.

7. Delete or archive old server logs, session logs, trace files, and old versions of the product.

Session logs are located in the %DOCUMENTUM%\dba\log\repository\_id (\$DOCUMENTUM/dba/log/repository\_id) directory.

Documentum CM Server and connection broker log files are found in the %DOCUMENTUM%\dba\log (\$DOCUMENTUM/dba/log) directory. The server log for the current server session is named *repository\_name.log*. The log for the current instance of the connection broker is named *docbroker.hostname.log*. Older versions of these files have the extension .save and the time of their creation appended to their name.

On Windows, you can use the del command or the File Manager to remove unwanted session logs, server logs, and connection broker logs. On Linux, use the rm command.

## 4.2.8 Checking consistency

Documentum CM Server provides the Consistency Checker, a tool that scans a repository and reports any inconsistencies. Inconsistencies typically include type or object corruptions, objects that reference a user, group, or other object that does not exist, and so forth. The tool does not fix the inconsistencies. Contact OpenText Global Technical Services for assistance in correcting errors found by the consistency checker.

The Consistency Checker tool is a job that can be run from the command line or using Documentum Administrator. For more information about running the job in Documentum Administrator, see “[Running jobs](#)” on page 440.

The job generates a report that lists the checked categories and any inconsistencies that were found. The report is saved in the /System/Sysadmin/Reports/ConsistencyChecker directory. If no errors are found, the current report overwrites the previous report. If an error is found, the current report is saved as a new version of the previous report. By default, the Consistency Checker job is active and runs once a day.

OpenText recommends that you run this tool on a repository before upgrading the repository to a new version of the Documentum CM Server.

### 4.2.8.1 Running the job from a command line

The Consistency Checker job is implemented as the consistency\_checker.ebs script. To run the script from the command line, enter the following syntax at the command-line prompt:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point --repository_name superuser password
```

where repository\_name is the name of the repository that is checked, superuser is the user name of a repository superuser, and password is the password of the superuser account.

The results of the checks are directed to standard output.

### 4.2.8.2 Example report

The following example describes a Consistency Checker report (in this case, the tool detected five inconsistencies in the Users & Groups section):

```
Beginning Consistency Checks.....  
  
Repository Name: buzzard  
Server Version: 5.1.0.63 Win32.SQLServer  
Database: SQLServer  
  
#####  
##  
## CONSISTENCY_CHECK: Users & Groups  
##  
##      Start Time: 09-10-2002 10:15:55  
##
```

```

#######
## Checking for users with non-existent group
## WARNING CC-0001: User 'docu' belongs to
## non-existent group ''
## WARNING CC-0001: User 'engr' belongs to
## non-existent group ''
## WARNING CC-0001: User 'marketing' belongs to
## non-existent group ''
## WARNING CC-0001: User 'nagboat' belongs to
## non-existent group ''
## WARNING CC-0001: User 'admingroup' belongs to
## non-existent group ''
Rows Returned: 5

Checking for users belonging to groups not in dm_user
Checking for users not listed in dmi_object_type
Checking for groups not listed in dmi_object_type
Checking for groups belonging to non-existent groups
Checking for groups with non-existent super groups

#####
###
###
## CONSISTENCY_CHECK: ACLs ##
###
## Start Time: 09-10-2002 10:15:55
###
#######
## Checking for ACLs with non-existent users
## Checking for ACLs with missing dm_acl_r table entries
## Checking for sysobjects with acl_domain set to
##   non-existent user
## Checking for sysobjects that belong to
##   non-existent users
## Checking for sysobjects with non-existent ACLs
## Checking for ACL objects with missing dm_acl_s entry
## Checking for ACL objects with r_accessor_permit
##   value but missing r_accessor_name value
## Checking for ACL objects with r_accessor_name value
##   but missing r_accessor_permit value
## Checking for ACL objects with r_is_group value but
##   missing r_accessor_permit value
## Checking for ACL objects with r_is_group value but
##   missing r_accessor_name value
## Checking for ACL object with r_accessor_name value
##   but missing r_is_group value
## Checking for ACL object with r_accessor_permit value
##   but missing r_is_group value

#####
###
###
## CONSISTENCY_CHECK: Sysobjects
###
###
## Start Time: 09-10-2002 10:15:58
###
#######
## Checking for sysobjects which are not referenced in
## dmi_object_type
## Checking for sysobjects that point to non-existent
##   content
## Checking for sysobjects that are linked to non-existent
##   folders
## Checking for sysobjects that are linked to non-existent

```

```
primary cabinets
Checking for sysobjects with non-existent i_chronicle_id
Checking for sysobjects with non-existent i_antecedent_id
Checking for sysobjects with missing
dm_sysobject_r entries
Checking for sysobjects with missing
dm_sysobject_s entry

#####
## 
## 
## CONSISTENCY_CHECK: Folders and Cabinets
##
##      Start Time: 09-10-2002 10:16:02
##
## 
#####

Checking for folders with missing dm_folder_r table
entries
Checking for folders that are referenced in dm_folder_r
but not in dm_folder_s
Checking for dm_folder objects that are missing an
entry in dmi_object_type
Checking for dm_folder objects that are missing
corresponding dm_sysobject entries
Checking for folders with non-existent ancestor_id
Checking for cabinet that have missing dm_folder_r
table entries
Checking for cabinets that are missing an entry in
dmi_object_type
Checking for folder objects with missing
dm_sysobject_r entries
Checking for folder objects with null r_folder_path

#####
## 
## 
## CONSISTENCY_CHECK: Documents
##
##      Start Time: 09-10-2002 10:16:03
##
## 
#####

Checking for documents with a dm_sysobject_s entry
but no dm_document_s entry
Checking for documents with missing dm_sysobect_s
entries
Checking for documents with missing dmi_object_type
entry

#####
## 
## 
## CONSISTENCY_CHECK: Content
##
##      Start Time: 09-10-2002 10:16:03
##
## 
## 
#####

Checking for content objects that reference
non-existent parents
Checking for content with invalid storage_id
Checking for content objects with non-existent format

#####
##
```

```

##  

## CONSISTENCY_CHECK: Workflow  

##  

##  

##      Start Time: 09-10-2002 10:16:03  

##  

##  

#####  

Checking for dmi_queue_item objects with non-existent  

queued objects  

Checking for dmi_workitem objects that reference  

non-existent dm_workflow objects  

Checking for dmi_package objects with missing  

dmi_package_s entries  

Checking for dmi_package objects that reference  

non-existent dm_workflow objects  

Checking for workflow objects with non-existent  

r_component_id  

Checking for workflow objects with missing  

dm_workflow_s entry  

Checking for work item objects with missing  

dm_workitem_s entry  

#####  

##  

##  

## CONSISTENCY_CHECK: Types  

##  

##      Start Time: 09-10-2002 10:16:04  

##  

##  

#####  

Checking for dm_type objects with a non-exis-  

t dm_type_info object  

Checking for dm_type_info objects with a non-existent  

dm_type object  

Checking for type objects with corrupted property  

positions  

Checking for types with invalid property counts  

#####  

##  

##  

## CONSISTENCY_CHECK: Data Dictionary  

##  

##      Start Time: 09-10-2002 10:16:04  

##  

##  

#####  

Checking for duplicate dmi_dd_attr_info objects  

Checking for duplicate dmi_dd_type_info objects  

Checking for any dmi_dd_attr_info objects that are  

missing an entry in dmi_dd_common_info_s  

Checking for any dmi_dd_type_info objects that are  

missing an entry in dmi_dd_common_info_s  

Checking for any dmi_dd_attr_info objects that are  

missing an entry in dmi_dd_attr_info_s  

Checking for any dmi_dd_type_info objects that are  

missing an entry in dmi_dd_type_info_s  

#####  

##  

##  

## CONSISTENCY_CHECK: Lifecycles  

##  

##      Start Time: 09-10-2002 10:16:11

```

```
##  
#####  
Checking for sysobjects that reference non_existent  
    policy objects  
Checking for any policy objects that reference  
non-existent types in included_type  
Checking for any policy objects with missing  
dm_sysobject_s entry  
Checking for any policy objects with missing  
dm_sysobject_r entries  
Checking for policy objects with missing dm_policy_r  
    entries  
Checking for policy objects with missing dm_policy_s  
    entry  
#####  
##  

```

```
Consistency Checker completed successfully
Total number of inconsistencies found: 5
Disconnected from the server.
```

### 4.2.9 Changing the repository owner password

If you need to change the password in the database used by the repository owner account (also referred to as the database owner account, and listed as database\_owner in the server.ini file), use the following procedure:

1. Shut down the repository.
2. Change the repository owner account password in the database.
3. Edit the dbpasswd.txt file to contain one line with the new password in plain text.
4. Encrypt the dbpasswd.txt file. From the \$DM\_HOME/bin/ directory, use the following command:  
For password-based AEK key:  

```
dm_encrypt_password -docbase <docbase_name> -rdbms -encrypt
<database_password> -keyname <keyname> [-passphrase <passphrase>]
```
5. Start the repository.

## 4.3 Adding repositories

Adding repositories requires creating a repository running the Documentum Server Manager on Windows or the server configuration program on Linux.

### To create a repository on Windows:

1. Click **Start > Programs > Documentum > Documentum Server Manager** to start the Documentum Server Manager.
2. Click the **Utilities** tab, then click **Server Configuration**.  
The server configuration program starts.
3. Click **Next** and follow the configuration instructions on the screen.

### To create a repository on Linux:

1. Start the server configuration program.
2. Follow the instructions in the server configuration sections to create new repositories.

For more information about pre-installation checklists and the server configuration options, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

## 4.4 Federations

A federation is a set of two or more repositories bound together to facilitate the management of a multi-repository distributed configuration. Federations share a common name space for users and groups and project to the same connection brokers.

Global users, global groups, and global permission sets are managed through the governing repository, and have the same property values in each member repository within the federation. For example, if you add a global user to the governing repository, that user added to all the member repositories by a federation job that synchronizes the repositories.

One enterprise can have multiple repository federations, but each repository can belong to only one federation. Repository federations are best used in multi-repository production environments where users share objects among the repositories. We do not recommend creating federations that include production, development, and test repositories, because object types and format definitions change frequently in development and test environments, and these must be kept consistent across the repositories in a federation.

The repositories in a federation can run on different operating systems and databases. Repositories in a federation can have different server versions; however, the client running on the governing repository must be version-compatible with the member repository in order to connect to it.

To create or modify federations, you do not have to be connected to a repository in the federation. To add a repository to a federation, your Documentum Administrator connection broker list must include a connection broker to which the particular repository projects.

For more information about the prerequisites before setting up a repository federation, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

### 4.4.1 Creating or modifying federations

Before you create a federation, obtain the user name and password of a superuser account in each repository.

All repositories in a federation must project to the same connection brokers. When you create a federation, Documentum Administrator updates the connection broker projection information in the server configuration object for each member repository. No manual configuration is necessary.

The repositories in a federation can run on different operating systems and databases. Repositories in a federation can have different server versions; however, the client running on the governing repository must be version-compatible with the member repository in order to connect to it.

**Table 4-3: Federation properties**

<b>Field</b>	<b>Description</b>
<b>Info tab</b>	
<b>Name</b>	Type the name of the new federation.
<b>Make All Governing Repository Users &amp; Groups Global</b>	Select to make all users and groups in the governing repository global users and global groups.
<b>Active</b>	This option is available if you are modifying an existing federation. To change the status of an existing federation, select or clear the Active checkbox.
<b>User Subtypes tab</b>	
<b>Add</b>	<p>Click <b>Add</b> to add user subtypes.</p> <p>If there are user subtypes in the repository, a list of user subtypes is displayed on the Choose a user subtype page. Select the user subtypes to propagate to member repositories.</p>
<b>Members tab</b>	
<b>Add</b>	<p>Click <b>Add</b> to add member repositories.</p> <p>Select the repositories that you want to be member repositories and click <b>Add</b>.</p> <p>Click <b>Edit</b> to edit a member repository. The <b>Edit</b> button will be available only after adding more than one repository.</p> <p>To remove any member repositories from the Selected Items list, select them and then click <b>Remove</b>.</p>
<b>Name</b>	The login name of a superuser account that is configured for the repository.
<b>Password</b>	The password of a superuser account this is configured for the repository.
<b>Skip this member and continue authentication</b>	Select this option if you want to skip entering the name and password at this time.

For more information about federation properties, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide* (EDCSY250400-IGD). For more information about creating or modifying federations, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

#### 4.4.2 Adding, modifying, or deleting federation members

You can add or delete federation member repositories using the Members tab on the Federation Configuration Properties page.

For more information about adding, modifying, or deleting federation members, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

#### 4.4.3 Deleting federations

For more information about deleting federations, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

You can make a federation inactive by accessing the Info page of the federation and clearing the **Active** check box.

#### 4.4.4 Connecting to the governing repository or a federation member

Provide the login information for the governing repository or a federation member.

For more information about connecting to the governing repository or a federation members, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

#### 4.4.5 Choosing user subtypes

On the **New Federation Configuration - User Subtypes or Federation Configuration Properties - User Subtypes** page, choose user subtypes to be propagated to all members of the federation. The type itself must be created in each repository in the federation. This page ensures that users of that particular subtype are propagated to the member repositories.

For more information about choosing user subtypes, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

#### 4.4.6 Choosing repository federation members

Select the members of a repository federation. The repositories listed are all repositories not already in a federation that are known to all the connection brokers in your preferences. You can sort the list of repositories by repository name or connection broker.

For more information about choosing repository federation members, see *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD).

# Chapter 5

## Managing sessions

### 5.1 dfc.properties file

The dfc.properties file contains most of the configuration parameters that specify how Foundation Java API handles repository sessions. The configuration parameters are stored as a key and a corresponding value. For example, the dfc.properties file contains keys that specify which connection brokers are used to obtain a session, how many sessions are allowed for one user, and enable persistent client caching. Many keys have default values, but some must be explicitly set by an administrator or application.

Some of the keys in the file are dynamic that affect open sessions. Changing non-dynamic keys affects only future sessions. By default, Documentum CM Server checks every 30 seconds for changes in the dfc.properties file.

The dfc.properties keys and associated values are described in the dfcfull.properties file, which is installed with Foundation Java API. The keys in the dfc.properties file have the following format:

```
dfc.<category>. <name>=<value>
```

The *<category>* identifies the functionality, feature, or facility that the key controls. When adding a key to the dfc.properties file, both the category and the name, in addition to a value must be specified. For example:

```
dfc.data.dir= <value>
dfc.tracing.enable= <value>
dfc.search.ecs.broker_count = <value>
```

For OpenText Documentum CM web-based products, the dfc.properties file is packaged in the application WAR file.

For desktop applications and Documentum CM Server, the dfc.properties file is installed in the C:\Documentum\Config directory on Windows hosts, and the \$DOCUMENTUM\_SHARED/config directory on Linux hosts. The file can be edited using any text editor.

The dfc.properties file is a standard Java properties file. If a key value has a special character, use a backslash (\) to escape the character. In directory path specifications, use a forward slash (/) to delimit directories in the path.

## 5.2 Managing connection requests

When a client requests a connection, the request is sent to a connection broker, which returns server connection information to the client. There must be at least one connection broker identified in the dfc.properties file of the client. If multiple connection brokers are defined in the file, the system uses the additional connection brokers for backup or failover.

To specify a connection broker in the dfc.properties file, use the following keys:

```
dfc.docbroker.host[<n>]=<host_name>|<IP_address>      #required  
dfc.docbroker.port[<n>]=<port_number>    #optional
```

The [*<n>*] is a numeric index, where *<n>* is an integer starting with 1. All keys for a particular connection broker must have the same numeric index. If there are entries for multiple connection brokers, Foundation Java API contacts the connection brokers in ascending order based on the numeric index by default.

The *<host\_name>* is the name of the machine on which the connection broker resides. The *<IP\_address>* is the IP address of the machine.

The port is the TCP/IP port number that the connection broker is using for communications. The port number defaults to 1489 if it is not specified. If the connection broker is using a different port, you must include this key.

The following example defines two connection brokers for the client and because lapdog is not using the default port number, the port number is also specified in the file:

```
dfc.docbroker.host[1]=bigdog  
dfc.docbroker.port[1]=1489  
  
dfc.docbroker.host[2]=lapdog  
dfc.docbroker.port[2]=1491
```

Only the host specification is required. The other related keys are optional.

If you add, change, or delete the keys of a connection broker, the changes are visible immediately. You do not have to restart your session.

## 5.3 Defining the secure connection default for connection requests

All connections between Documentum CM Server and a client application are either secure or native (unsecured) connections. Which option is used for a particular connection depends on how the server is configured and what sort of connection is requested by the client application when it attempts to obtain a session. If the request does not specify what type of connection is requested, the connection type specified in the dfc.properties file, in the dfc.session.secure\_connect\_default key, is used.

There are four possible settings for this key:

- native

Only a native connections are allowed. If Foundation Java API cannot establish a native connection, the connection attempt fails.

- secure

Only secure connection are allowed. If Foundation Java API cannot establish a secure connection, the connection attempt fails.

- try\_secure\_first

A secure connection is preferred, but a native (unsecured) connection is excepted. Foundation Java API attempts to establish a secure connection first. If it cannot, it tries to establish a native connection. If that also fails, the connection attempt fails.

- try\_native\_first

A native connection is preferred, but a secure connection is also accepted. Foundation Java API attempts to establish a native connection first. If it cannot, it tries to establish a secure connection. If that also fails, the connection attempt fails.

The default setting for the key is try\_native\_first.

Specifying a connection type in the application overrides the default setting in the secure\_connect\_default key. *OpenText Documentum Content Management - Foundation Java API Development Guide (EDCPKCL250400-DGD)* contains information on how to specify it in an application. For information about configuring the server default for connections, read the Secure Connect Mode property in “[Modifying general server configuration information](#)” on page 32.

## 5.4 Modifying the connection request queue size

Documentum CM Server creates a socket listener for incoming connection requests. By default, the maximum backlog queue value is 200. The value can be changed on Windows by modifying the `listener_queue_length` key in the `server.ini` file. The key must be a positive integer value. Documentum CM Server passes the specified value to the `listen()` Windows Sockets call.

## 5.5 Stopping a session server

A kill method should be used to shut down a session server. Using a kill method requires system administrator or superuser privileges and the session ID. The session ID can be obtained using the `LIST_SESSIONS` or `SHOW_SESSIONS` administration method. The *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* contains more information on the administration methods.

A session can be terminated in one of three ways:

- Default kill

The default kill provides the least disruption to the end user. The targeted session terminates when it has no more open transactions and no more open collections. The client remains functional.

- After current request kill

An after current request kill provides a safe and more immediate means of terminating a session. If the session is not currently executing a request, the session is terminated. Transactions can be rolled back and collections can be lost.

- Unsafe kill

An unsafe kill can be used to terminate a session when all other techniques have failed and should be used with caution. It can result in a general server failure.

# Chapter 6

## Managing Java Method Servers

### 6.1 Java Method Servers

OpenText Documentum CM includes Java Method Server, a customized version of Tomcat to execute server Java methods. One Java Method Server is installed with each Documentum CM Server installation. You can use Documentum Administrator to modify existing Java Method Servers, but you cannot add new Java Method Servers from the Documentum Administrator interface. To add a Java Method Server, you have to run the server configuration program. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains more information on installing multiple Documentum CM Servers, Java Method Servers, and the supported Java Method Server failover configurations.

OpenText Documentum CM provides a servlet called DO\_METHOD to execute the server methods. The compiled servlet code is found in the mthdsvrlet.jar file located on the same host as Documentum CM Server. The file contains the IDmMethod class. Java Method Server runs as an independent process. The process can be stopped or started without recycling the Documentum CM Server. On Windows, the Java Method Server can be run as a Windows service or as a process.

The method server itself is a Java-based web application. Each time a method is invoked, the Documentum CM Server makes an HTTP request passing the name of the Java class which implements the method along with any specified arguments to a servlet which knows how to execute the specified method.



**Note:** The Java Method Server can also be used to execute Java methods that are not associated with a method object. Use an HTTP\_POST administration method to send the request to the Java method server. *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* contains information on the administration method.

Documentum Administrator provides a Java Method Server configuration page for:

- Viewing and updating Java Method Servers.
- Associating Documentum CM Servers with Java Method Servers.
- Viewing the Java Method Server status information in the Documentum CM Server memory cache.
- Resetting the Java Method Server information in the Documentum CM Server memory cache.

### 6.1.1 Viewing Java Method Server information

All available Java Method Server are displayed on the Java Method Server Configuration page. Users with superuser or system administrator privileges can access the Java Method Server Configuration page. To access the page, log into a repository and navigate to **Administration > Basic Configuration > Java Method Servers**.

Each Java Method Server is represented by a Java Method Server configuration object. The Java Method Server Configuration page displays information for all Java Method Server configuration objects in the repository.

**Table 6-1: Java method server information**

Column Label	Description
Name	The name of the Java Method Server configuration object.
Is Enabled	Specifies whether the Java method server is enabled or disabled.
Associated Content Servers	The Documentum CM Server with which the Java Method Server configuration object is associated.

The **Tools** menu on the Java Method Server Configuration page also provides the option to view information about all active Java method servers. Select **Tools > Active Java Method Servers List** to display the Active Java Method Servers List page.

### 6.1.2 Modifying Java Method Server configuration

Only users with superuser privileges can modify Java Method Server configurations.

**Table 6-2: Java Method Server configuration information**

Field	Description
Name	The name of the Java Method Server configuration.
Enable	Enables or disables the Java Method Server. Select this option to enable the Java Method Server configuration or deselect to disable the Java Method Server.
<b>Associated Content Servers</b>	

Field	Description
<b>Documentum Server</b>	The list of Documentum CM Servers that is associated with the Java Method Server configuration.  A Java Method Server configuration can be associated with one or more Documentum CM Servers. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-JGD)</i> contains more information on installing multiple Documentum CM Servers, Java Method Servers, and the supported Java Method Server failover configurations.
<b>Documentum Server location</b>	Specifies whether the Java Method Server is associated with a remote Content Server. Valid values are: <ul style="list-style-type: none"> <li>• <i>Java Method Server for primary Documentum Server</i>: The Accelerated Content Services is local.</li> <li>• <i>Java Method Server for secondary (or additional) Documentum Server</i>: The Accelerated Content Services is remote.</li> </ul>
<b>Add</b>	Click <b>Add</b> to add and associate a Documentum CM Server with the Java Method Server configuration.  The Servlet URL Editor page displays. Select the Documentum CM Server and intended purpose, as described in <a href="#">“Adding or modifying Associated Content Servers” on page 128</a> .
<b>Edit</b>	Select the Documentum CM Server and click <b>Edit</b> to modify the Documentum CM Server associated with the Java Method Server configuration.  The Servlet URL Editor page displays. Modify the intended purpose, as described in <a href="#">“Adding or modifying Associated Content Servers” on page 128</a> .
<b>Remove</b>	Select the Documentum CM Server and click <b>Remove</b> to remove the Documentum CM Server from the Java Method Server configuration.
<b>Java Method Server Servlet URLs</b>	
<b>Name</b>	The name of the Java servlet.
<b>URL</b>	The location of the Java servlet.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on modifying a Java Method Server configuration.

### 6.1.3 Adding or modifying Associated Content Servers

Use the Associated Content Servers page to add or modify Documentum CM Servers that are associated with a Java Method Server.

*OpenText Documentum Content Management - Administrator User Guide* (*EDCAC250400-UGD*) contains the instructions on adding or modifying Associated Content Servers.

**Table 6-3: Associated Content Servers information**

Column Label	Description
<b>Documentum Server</b>	The name of the Documentum CM Server associated with the Java Method Server.  To add a Documentum CM Server, select the Documentum CM Server from the list.  The list displays Documentum CM Server that were previously installed on the host machine using the Documentum CM Server Configuration program. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide</i> ( <i>EDCSY250400-IGD</i> ) contains more information on installing multiple Documentum CM Servers, Java Method Servers, and the supported Java Method Server failover configurations.
<b>Documentum Server location</b>	Specifies whether the Java Method Server is associated with a remote Content Server. Valid values are: <ul style="list-style-type: none"><li>• <i>Java Method Server for primary Documentum Server</i>: The Accelerated Content Services is local.</li><li>• <i>Java Method Server for secondary (or additional) Documentum Server</i>: The Accelerated Content Services is remote.</li></ul>

### 6.1.4 Viewing active Java Method Server

All active Java method servers are displayed on the Active Java Method Servers List.

**Table 6-4: Active Java Method Server information**

Field	Description
<b>Associated Content Server</b>	The Documentum CM Server with which the Java Method Server cache is associated.
<b>Last Refreshed Time</b>	The last time the Documentum CM Server Java Method Server cache was reset.
<b>Incremental Wait Time on Failure</b>	<p>The time Documentum CM Server waits before contacting the Java Method Server, if the Java Method Server fails to respond.</p> <p>The wait time is doubled each time the Java Method Server fails to respond until the maximum wait time is reached.</p>
<b>Maximum Wait Time on Failure</b>	The maximum wait time Documentum CM Server keeps trying to contact the Java Method Server, if the Java Method Server fails to respond.
<b>Java Method Server in Use</b>	The name of the active Java method server that was used last time.
<b>Java Method Servers associated with the Documentum Server</b>	
<b>Name</b>	The name of the Java Method Server configuration object.
<b>Is Enabled</b>	Specifies whether the Java Method Server is enabled or disabled.
<b>Status</b>	The current status of the Java Method Server configuration object.
<b>Documentum Server location</b>	<p>Specifies whether the Java Method Server is associated with a remote Content Server. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>Java Method Server for primary Documentum Server</i>: The Accelerated Content Services is local.</li> <li>• <i>Java Method Server for secondary (or additional) Documentum Server</i>: The Accelerated Content Services is remote.</li> </ul>
<b>Last Failure Time</b>	The last time the Java Method Server failed to respond.
<b>Next Retry Time</b>	The next time the Documentum CM Server tries to contact the Java Method Server, if the Java Method Server fails to respond.

Field	Description
<b>Failure Count</b>	The number of times the Java Method Server failed to respond.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing active Java method servers.

## 6.2 Java methods

Technically, all OpenText Documentum CM Java methods are simple Java classes. A plain Java class becomes a Java method if it implements either the IDfMethod or IDmMethod interfaces. If a program starts a repository session, the program should call an explicit Disconnect when the session is finished.

Methods are deployed as a BOF module and executed on a Java method server. The methods must have the following property values:

- The method must implement the IDfMethod interface.
- The module must be a simple module, one which implements the IDfModule interface.
- The method\_verb property of the dm\_method object must be set to the module name, not the class name.
- The method\_type property must be set to Java.
- The use\_method\_server property must be set to T (TRUE).
- The run\_as\_server property must be set to T (TRUE).



### Notes

- Linux users who are authenticated against a Windows domain cannot execute methods under their own accounts. All methods executed by such users must be run with run\_as\_server set to TRUE.
- OpenText Documentum CM does not provide basic support for resolving problems encountered when creating or executing custom Java methods or classes. For help, contact OpenText Global Technical Services.

## 6.3 Recording Java method output

If the DO\_METHOD method is executed on the Java method server, OpenText Documentum CM recommends to include the IDmMethod interface in the program. The interface saves the response to the repository in a document. The interface can also be used to capture error or trace messages from the Java method or servlet.

```
package com.documentum.mthdservlet;
import java.io.OutputStream;
import java.util.Map;

/**
 * Interface for Java Methods that are invoked by the
 * Documentum Server.
 *
 */

public interface IDmMethod
{

    /**
     * Serves as the entry point to a Java method (installed
     * in application server) executed by the Content
     * Server DO_METHOD apply method.
     *
     * @param parameters A Map containing parameter names as keys
     * and parameter values as map values. The keys in the parameter
     * are of type String.
     * The values in the parameter map are of type String array.
     * (This map corresponds to the string ARGUMENTS passed by the
     * DO_METHOD apply call.)
     *
     * @param output OutputStream to be sent back as the
     * HTTP response content, to be saved in the repository
     * if SAVE_RESULTS was set to TRUE in the DO_METHOD apply call.
     * NOTE: This output stream is NULL if the DO_METHOD was
     * launched asynchronously. Always check for a null before
     * writing to the OutputStream.
     */
    public void execute(Map parameters, OutputStream output) throws
        Exception;
}
```

## 6.4 Deploying Java methods

Java methods are developed as self-contained BOF modules. Developing and deploying a Java method has the following advantages:

- Developers can package and deploy the Java server method implementation in the same DAR file as the dm\_method definition.
- The Java method is self contained and is stored automatically in the default location for the module.
- The Java method server does not have to be restarted to implement the method.



**Note:** We strongly recommend that developers avoid using the dba \\java\_methods directory to deploy Java methods.

## 6.5 Adding additional servlets to Java Method Server

To use the HTTP\_POST administration method, you must write and install the servlet or servlets that handles those calls. Use the following procedure to implement such a servlet:

**To implement a new servlet:**

1. Write the servlet.
2. Install the servlet on the Java method server.
3. Update the server configuration object for each server from which HTTP\_POST methods might originate.

Add the name of new servlet to the app\_server\_name property and the URI of servlet to the app\_server\_uri property.

Use Documentum Administrator to modify the server configuration object.

4. Select **Re-initialize**.
5. Click **Check In**.

# Chapter 7

## Managing LDAP servers

### 7.1 LDAP servers

An Lightweight Directory Access Protocol (LDAP) directory server is a third-party product that maintains information about users and groups. Documentum CM Servers use LDAP directory servers for managing users and groups from a central location.

It is not necessary for all users and groups in a repository to be managed through an LDAP directory server. A repository can have local users and groups in addition to the users and groups managed through a directory server. You can use more than one LDAP directory server for managing users and groups in a particular repository.

Using an LDAP server provides a single place for making additions and changes to users and groups. Documentum CM Server runs a synchronization job to automatically propagate the changes from the directory server to all the repositories using the directory server.

The LDAP support provided by Documentum CM Server allows mapping LDAP user and group attributes to user and group repository properties or a constant value. When the user or group is imported into the repository or updated from the directory server, the repository properties are set to the values of the LDAP properties or the constant. The mappings are defined when Documentum CM Server creates the LDAP configuration. The mappings can be modified later.

Using an LDAP directory server includes the following constraints:

- The `changePassword` method is not supported for users managed through an LDAP directory server.
- Dynamic groups are supported only on Sun Java System directory servers.
- The LDAP synchronization job must have at least read access to a unique identifier on the directory server, as follows:
  - **nsuniqueid** on SunDirectory processor
  - **objectguid** on Active Directory Server
  - **ibm-entryuuid** on IBM
  - **guid** on Novell
  - **orclguid** on Oracle

Apart from the unique identifiers, all the attributes that have been mapped in the LDAP configuration object should also have read access in the directory server.

### 7.1.1 Viewing LDAP server configurations

LDAP directory server configurations are managed under the **Administration > Basic Configuration > LDAP Servers** node. You can configure and map your existing LDAP configuration to a Documentum CM Server. Each LDAP server is associated with an LDAP configuration object. You must have superuser privileges to create, view, modify, or delete LDAP configuration objects.

Select **Administration > Basic Configuration > LDAP Servers** to view all primary LDAP servers that are configured to the repository. If there are no LDAP servers configured to the repository, Documentum Administrator displays the message *No LDAP Server Configurations*. “[LDAP server configuration page properties](#)” on page 134 describes the properties that are displayed on the LDAP Server Configuration page.

From the LDAP Server Configuration page, you can:

- Add new LDAP servers
- View or modify existing LDAP server properties
- Synchronize LDAP servers
- Duplicate an existing LDAP server configuration
- Delete existing LDAP servers configurations

**Table 7-1: LDAP server configuration page properties**

Field	Value
<b>Name</b>	The name of the LDAP configuration object.
<b>Hostname</b>	The name of the host on which the LDAP directory server is running.
<b>Port</b>	The port number where the LDAP directory server is listening for requests.
<b>SSL Port</b>	The SSL port for the LDAP directory server.
<b>Directory Type</b>	The directory type used by the LDAP directory server.
<b>Import</b>	Indicates if users and groups, groups and member users, or users only are imported.
<b>Sync Type</b>	Indicates if synchronization is full or incremental.
<b>Failover</b>	Indicates if failover settings have been established for the primary server.
<b>Enabled</b>	Indicates whether the LDAP server is active.

## 7.1.2 Adding or modifying LDAP server configurations

When adding an LDAP directory server to an existing OpenText Documentum CM installation, the users and groups defined in the LDAP directory server are given precedence. The user or group entry in the directory server matches a user or group in the repository, the repository information is overwritten by information in directory server in case synchronization type is set to full synchronization on Sync and Authentication tab. To run the LDAP synchronization job for nested groups, new users and groups are not synchronized in the repository.

To create a new LDAP configuration, you need the following information about the LDAP directory server:

- The name of the host where the LDAP directory server is running
- The port where the LDAP directory server is listening
- The type of LDAP directory server
- The binding distinguished name and password for accessing the LDAP directory server
- The person and group object classes for the LDAP directory server
- The person and group search bases
- The person and group search filters
- The OpenText Documentum CM attributes that you are mapping to the LDAP attributes



### Notes

- Make sure that the binding user has the List Contents and Read Property (LCRP) permission on the deleted objects container for configuring the LDAP objects. Otherwise, the deleted users in the Active Directory server are shown as active LDAP users in the repository. If the optional job argument for LDAP Synchronization, `container_for_deleted` is set, the argument value will be used instead of Deleted Objects while checking for objects deleted at Active Directory.
- To avoid the null pointer exception while using `ldap_matching_rule_in_chain` for nested group synchronization iteration through a collection of objects retrieved from Active Directory, make sure that you set the value of `ldap_matching_rule_in_chain` to `<false>`. By default, the value is `<true>`.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding or modifying an LDAP server configuration.

Documentum CM Server creates an `ldap<objectID>.cnt` password when you create the LDAP configuration object. If you have more than one Documentum CM Server associated with the repository, the password file must be copied to each Documentum CM Server in the environment or authentication fails.

### 7.1.2.1 LDAP server configuration properties

“LDAP server configuration properties” on page 136 describes the properties on the Info tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 7-2: LDAP server configuration properties**

Field	Description
<b>Name</b>	The name of the new LDAP configuration object.  This field is read-only if you are viewing or modifying the LDAP configuration object.
<b>Status</b>	Select the Enable this LDAP Configuration checkbox to enable the LDAP configuration.
<b>Directory Type</b>	The Release Notes documents for your version of Documentum CM Server contains information on which LDAP server versions are supported.  Options are: <ul style="list-style-type: none"> <li>• Sun ONE/Netscape/iPlanet Directory Server (default)</li> <li>• Microsoft Active Directory</li> <li>• Microsoft ADAM</li> <li>• Oracle Internet Directory Server</li> <li>• IBM Directory Server</li> <li>• Novell eDirectory</li> </ul>
<b>Hostname / IP Address</b>	The name of the host on which the LDAP directory server is running. <div style="background-color: #e0e0e0; padding: 10px; margin-top: 10px;">  <b>Caution</b>            For the 7.0 release, use only the hostname and not the IP address. However, you can use both the hostname and IP address in pre-7.0 releases.         </div>
<b>Port</b>	The port number where the LDAP directory server is listening for requests.  The default is 389.
<b>Binding Name</b>	The binding distinguished name used to authenticate requests to the LDAP directory server by Documentum CM Server or the check password program.

Field	Description
<b>Binding Password</b>	<p>The binding distinguished password used to authenticate requests to the LDAP directory server by Documentum CM Server or the check password program.</p> <p>The Binding Password field only appears on the New LDAP Server Configuration - Info page.</p>
<b>Confirm Password</b>	<p>If adding a new LDAP server configuration, re-enter the binding password for verification.</p> <p>The Confirm Password field only appears on the New LDAP Server Configuration page.</p>
<b>Set</b>	<p>Click to access the LDAP Server Configuration Properties page to set the password. This link appears only on the LDAP Server Configuration Properties - Info page.</p>
<b>Use SSL</b>	<p>Specifies whether SSL is used for authentication.</p>
<b>SSL Port</b>	<p>Specifies the SSL port. This option only displays when the <b>Use SSL</b> option is selected.</p> <p>Enter 636 for the SSL port value.</p>
<b>Certificate Location</b>	<p>Specifies the location of the LDAP certificate database. If you selected <b>Use SSL</b>, the default location is <i>ldapcertdb_loc</i>.</p> <p> <b>Note:</b> For LDAP in SSL mode:</p> <ul style="list-style-type: none"> <li>To use the certificate chain, create the <code>&lt;DM_LDAP_CERT_FILE&gt;</code> environment variable and set it to 1.</li> <li>To ignore the hostname check, create the <code>&lt;DM_LDAP_IGNORE_HOSTNAME_CHECK&gt;</code> environment variable and set it to 1.</li> </ul> <p>If you are using more than one LDAP server in SSL mode, you must store the LDAP certificates a single location, as described in <a href="#">“Using multiple LDAP servers in SSL mode” on page 150</a>.</p>

Field	Description
<b>Validate SSL Connection</b>	If you selected Use SSL, click to validate that a secure connection can be established with the LDAP server on the specified port. If the validation fails, the system displays an error message and you cannot proceed further until valid information is provided.

**Perform these manual steps for SSL validation for 6.5x and earlier versions of Documentum CM Servers:**

1. Depending on the operating system (other than Windows 64-bit) on which the application server is installed, copy all the jar files from \$Application\_root\$/WEB-INF/thirdparty/\$osname\$ to \$Application\_root\$/WEB-INF/lib

For example, if the operating system on which the Documentum Administrator application is installed is Windows, copy all the jar files from \$Application\_root\$/WEB-INF/thirdparty/win32/ to \$Application\_root\$/WEB-INF/lib

If the operating system on which the application server is installed is Windows 64-bit and the application server is using 64-bit JDK, do the following:

1. Backup the jss311.jar file and delete it from \$Application\_root\$/WEB-INF/lib
2. Copy the jss42.jar file from \$Application\_root\$/WEB-INF/thirdparty/win64/6.0.6 to \$AppServer\_root\$/WEB-INF/lib
2. Depending on the operating system (other than Windows 64-bit) on which the application server is installed, copy all \*.dll, (for Windows) or \*.so (for Linux) files from \$Application\_root\$/WEB-INF/thirdparty/\$osname\$ to \$AppServer\_root\$/da\_dlls



**Note:** If the da\_dlls folder does not exist in the preceding location, create it.

For example, if the operating system on which the Documentum Administrator application is installed is Windows, copy all the dll files from \$Application\_root\$/WEB-INF/thirdparty/win32/ to \$Application\_root\$/da\_dlls

If the operating system on which the application server is installed is Windows 64-bit and the application server is using 64-bit JDK, do the following:

- a. Copy the Microsoft.VC90.DebugCRT.manifest file from \$Application\_root\$/WEB-INF/thirdparty/win64/6.0.6 to \$AppServer\_root\$/da\_dlls
- b. Copy all \*.dll files from \$Application\_root\$/WEB-INF/thirdparty/win64/6.0.6 to \$AppServer\_root\$/da\_dlls
3. Set the path of the dlls in startup batch file of the application server.
  - For Windows: PATH=\$AppServer\_root\$\da\_dlls;%PATH%;
  - For Linux: LD\_LIBRARY\_Path=\$AppServer\_root\$/da\_dlls:%LD\_LIBRARY\_PATH%;

### 7.1.2.2 LDAP server sync & authentication properties

“LDAP server sync & authentication properties” on page 139 describes the properties on the Sync & Authentication tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 7-3: LDAP server sync & authentication properties**

Field	Description
<b>Import</b>	Specifies how users and groups are imported. Available options are: <ul style="list-style-type: none"> <li>• Users and groups (default)</li> <li>• Users only</li> <li>• Groups &amp; member users</li> </ul>
<b>Synchronize Nested Groups in the repository</b>	Select to synchronize the nested groups in the repository. <p> <b>Note:</b> This option is enabled only if <b>Import</b> field has the value <b>Users and groups</b> or <b>Groups &amp; member users</b>. This option is disabled if you select <b>Users only</b> for <b>Import</b> field.</p>
<b>Sync Type</b>	Specifies how users and groups are synchronized. Available options are: <ul style="list-style-type: none"> <li>• Full: Import all based on user/group mappings (default)</li> <li>• Incremental: Import only new or updated user/groups/members</li> </ul> If <b>Groups and member users</b> is selected in the Import field and a group was not updated but any of the group members were, the incremental synchronization is updating users identified by the user search filter. <p> <b>Note:</b> To run an incremental synchronization job, set the LDAP server and the Documentum CM Server in the same time and time zone without any clock drifts.</p>
<b>Deleted Users</b>	Specifies whether deleted user accounts are marked inactive. Available options are: <ul style="list-style-type: none"> <li>• set to inactive (default)</li> <li>• unchanged</li> </ul>

Field	Description
<b>Update Names</b>	Select to <b>Update user names in repository</b> or <b>Update group names in repository</b> .  The Update group names in repository checkbox is not enabled if Users Only is selected in the Import field.
<b>User Type</b>	Select a user type. The default is <i>dm_user</i> .
<b>Bind to User DN</b>	Options are: <ul style="list-style-type: none"><li>• <i>Search for DN in directory using user's login name</i></li><li>• <i>Use DN stored with user record in repository (default)</i></li></ul>
<b>External Password Check</b>	Select to use external password check to authenticate users to directory.

The LDAP synchronization job must have at least read access to a unique identifier on the directory server, as follows:

- **nsuniqueid** on Sun One/Netscape/iPlanet Directory Server
- **objectguid** on Microsoft Active Directory Server
- **ibm-entryuuid** on IBM Directory Server
- **guid** on Novell eDirectory
- **orclguid** on Oracle Internet Directory Server

Apart from the unique identifiers, all the attributes that have been mapped in the LDAP configuration object should also have read access in the directory server.

### 7.1.2.3 LDAP nested groups

Starting with the 7.0 release, nested groups in LDAP is supported. You can synchronize nested groups in the repository between Documentum CM Server and the LDAP directory server. The group search filter of the default LDAP config object needs to be set to the appropriate group name that forms the root group of the nested group structure. Starting with the 7.1 release, nested cyclic groups are also supported where a group forms a cycle with another in LDAP and both these groups are then synchronized into the repository. The cycles within these two groups are not retained since Documentum CM Server does not support cycles in groups.

To activate the nested cyclic group feature, you must update the *dm\_docbase\_config* object as follows:

```
API>
retrieve,c,dm_docbase_config
...
3c00014d80000103
API> append,c,l,r_module_name
```

```

SET> LDAP_CYCLIC_SAVE
...
OK
API> append,c,1,r_module_mode
SET> 1
...
OK
API> save,c,1
...
OK
API>

```

#### 7.1.2.4 LDAP server mapping properties

“LDAP server mapping properties” on page 141 describes the properties on the Mapping tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 7-4: LDAP server mapping properties**

Field	Description
<b>User Object Class</b>	Type the user object class to use for searching the users in the directory server.
<b>User Search Base</b>	Type the user search base. This is the point in the LDAP tree where searches for users start. For example:  cn=Users,ou=Server,dc=sds,dc=inengvm1llc,dc=corp,dc=test,dc=com.
<b>User Search Filter</b>	Type the person search filter. This is the name of the filter used to make an LDAP user search more specific. The typical filter is cn=*
<b>Search Builder</b>	Click to access the Search Builder page. This page enables you to build and test a user search filter. When finished, the User Search Filter field is populated with the resulting filter.
<b>Group Object Class</b>	Type the group object class to use for searching the groups in the directory server. Typical values are: <ul style="list-style-type: none"> <li>• For Netscape and Oracle LDAP servers: groupOfUniqueNames</li> <li>• For Microsoft Active Directory: group</li> </ul>
<b>Group Search Base</b>	Type the group search base. This is the point in the LDAP tree where searches for groups start. For example:  cn=Groups,ou=Server,dc=sds,dc=inengvm1llc,dc=corp,dc=test,dc=com.

Field	Description
<b>Group Search Filter</b>	Type the group search filter. This is the name of the filter used to make an LDAP group search more specific. The typical filter is cn=*
<b>Search Builder</b>	Click to access the Search Builder page. This page enables you to build and test a group search filter. When finished, the Group Search Filter field is populated with the resulting filter.
<b>Property Mapping</b>	When a new configuration is added, this table populates with the mandatory mapping attributes. The mappings are dependent upon the directory type. This table defines the pre-populated attributes and their mappings. All mapping types are LDAP Attribute.
<b>Add</b>	Click to access the Map Property page to add an attribute. From there, select a OpenText Documentum CM attribute, then select the LDAP attribute to which the OpenText Documentum CM attribute maps or type in a custom value.
<b>Edit</b>	Select an attribute and then click Edit to access the Map Property page. On the Map Property page, edit the attribute properties.
<b>Delete</b>	Select an attribute and then click Delete to remove an attribute. The system displays the Deletion Confirmation page.
<b>Repository Property</b>	Displays the repository property that is the target of the mapping.
<b>Type</b>	Identifies the source of the property: User or Group.
<b>Map To</b>	Displays which attributes on LDAP that the property is mapped to.
<b>Map Type</b>	Identifies the type of data: LDAP attribute, expressions, or a fixed constant.

Field	Description
<b>Mandatory</b>	<p>Indicates if the mapping is mandatory for the attribute.</p> <p>Documentum CM Server requires three properties to be defined for a user and one property to be defined for a group. The mandatory properties are:</p> <ul style="list-style-type: none"> <li>• user_name</li> <li>• user_login_name</li> <li>• group_name</li> </ul> <p>You can change the defaults, but you must provide some value or mapping for these properties. Users cannot be saved to the repository without values for these three properties, nor can a group be saved to the repository without a group name.</p>

### 7.1.2.5 LDAP server failover properties

“LDAP server failover properties” on page 143 describes the properties on the Failover tab of the LDAP Server Configuration page. The properties apply to new and existing LDAP configuration objects.

**Table 7-5: LDAP server failover properties**

Field	Description
<b>Failover Settings</b>	Use this section to enter settings for the primary LDAP server.
<b>Retry Count</b>	<p>The number of times Documentum CM Server tries to connect to the primary LDAP server before failing over to a designated secondary LDAP server. The default is 3.</p> <p>If the retry count value is set to 0, Documentum CM Server immediately reports that it failed to contact the primary LDAP directory server.</p>
<b>Retry Interval</b>	<p>Enter an interval number and select a duration (seconds, minutes, or hours) between retries. The default is at 3 seconds.</p> <p>Documentum CM Server fails to bind to the primary LDAP directory server, it waits the number of seconds specified before attempting to bind to the primary LDAP directory server again.</p>

Field	Description
<b>Reconnect</b>	<p>Enter an interval number and select a duration (seconds, minutes, or hours) after failover for the system to try to reconnect to the primary LDAP server.</p> <p>The default is set at 5 minutes.</p>
<b>Secondary LDAP Servers</b>	<p>Specifies secondary LDAP servers.</p> <ul style="list-style-type: none"> <li>To add a new secondary LDAP server, click <b>Add</b>. The Secondary LDAP Server page is displayed.</li> <li>To modify an existing secondary LDAP server, select the checkbox next to the name and click <b>Edit</b>. The Secondary LDAP Server page is displayed.</li> <li>To delete an existing secondary LDAP server, select the checkbox next to the name and click <b>Delete</b>.</li> <li>To reorder the list of LDAP servers, click <b>Move Up</b> or <b>Move Down</b>.</li> </ul>
<b>Name</b>	Name of the secondary LDAP server.
<b>Hostname</b>	The name of the host on which the secondary LDAP directory server is running.
<b>Port</b>	The port information.
<b>SSL Port</b>	The SSL port number.

### 7.1.3 Mapping LDAP servers

LDAP directory servers allow you to define attribute values for user and group entries in the directory server. Documentum CM Server supports mapping those directory server values to user and group properties in the repository. Using mapping automates setting user and group properties.

Mappings between LDAP attributes and repository properties are defined when you create the LDAP configuration object. You can map the LDAP values to the following properties:

- System or user-defined properties
- Multiple directory values to a single repository property, using an expression.

For example, the following expression uses the LDAP attributes sn and given name to generate a user\_address value:

```
${sn}_${givenname#1}@company.com
```

If the sn (surname) of user is Smith and the given name is Patty, the preceding expression resolves to smith\_p@company.com. The 1 at the end of given name directs the system to only use the first letter of the given name.

You can specify an integer at the end of an LDAP attribute name in an expression to denote that you want to include only a substring of that specified length in the resolved value. The integer must be preceded by a pound (#) sign. The substring is extracted from the value from the left to the right. For example, if the expression includes \${sn#5} and the surname is Anderson, the extracted substring is Ander.

 **Note:** Documentum CM Server does not support powershell or any other scripting extensions for the expression notation.

Values of repository properties that are set through mappings to LDAP attributes can only be changed either through the LDAP entry or by a user with superuser privileges.

 **Note:** Changing mappings for the user\_name, user\_login\_name, or group\_name after the user or group is synchronized for the first time is not recommended. Doing so may cause inconsistencies in the repository.

“[Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory example](#)” on page 145 contains examples of how the Attribute Map page for LDAP configurations is typically completed for Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory LDAP servers.

**Table 7-6: Netscape iPlanet, Oracle Internet Directory Server, and Microsoft Active Directory example**

DM attribute	DM type	LDAP attribute	Type
user_name	dm_user	cn	A
user_login_name	dm_user	uid	A

### 7.1.3.1 Mapping guidelines

The following rules apply when mapping LDAP group or user attributes to a repository property:

- In expressions, spaces are not required between references to LDAP attributes due to the bracket delimiter. If there is a space between mapped values, it appears in the result of the mapping.
- The length of the expression mapped to a single repository property cannot exceed 64 characters. Expressions that exceed 64 characters are truncated. The expression is recorded in the map\_val property of the ldap config object. This property has a length of 64.
- All standard OpenText Documentum CM property lengths apply to the mappings. For example, the mapping string for user\_name must resolve to 32 characters or less.

### 7.1.3.2 Building and testing user or group search filter using Search Builder

Access the Search Builder page by clicking the Search Builder button on the Mapping tab of the New LDAP Server Configuration or LDAP Server Configuration Properties page.

The Search Builder page enables you to build and test a user or group search filter. You can enter up to ten lines of search criteria. When finished, the User Search Filter or Group Search Filter field is populated with the resulting filter.

### 7.1.3.3 Adding or modifying repository property mapping

On the Map Property page, you can add or modify mapping properties.

#### To add or modify repository property mapping:

1. Access the Map Property page.
2. Select a repository property to map.
3. In the **Map To** section, select the LDAP property to which the repository property maps or type a custom value. Options are:
  - **Single LDAP Attributes:** If selected, select an LDAP attribute from the drop-down list.
  - **Fixed Value:** If selected, type a custom value.
  - **Expression:** If selected, type an expression and select an LDAP attribute reference from the drop-down list. Click the **Test Expression** button to test.
4. In the **Reject User/Group** section, select to reject synchronization of any LDAP user or group. Options for when to reject synchronization are:
  - Is empty or has insufficient characters
  - Is empty
  - Never reject any user/group
5. Click **OK** to save the changes or click **Cancel**.

### 7.1.4 Configuring secondary LDAP servers

You can configure Documentum CM Server to use other LDAP directory servers for user authentication in the event that the first LDAP directory server is down. By default, the primary LDAP server handles all user authentication requests. However, if Documentum CM Server fails to bind to the primary LDAP directory server, you can define a way for it to bind to secondary LDAP servers, authenticate users, and then reattempt the connection with the primary LDAP directory server.

Provide the information for the secondary LDAP server, as described in “[Secondary LDAP server page properties](#)” on page 147.

**Table 7-7: Secondary LDAP server page properties**

Field	Description
<b>Name</b>	Enter the name of the secondary LDAP server.
<b>Hostname / IP Address</b>	Type the name of the host on which the secondary LDAP directory server is running.
<b>Port</b>	The port information is copied from the primary LDAP server.
<b>Binding Name</b>	The binding name is copied from the primary LDAP server.
<b>Binding Password</b>	Type the binding distinguished password used to authenticate requests to the secondary LDAP directory server by Documentum CM Server or the check password program.
<b>Confirm Password</b>	Re-enter the binding password for verification.
<b>Bind to User DN</b>	The bind to user DN information is copied from the primary LDAP server.
<b>Use SSL</b>	The SSL information is copied from the primary LDAP server.
<b>SSL Port</b>	The SSL port number is copied from the primary LDAP server.
<b>Certificate Location</b>	The certificate location is copied from the primary LDAP server.

### 7.1.5 Changing the binding password

Change the binding password for LDAP directories on the LDAP Server Configuration Properties page. Access this page by clicking the Change link on the Info tab of the LDAP Server Configuration Properties page.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on changing the binding password.

### 7.1.6 Forcing LDAP server synchronization

The Synchronize Now option calls the SBO API to synchronize the LDAP configuration. The type of synchronization is determined by the first\_time\_sync flag on the LDAP configuration object.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on forcing LDAP server synchronization.

### 7.1.7 Duplicating LDAP configurations

Use the Save As option to create a copy of an LDAP configuration. The new LDAP configuration contains all the details of the original configuration object except for the secondary, or failover, servers. Secondary servers cannot be shared by the primary server.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on duplicating LDAP configurations.

### 7.1.8 Deleting LDAP configurations

You must be a superuser to delete an LDAP configuration.

Before deleting an LDAP configuration object, note the following potential consequences:

- If you delete an LDAP configuration object that is referenced by server configuration object of Documentum CM Server, the Documentum CM Server cannot use that LDAP server to authenticate users and there is no default LDAP object referenced in the server configuration object.
- If you delete an LDAP configuration object that is referenced by server configuration object of Documentum CM Server and by user or group objects, the server cannot use the LDAP server to authenticate users, no default LDAP object is referenced in the server configuration object, and user and group objects referencing the LDAP object cannot be updated correctly.

If you delete the LDAP configuration object, you must manually update user and group objects referencing the LDAP object so that the users and groups can be authenticated with a different authentication mechanism. To locate users

referencing the LDAP configuration object, click **User Management > Users** and search by typing the LDAP Config object name in the **User Login Domain** field.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting LDAP configurations.

### 7.1.9 Using LDAP directory servers with multiple Documentum CM Servers

If multiple Documentum CM Servers are running against a particular repository, you must perform some additional steps to enable LDAP authentication regardless of the particular Documentum CM Server to which a user connects.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on using LDAP directory servers with multiple Documentum CM Servers.

### 7.1.10 LDAP proxy server support

Documentum CM Server supports LDAP proxy servers, for use in LDAP configurations. If you are using Global Catalog in Microsoft Active Directory Server, you have to make sure that all attributes required during LDAP synchronization are present in the Global Catalog.

## 7.2 LDAP certificate database management

The LDAP certificate database management system enables administrators to:

- Import certificates into the LDAP certificate database on the Documentum CM Server.
- View certificate information in the LDAP certificate database.

Only an administrator who is the installation owner can access the LDAP Certificate Database Management node.

### 7.2.1 Viewing LDAP certificates

Documentum CM Server creates a certificate database when an administrator attempts to view the LDAP Certificate Database List page for the first time and the certificate database is not present at the certificate location that was specified when the LDAP server was added.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing LDAP certificates.

## 7.2.2 Importing LDAP certificates

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on importing LDAP certificates.

## 7.2.3 Using multiple LDAP servers in SSL mode

Documentum CM Server supports running more than one LDAP server in SSL mode. However, in this case all SSL-enabled LDAP configuration objects must point to the same certificate database location. Otherwise, LDAP synchronization does not work properly.

### To set up multiple LDAP servers in SSL mode:

1. Identify a location for the certificate database.  
The default location for the certificate database is the location that is specified in the `ldapcertdb_loc` object.
2. Import all required certificates into the certificate database, as described in [“Importing LDAP certificates” on page 150](#).
3. Modify the certification location field for each LDAP server configuration that uses SSL to point to the same certificate database location.  
By default, Documentum CM Server assigns the file path that is specified in the `ldapcertdb_loc` object.

## 7.2.4 Replacing or removing LDAP certificates

Replacing, deleting, or revoking of LDAP database certificates in the LDAP certificate database is not supported using the LDAP Certificate Management functionality. To update the certificates, manually remove the existing LDAP certificate database on the Documentum CM Server, restart the method server, then import the new certificates, as described in [“Importing LDAP certificates” on page 150](#).

## Chapter 8

# Managing MSA for OpenText Documentum CM services

You can manage Managed Service Accounts (MSA) for OpenText Documentum CM services. Use the instructions described in this chapter to configure MSA for starting or stopping OpenText Documentum CM processes securely using MSA user account. The OpenText Documentum CM processes include repository service, connection broker service, and Java Method Server service.

## 8.1 Windows

### 8.1.1 Prerequisites

1. Configure the Active Directory Module for Powershell and install the Active Directory Domain Services tools in a Windows Server machine. *Microsoft documentation* contains the instructions.
2. (For Windows Server 2016) Perform the following tasks:
  - a. Navigate to the Windows Server Manager, click **Promote Server to a Domain > Add new Forest**, and then provide the login credentials.
  - b. Restart the Windows Server and log in as an administrator.
  - c. In Windows Server Manager, navigate to **Tools** and open Active Directory Module for Powershell.
3. (For Windows Server 2012) Perform the following tasks:
  - a. Configure the Active Directory Module for Powershell in a Windows Server machine as described in [step 1](#).
  - b. Navigate to **Windows Server Manager > Active Directory Domain Services**.
  - c. Click **Create New**. Provide a name and password for the Domain Controller and click **OK**.
  - d. Install the Active Directory Domain Services.
  - e. Restart the Windows Server and log in as a Domain Controller user.

## 8.1.2 Creating and associating MSA with Windows server

1. Open the configured Active Directory Module for Powershell in any of the Windows Server.
2. Import the Active Directory Module in the Windows Server. For example:  

```
> Import-Module ActiveDirectory
```
3. Create the MSA in the Active Directory manually (for example, myacc4) or using the Active Directory Module for Poweshell. For example:
  - a. Create Key Distribution Service (KDS).  

```
"root key":  
> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10));
```
  - b. Create MSA.  

```
> New-ADServiceAccount -Name myacc4 -Enabled $true  
// DNSHostName : hostname.Primary DNS Suffix (for example,  
win12r2orcl-001.ottest.local)
```
4. Verify if the new MSA, myacc4, is created in the Active Directory. For example, fetch an Active Directory MSA details in Powershell:  

```
> Get-ADUser -Server <IP address of Active Directory Server or DNS Host Name>  
> Filter : SAMAccountName -like "myacc4"
```
5. Associate the new MSA, myacc4, with a target machine. For example:  

```
> Add-ADComputerServiceAccount -Identity win12r2orcl-001 -ServiceAccount myacc4
```
6. Import the Active Directory Module to a target machine. For example:  

```
> Import-Module ActiveDirectory
```
7. Install the MSA you created in the local machine. Provide the permission to the Server to retrieve password of MSA from the Active Directory. For example:  

```
> Set-ADServiceAccount myacc4 -PrincipalsAllowedToRetrieveManagedPassword  
win12r2orcl-001$  
> Install-ADServiceAccount -identity myacc4;
```
8. Restart the machine.
9. Log in as an administrator and install Documentum CM Server.
10. Use OpenText Directory Services (OTDS) partition consolidation to synchronize the MSA user in Documentum CM Server from Active Directory.
11. Verify the synchronized user in the repository using IAPI. For example:  

```
retrieve,c,dm_user where user_name='myacc4'
```



### Caution

Do not change user\_password of the MSA user using IAPI, as it is encrypted. Changing it could lead to corruption and cause issues with

the synchronization between Documentum CM Server and Active Directory.

12. Dump the synchronized user using IAPI.  
The user, system, application, and the internal attributes are updated.
13. Associate the MSA with your services. For example, for Documentum CM Server, associate with the OpenText Documentum CM repository, connection broker, and Java Method Server services.
14. Change the installation owner manually to a domain user account as follows:
  - a. Add any existing Documentum CM Server machine to the domain, configure the config.xml file, and then run the migration utility to change the install owner.
  - b. Run the following queries on the database:

```
BEGIN TRAN
update dm_user_s set user_os_domain = 'otxmsa.local' where
user_login_name='myacc4$';
update dm_user_s set user_global_unique_id = 'otxmsa.local:myacc4$' where
user_login_name='myacc4$';
update dm_user_s set user_login_domain = 'otxmsa.local' where
user_login_name='myacc4$';
update dm_server_config_s set r_install_domain = 'otxmsa.local';
COMMIT TRAN
```

- c. Edit the server.ini file (if it has not changed). For example:

```
user_auth_target = <DOMAIN NAME> install_owner = <DOMAIN USER>
```

- d. Modify the following entries manually in the Windows registry. For example:

- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\  
\DmServer<Docbasename>]  
ObjectName=<DOMAIN NAME>\<DOMAIN USER>
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\  
\DmServer<Docbasename>]  
ImagePath=C:\Documentum\product\16.7\documentum.exe -docbase name testenv -  
security acl -init\_file  
C:\Documentum\dba\config\testenv\server.ini -run as service -install owner  
myacc4\$ -logfile
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmMethodServer]  
ObjectName=<DOMAIN NAME>\<DOMAIN USER>
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DmDocBroker]  
ObjectName=<DOMAIN NAME>\<DOMAIN USER>
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Documentum\Server\16.4]  
"DM\_DMADMIN\_USER"=<DOMAIN USER>  
"DM\_DMADMIN\_DOMAIN"=<DOMAIN NAME>

- e. Right-click on **DmServer<repository name>** > Permissions > Advanced > Change owner > Object Types > Service accounts, enter the name of MSA and click OK.

Make sure that the full control is provided to this user, similar to the DmMethodServer and DmDocBroker services.

- f. Invoke regedit and verify if the install owner has full permissions on the following entries:

- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\Documentum]
- [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog]
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\DOCUMENTUM\DOCBASES]

- g. Run the following command and grant permission for the new installation owner:

```
> icacls C:\Documentum /grant <DOMAIN NAME>\<DOMAIN USER>:F /t /q
```

After the completion of all the steps, make sure that all services are up and running.

15. Make sure that connection broker and Java Method Server services starts from services.msc.
16. To start the repository using MSA, instead of using services.msc, open the command prompt window and set the installation owner explicitly for your MSA user. For example:

```
> C:\Documentum\product\16.7\bin\documentum.exe -docbase_name testusername -  
security acl -init_file  
C:\Documentum\dba\config\testusername\server.ini -install_owner myacc4
```

If the repository fails to start, run the dm\_crypto\_boot utility and verify the password.

17. Navigate to %DCTM\_HOME%\bin and run the following command to start the agent exec program:

```
> dm_agent_exec.exe -docbase_name testenv -docbase_owner Administrator
```

You can use IAPI as a trusted administrator user and run jobs such as dm\_UserRename.

### 8.1.3 Removing MSA

1. Run the migration utility and change the installation owner to administrator for Documentum CM Server.
2. Run the following PowerShell Command let to remove the MSA from the local machine:

```
> Remove-ADServiceAccount -identity <MSA name>
```

3. (Optional) Remove the service account from Active Directory. For example:

```
> Remove-ADComputerServiceAccount -Identity <the machine where MSA is assigned to> -  
ServiceAccount <MSA>
```

Skip this step if you want to reassign an existing MSA from one machine to another.

### Notes

- Configuration is for MSA user domain only. Active Directory different from MSA domain is not supported for MSA configuration.
- When you want to create new dm\_ldap\_config object other than the one already created, you must manually provide full access permission to the MSA user to access the new .cnt file generated at C:\Documentum\dba\config\testenv\. Otherwise, it results in the access denied error when you run the LDAP synchronization job using the new LDAP configuration object. This is because, Windows does not allow default user permissions on a new file or folder.

## 8.2 Linux

### 8.2.1 Prerequisites

1. Configure a Windows Server machine with Active Directory. *Microsoft documentation* contains the instructions.
2. Make sure that all Linux servers where Documentum CM Server services need to be managed are connected to the Windows Active Directory domain.
3. Install Documentum CM Server in a location where Active Directory user has full access. For example: /opt/dctm/.
4. Make sure that you allow Secure Shell (SSH) or OpenSSH to access Linux servers from Windows Active Directory machine.

### 8.2.2 Creating and associating MSA with Linux server

1. In Windows Active Directory, create MSA user and group to manage OpenText Documentum CM services.
2. Set the value of `use_fully_qualified_names` to `False`.
3. Use the migration tool to change the installation owner (`install_owner`) from local user (for example, `dmadmin`) to the Windows Active Directory domain user.
4. Update the `config.xml` as needed and add the path of `ojdbc.jar` in the `MigrationUtil.sh` launch script.
5. Create a RSA key pair (without password) to allow you to access the Linux Servers from the Windows Server without the need to remember the password.

A MSA user gets the privileged access from the Windows Active Directory machine to perform actions on Linux server where OpenText Documentum CM services are installed.



**Note:** You can change the password of Documentum administrator (Active Directory user) from Windows Active Directory without affecting the privileged access already provided to access the Linux server.

6. Register the public key in authorized\_keys.
7. Use SSH or OpenSSH to connect and manage OpenText Documentum CM services.
8. You can use the example commands described in the following table to manage OpenText Documentum CM services:

Action	Command
Verify if the connection broker or repository or Java Method Server is running.	<p>Connection broker:</p> <pre>ssh documentum@&lt;IP address of Linux server&gt; "ps -ef   grep [d]mocbroker"</pre> <p>Repository:</p> <pre>ssh documentum@&lt;IP address of Linux server&gt; "ps -ef   grep [d]ocumentum   grep 'docbase_name msadoc'"</pre> <p>Java Method Server:</p> <pre>ssh documentum@&lt;IP address of Linux server&gt; "ps -eaf   grep [D]ctmServer_MethodServer"</pre>
Stop the connection broker or repository or Java Method Server.	<p>Connection broker:</p> <pre>ssh msauser@&lt;IP address of Linux server&gt; "opt/dctm/dba/dm_stop_DocBroker"</pre> <p>Repository:</p> <pre>ssh msauser@&lt;IP address of Linux server&gt; "opt/dctm/dba/dm_shutdown_msadoc"</pre> <p>Java Method Server:</p> <pre>ssh msauser@&lt;IP address of Linux server&gt; "\$DM_JMS_HOME/bin/stopMethodServer.sh"</pre>
Start the connection broker or repository or Java Method Server.	<p>Connection broker:</p> <pre>ssh msauser@&lt;IP address of Linux server&gt; "opt/dctm/dba/dm_launch_DocBroker"</pre> <p>Repository:</p> <pre>ssh msauser@&lt;IP address of Linux server&gt; "export ORACLE_HOME=/opt/app/oracle/product/&lt;oracle_version&gt;/db_1;opt/dctm/dba/dm_start_msadoc"</pre> <p>Java Method Server:</p> <pre>ssh msauser@&lt;IP address of Linux server&gt; "\$DM_JMS_HOME/bin/startMethodServer.sh"</pre>

## Chapter 9

# Managing OTDS authentication license server

## 9.1 Overview

The OTDS authentication license module has been separated from Java Method Server and created as a standalone, lightweight OTDS authentication license server. This license server operates independently both on the Documentum CM Server in an on-premises environment and within a cloud pod. It runs on the loopback address using port 8400 (recommended) and is integrated with Documentum CM Server. The license server starts automatically when the repository is initialized. If the license service does not start, any new request starts it, ensuring continuous availability.

The license server offers the following benefits:

- Helps to avoid the dependency with Java Method Server
- Manages the operations related to OTDS licensing module
- Acts as a plug-in for Documentum CM Server and leverages the Documentum CM Server's high-availability



**Note:** The OTDSAuthentication servlet is removed from Java Method Server.

## 9.2 Configuring OTDS authentication in license server

1. Obtain OTDS certificate using the following URL format:

`https://<otds_ip>:<otds_port>/otdsws/rest/systemconfig/certificate_content`

2. Configure the OTDS certificate located at `$DM_HOME\OTDSAuthLicenseHttpServerBin\config\otdsauth.properties`.

You can configure multiple certificates in the `certificate_n` format for Documentum CM Server to support OAuth token authentication for multiple OTDS.

3. Configure the OTDS web service endpoint for password authentication, `http://<otds_ip>:<otds_port>/otdsws/rest/authentication/credentials`, in the `otdsauth.properties` file.

4. **Optional** Do the following only for OTDS ticket authentication:

- a. Configure the OTDS web service endpoint, `http://<otds_ip>:<otds_port>/otdssws/rest/authentication/resource/validation`, in the `otdsauth.properties` file.
  - b. Configure the repository name, resource ID, and secret key of the resource in the `otdsauth.properties` file.
5. **Optional** Do the following only for OTDS token-based password authentication:  
If you do not want partition name in the user login name then set `passauth_use_oauth2_token` to true in the `otdsauth.properties` file and configure `client_id` and `client_secret`.
- For example:
- ```
passauth_use_oauth2_token = true
client_id = <OAuth client ID>
client_secret = <secret>
otds_rest_oauth2_url = http://<host IP>:<port>/otdssws/oauth2/token
synced_user_login_name = <source of user login name>
```
- The valid value for `synced_user_login_name` must be `sAMAccountName` when the user is synchronized from the Active Directory.
6. Restart the license server.



### Notes

- To modify the recommended port 8400 for the license server, change the port value in the `$DM_HOME\OTDSAAuthLicenseHttpServerBin\config\otdsauthlicense.properties` file and the `app_server_uri` of `OTDSAAuthentication` in the `dm_server_config` object. Then, restart both the repository and the license server. The modification of port is supported only in an on-premises environment.
- Restart the license server if you make changes to either the `otdsauth.properties` or `otdsauthlicense.properties` file using the start and stop scripts.

The start and stop scripts are located at `$DM_HOME\OTDSAAuthLicenseHttpServerBin`.

- If you modify the `dm_otds_license_config` object, run the following command in IAPI:

```
API> apply,c,NULL,FLUSH_OTDS_CONFIG
```

- If you make any changes to the license assigned to a user such as allocation, deallocation, revocation, and so on and deletion of user in OTDS and want the changes to take effect immediately in Documentum CM Server, run the following command in IAPI:

- For all users:

```
API> apply,c,NULL,FLUSH_OTDS_CACHE
```

- For a specific user:

```
API> apply,c,NULL,FLUSH_OTDS_CACHE,FLUSH_USERS_LIST,S,user1
```

- For multiple users:

```
API> apply,c,NULL,FLUSH_OTDS_CACHE,FLUSH_USERS_LIST,S,'user1,user2,user3'
```

## 9.3 Additional information

Use the following information, as appropriate:

- To troubleshoot the authentication mechanism in Documentum CM Server, enable the `trace_authentication` and `trace_http_post` parameters on Documentum CM Server.
- To troubleshoot the license server, set the value of the `rootLogger.level` and `logger.OTDS_AUTH_TRACE.level` parameters to `DEBUG` in the `$DM_HOME\OTDSAAuthLicenseHttpServerBin\config\log4j2.properties` file.
- Location of the OTDS authentication log file, `otdsauth.log`, is `$DOCUMENTUM\dba\log`.



## Chapter 10

# OpenText Directory Services integration with Documentum CM Server

### 10.1 Overview

With the OTDS integration with Documentum CM Server, the following are supported:

- Users and groups (existing or new) in OTDS can be pushed or synchronized to Documentum CM Server.
- Users in OTDS can be authenticated against OTDS using the OAuth2 token (authentication and authorization protocol), OTDS ticket, and also using plain password mechanisms.
- Using the OAuth2 token, OpenText Documentum CM client products can leverage OTDS capabilities to support additional SSO mechanism.

### 10.2 Configuring OTDS integration with Documentum CM Server

You must perform the following instructions in OTDS:

1. Create a partition.

You can create partition using AD server details, create user and group filters, monitor protocol, perform AD to OTDS attributes mapping, and so on.

2. Create a resource.

Resource represents any enterprise content management (ECM) server (for example, Documentum CM Server). In resource, you can configure resource Foundation REST API (Generic) server URL ([http://<Java\\_Method\\_Server\\_Host>:<Java\\_Method\\_Server\\_Port>/dmotdsrest](http://<Java_Method_Server_Host>:<Java_Method_Server_Port>/dmotdsrest)), administrator credentials of repository, and OTDS to repository attribute mappings.



**Note:** Make sure that the value of the `user_name` and `_NAME_` resource attributes in **User Attributes Mappings** are same.

3. **Optional** Select **Actions > Include Groups** of the access role to synchronize groups.

4. Map the resources to partition in access role.

Access role is created automatically when creating a resource. In access role, you need to add the partition and the users or groups that need to be pushed to Documentum CM Server.

**Caution**

You must not consolidate resources manually using the **Actions > Consolidate** option in the resources page because the synchronization of the resource is automatic.

*OpenText Directory Services* documentation contains detailed instructions.

## 10.3 Supported functions

LDAP synchronization is deprecated. This section describes the various functions that you can perform using OTDS instead of LDAP.

| Function                     | Using LDAP                                                             | Using OTDS                                                                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full synchronization         | Synchronize LDAP configuration in full synchronization mode.           | Consolidation of partition or resources in OTDS.                                                                                                                                                                            |
| Incremental synchronization  | Synchronize LDAP configuration in incremental synchronization mode.    | Automatically monitored by OTDS.<br><br> <b>Note:</b> Restarting partition for incremental synchronization is for troubleshooting only. |
| Import mode                  | Import mode option in LDAP configuration.                              | Use <b>Include Groups</b> option in <b>Access Role</b> .                                                                                                                                                                    |
| Deleting users in repository | Inactive or unchanged options for user deletion in LDAP configuration. | Set <code>inactive_deleted_user</code> to T or F in <code>dmotds.properties</code> of the <code>dmotdsrest.war</code> in Java Method Server.<br><br>The default value is T.                                                 |

| Function                                      | Using LDAP                                                                          | Using OTDS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deactivating unsubscribed users in repository | None                                                                                | <p>Set <code>inactive_unsubscribed_user</code> to T or F in <code>dmotds.properties</code> of the <code>dmotdsrest.war</code> in Java Method Server.</p> <p>The default value is F.</p> <p>When set to T, the following operations occur:</p> <ul style="list-style-type: none"> <li>• If a user is removed from the <code>subscriptionusers</code> group, then the user is deactivated in Documentum CM Server.</li> <li>• If a user is added to the <code>subscriptionusers</code> group, then the user is activated in Documentum CM Server.</li> </ul> |
| Renaming users in repository                  | Enable or disable user renaming option in LDAP configuration.                       | <p>Set <code>user_rename_enabled</code> to T or F in <b>Resources &gt; User Attribute Mappings</b> in OTDS.</p> <p>The default value is F.</p>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Renaming groups in repository                 | Enable or disable group renaming option in LDAP configuration.                      | <p>Set <code>groups_rename_enabled</code> to T or F in <b>Resources &gt; Group Attribute Mappings</b> in OTDS.</p> <p>The default value is F.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |
| Custom user type                              | User Type option in LDAP configuration.                                             | <p>Set <code>user_type</code> to the corresponding type in <b>Resources &gt; User Attribute Mappings</b> in OTDS.</p> <p>The default type is <code>dm_user</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                     |
| Creating default cabinet for users            | Using the <code>create_default_cabinet</code> in LDAP synchronization job argument. | <p>Set <code>create_default_cabinet</code> to T or F in <b>Resources &gt; User Attribute Mappings</b> in OTDS.</p> <p>The default value is F.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |

## 10.4 Configuring OTDS authentication in Documentum CM Server

1. Update the `dm_server_config` object with the `app_server_uri` of OTDSAuthentication as follows:

```
API> retrieve,c,dm_server_config
API> append,c,1,app_server_name
SET> OTDSAAuthentication
API> append,c,1,app_server_uri
SET> http://localhost:<port>/otdsauthlicense
API> save,c,1
```

2. Obtain OTDS certificate using the following URL format:

`https://<otds_ip>:<otds_port>/otdsws/rest/systemconfig/certificate_content`

3. Configure the OTDS certificate at `$DM_HOME\OTDSAAuthLicenseHttpServerBin\config\otdsauth.properties`. You can configure multiple certificates in the `certificate_n` format for Documentum CM Server to support OAuth token authentication for multiple OTDS.
4. Configure the OTDS web service endpoint for password authentication, `http://<otds_ip>:<otds_port>/otdsws/rest/authentication/credentials`, in the `otdsauth.properties` file.
5. **Optional** Do the following only for OTDS ticket authentication:
  - a. Configure the OTDS web service endpoint, `http://<otds_ip>:<otds_port>/otdsws/rest/authentication/resource/validation`, in the `otdsauth.properties` file.
  - b. Configure the repository name, resource ID, and secret key of the resource in the `otdsauth.properties` file.

6. **Optional** Do the following only for OTDS token-based password authentication:

If you do not want partition name in the user login name, set `passauth_use_oauth2_token` to true in the `otdsauth.properties` file and configure `client_id` and `client_secret`.

For example:

```
passauth_use_oauth2_token = true
client_id = <OAuth client ID>
client_secret = <secret>
otds_rest_oauth2_url = http://<host IP>:<port>/otdsws/oauth2/token
synced_user_login_name = <source of user login name>
```

The valid value for `synced_user_login_name` must be `sAMAccountName` when the user is synchronized from the Active Directory.

## 10.5 Authenticating OTDS users

You can authenticate the OTDS users using the following IAPI commands:

- Password-based authentication: `connect,<docbase_name>,<user_login_name>,dm_otds_password=<user_password>`
- oAuth2 token-based authentication: `connect,<docbase_name>,<user_login_name>,dm_otds_oauth=<oAuth2_token>`
- oAuth2 token-based authentication without user login name: `connect,<docbase_name>,null,dm_otds_ticket=<oAuth2_token>`
- OTDS ticket-based authentication: `connect,<docbase_name>,null,dm_otds_ticketex=<OTDS_ticket>`

## 10.6 Configuring OTDS as SAML service provider

Documentum CM Server supports configuring of OTDS as the Security Assertion Markup Language (SAML) service provider. You can use the configured OTDS as a centrally-managed authentication service provider. OpenText Documentum CM clients can leverage the OTDS authentication handler to configure the SAML authentication handler to validate the identity with the identity provider and obtain the OAuth token. The OAuth token is forwarded to Documentum CM Server which validates the token to provide the session to the OpenText Documentum CM clients.

1. Complete all the steps in “[Configuring OTDS integration with Documentum CM Server](#)” on page 161.
2. Configure the SAML authentication handler.
3. Configure OAuth clients.

*OpenText Directory Services* documentation contains detailed information.

## 10.7 Configuring OTDS for Kerberos SSO

Documentum CM Server supports configuring of OTDS for the Kerberos secure Single sign-on (SSO) authentication. When OpenText Documentum CM clients request for OAuth token, OTDS chooses one of the authentication handlers based on the priority set for authentication handlers (for example, Kerberos). For the Kerberos authentication handler, the Ticket Granting Ticket (TGT) of the user is used to obtain the Service Ticket (ST) of OTDS service. After the ST is validated, OTDS provides the OAuth token for that user. The OAuth token is forwarded to Documentum CM Server which validates the token to provide the session to the OpenText Documentum CM clients.

1. Complete all the steps in “[Configuring OTDS integration with Documentum CM Server](#)” on page 161.
2. Configure OAuth clients.

*OpenText Directory Services documentation* contains detailed information.

## 10.8 Migrating LDAP users and groups as OTDS users and groups

Documentum CM Server supports migration of LDAP users and groups as OTDS users and groups in the repository. Perform the following steps:

1. Take a backup of dm\_user and dm\_group tables in the database.
2. In dmotds.properties, do the following:
  - a. Set the value of migrate\_ldap\_users to T.
  - b. Provide the name(s) of the repository, separated by a comma, that needs to be migrated as values for migrate\_ldap\_docbases.

For example: migrate\_ldap\_docbases=repo1, repo2
  - c. Optional Provide the delimiter (for example, comma) you want to use to separate the dm\_ldap\_config objects in <docbase\_name>\_migrate\_ldap\_configs as value for ldap\_configs\_tokenizer.

For example: ldap\_configs\_tokenizer=,
  - d. Disable the dm\_ldap\_config objects whose users and groups need to be migrated.
  - e. Provide the name of the repository for <docbase\_name> in <docbase\_name>\_migrate\_ldap\_configs.

For example, repo1\_migrate\_ldap\_configs.

In addition, provide the names of dm\_ldap\_config object as values for <docbase\_name>\_migrate\_ldap\_docbases.

For example: repo1\_migrate\_ldap\_configs=ldapconfig1,ldapconfig2

Then, restart the application server for the changes to take effect.

3. Create partitions in OTDS that are similar to dm\_ldap\_config objects provided as values for <docbase\_name>\_migrate\_ldap\_configs.
4. Create resources in OTDS to the repositories provided as values for <docbase\_name>\_migrate\_ldap\_configs.
5. Configure the partitions to the appropriate access role of the resources to migrate the LDAP users and groups as OTDS users and groups in the repository.

## 10.9 Additional information

Use the following information, as appropriate:

- To troubleshoot the authentication mechanism in Documentum CM Server, enable the `trace_authentication` and `trace_http_post` parameters on Documentum CM Server.
- To troubleshoot the user synchronization between OTDS and repository of the Documentum CM Server, set the value of the `log4j.category.com.documentum.cs.otds` parameter to `DEBUG` in the `$DM_HOME\OTDSAuthLicenseHttpServerBin\config\log4j2.properties` file.
- To troubleshoot the user authentication, set the value of the `log4j.rootCategory` parameter to `DEBUG` in the `$DM_HOME\OTDSAuthLicenseHttpServerBin\config\log4j2.properties` file.
- Location of the `dmotdsrest` log file, `dmotdsrest.log`, is at `%DM_JMS_HOME%\logs`.
- Location of the OTDS authentication log file, `otdsauth.log`, is at `$DOCUMENTUM\dba\log`.
- To obtain the list of all the users and groups synchronized from OTDS to the repository, use the following DQL queries:
  - List of users: `select user_name from dm_user where user_source = 'OTDS'`
  - List of groups: `select group_name from dm_group where group_source = 'OTDS'`



# Chapter 11

## Integration with Content Aviator services

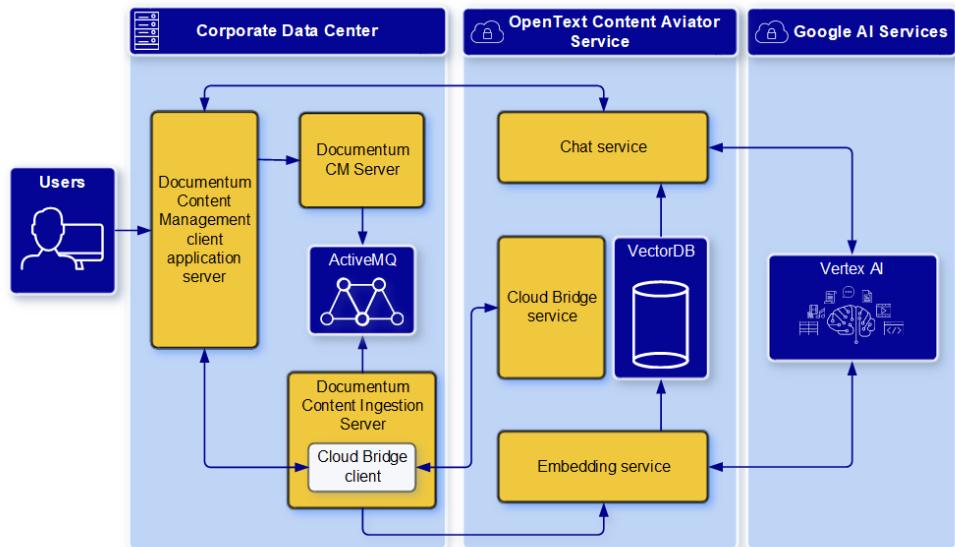
### 11.1 Overview

Content Aviator is an OpenText chat-based conversational search feature that helps you to search and query the content that is stored in the OpenText Documentum CM folders. Content Aviator deployment enables the communication between the OpenText Documentum CM and Content Aviator that is deployed in a Google Cloud Platform hosted by OpenText.

### 11.2 Content Aviator integration solution view

The SaaS proxy client (Cloud Bridge client) along with Documentum Content Ingestion Service (DCIS) are included with the OpenText Documentum CM deployment. The SaaS proxy client helps to establish a communication with a SaaS proxy service (Cloud Bridge service) that is deployed along with the Content Services AI (CSAI) services. Proxy client configuration includes callback URLs for authentication (OTDS) and authorization (OpenText™ Documentum™ Content Management Client REST API) endpoints. The SaaS proxy client and SaaS proxy service are used for validating the authentication and authorization of chat requests.

CSAI services communicates with Aviator Model Services or with any available Large Language Models. For more information, see *OpenText Content Aviator - Installation and Administration Guide (AICS250400-IGD)*



| Component                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aviator Model Services              | Aviator Model Services framework contains a Large Language Model (LLM) that provides responses to queries from OpenText Documentum Content Management.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Content Aviator Services            | <p>Content Services AI contains services that help to integrate content systems with Large Language Models (LLM):</p> <ul style="list-style-type: none"> <li>• Embeddings service: This is an HTTP RESTful API that receives text-based documents and adds them to the Embeddings queue. These documents are then embedded and stored for future use.</li> <li>• Chat service: This is an HTTP RESTful API that allows you to chat with a Large Language Model about the embedded documents. The service receives messages, retrieves related document chunks from the vector database, and uses the LLM to generate a response.</li> </ul> |
| ActiveMQ                            | <p>ActiveMQ server components helps to process the event messages for embedding process and creates the required queues for event messages.</p> <p>Embedding Queue retains the messages of the documents that are to be processed for a folder or to a document.</p> <p>Notification Queue retains the notification event messages for each document.</p>                                                                                                                                                                                                                                                                                   |
| Documentum Content Ingestion Server | To generate embeddings for the documents qualified for the intelligent service, each document must be retrieved from Documentum CM Server and the text to be extracted. Later, extracted texts are sent to the CSAI Embedding service. To make system to work concurrently with multiple documents at any point in time, multiple pipeline thread is spawned by Ingestion pipeline manager. A pipeline represents collection of sequential activity performed by the individual components as a one work unit.                                                                                                                              |

## 11.3 Prerequisites

| Requirement            | Details                                                                                         |
|------------------------|-------------------------------------------------------------------------------------------------|
| JDK 17.x.x             | Supported JDK version details.                                                                  |
| Documentum xPlore      | 22.1 Patch 14                                                                                   |
| OTDS                   | Ensure that OTDS is deployed in a environment where it is accessible to OpenText Documentum CM. |
| ActiveMQ Artemis       | Ensure that ActiveMQ Artemis is deployed and configured.                                        |
| OpenText Documentum CM | Ensure that OpenText Documentum CM is deployed.                                                 |
| Content Aviator        | OpenText Documentum CM requires the Content Aviator add-on.                                     |

| Requirement                        | Details                                                                                                                                                                                                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content Services AI (CSAI) service | <p>Ensure that the CSAI service is deployed in a Google Cloud Platform cloud environment.</p> <p> <b>Note:</b> For more details on the CSAI deployment details, contact OpenText Global Technical Services.</p> |

## 11.4 Deploying and configuring Content Aviator components

1. Locate the Content Aviator setup file from the <Documentum\_Server>/AviatorSetup.zip path.
2. Copy and extract the AviatorSetup.zip ZIP file to the system where Content Aviator components has to be deployed.

 **Note:** OpenText recommends that you deploy Content Aviator, ActiveMQ, and OpenText Documentum CM in different systems.

3. To configure the SaaS proxy client or Cloud Bridge for Hybrid Aviator, do the following:
  - a. Locate the <Extracted Path>/SaaS-Proxy-Client/config.properties file.
  - b. Update the required values for the following variables:

**Table 11-1: SaaS proxy client configuration properties**

| Parameter                                | Description                                                                                                                                                           |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SaaS proxy service configurations</b> |                                                                                                                                                                       |
| websocket.endpoint                       | Specify the websocket endpoint that will be used to establish a connection between a SaaS proxy client and SaaS proxy service.<br>For example: ws : / <FQDN> : <port> |
| websocket.auth                           | Specify the authentication credentials for the websocket to establish a connection with the SaaS proxy service.<br>For example: <Username> : <Password>               |
| websocket.connections.per.client         | Specify the number of websocket connections that can be established in parallel between the SaaS proxy client and the SaaS proxy service.                             |
| <b>Server URLs configurations</b>        |                                                                                                                                                                       |

| Parameter                            | Description                                                                                                                                                                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| servers.jwks                         | Specify the URL path of OTDS authentication endpoint.<br>For example: <code>https://&lt;host&gt;:&lt;port&gt;/otdsws</code>                                                                                                        |
| servers.perms                        | Specify the URL path for the OpenText™ Documentum™ Content Management Foundation REST API user authorization endpoint.<br>For example: <code>http://&lt;host&gt;:&lt;port&gt;/D2-Smartview/repositories/&lt;docbase&gt;</code>     |
| servers.dctmauth                     | Specify the URL path for the OpenText Documentum Content Management (CM) Foundation REST API user authentication endpoint.<br>For example: <code>http://&lt;host&gt;:&lt;port&gt;/D2-Smartview/repositories/&lt;docbase&gt;</code> |
| <b>List of allowed URL endpoints</b> |                                                                                                                                                                                                                                    |
| callbacks.dctmauth.endpoint          | Specify the OpenText Documentum CM client user authentication endpoint.<br>For example: <code>/currentuser</code>                                                                                                                  |
| callbacks.jwks.endpoint              | Specify the DCIS OTDS token validation endpoint.<br>For example: <code>/oauth2/jwks/</code>                                                                                                                                        |
| callbacks.perms.endpoint             | Specify the permission check endpoint for content objects.<br>For example: <code>/objects-specific-permission</code>                                                                                                               |



**Note:** The preceding steps are not applicable for on-premises Aviator.

4. To configure Documentum Content Ingestion Service, do the following:
  - a. Locate the <Extracted Path>/setup.properties file.
  - b. Update the required values for the following variables:

**Table 11-2: DCIS config properties**

| Parameter                  | Description                                                                         |
|----------------------------|-------------------------------------------------------------------------------------|
| <b>DCIS Configurations</b> |                                                                                     |
| llm_enabled                | To enable or disable the CSAI feature during deployment. The default value is true. |
| <b>Vault details</b>       |                                                                                     |

| Parameter                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vault_enabled                                   | <p>The default value is <code>false</code>.</p> <p>For the Vault-enabled environment, set the value of <code>vault_enabled</code> to <code>true</code> and also set the following environment variables:</p> <ul style="list-style-type: none"> <li>• <code>IS_VAULT_ENABLED</code>: Set this value to <code>true</code>.</li> <li>• <code>DSIS_URL</code>: Specify the URL to connect to the DSIS daemon agent. The format is: <code>http://localhost:&lt;dsis.port&gt;/dsis</code></li> <li>• <code>DSIS_TOKEN</code>: Token to authenticate with the DSIS daemon agent. Set the value to the same value provided for <code>dsis.dctm.token</code>. This is an optional argument.</li> </ul> |
| <b>Connection broker and repository details</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| docbroker_host                                  | Specify the connection broker host address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| docbroker_port                                  | Specify the connection broker host port. The default port is 1489.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ssl_truststore                                  | Allows to use a customized trust store.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ssl_truststore_password                         | Specify the password for the customized trust store.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| use_existing_truststore                         | Indicates to use the existing trust store. The default value is <code>false</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| docbase_name                                    | Specify the name of the repository.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| docbase_user                                    | Specify the name of the repository installation owner.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| docbase_password                                | Specify the installation owner password. If Vault is enabled, you must specify the secret key and store the password in Vault with a secret key in the following format:<br><code>DOCBASE_PASSWORD/DOCBASE_PASSWORD</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>ActiveMQ details</b>                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| activemq_broker_url                             | Specify the ActiveMQ URL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| activemq_user                                   | Specify the ActiveMQ user name.<br>For example: <code>artemis</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Parameter                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| activemq_password           | Specify the password for the embedding queue user. If Vault is enabled, this value should be empty and store the password in Vault in the following format:<br>ACTIVEMQ_PASSWORD/dcis                                                                                                                                                                                                                                                           |
| activemq_queue              | Specify the embedding queue name.                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>CSAI details</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| embedding_url               | Specify the CSAI embedding service URL.<br>For example: <a href="http://localhost/embeddings">http://localhost/embeddings</a>                                                                                                                                                                                                                                                                                                                   |
| query_url                   | Specify the CSAI chat or query service URL.<br>For example: <a href="http://localhost/chat">http://localhost/chat</a>                                                                                                                                                                                                                                                                                                                           |
| proxy_enable                | Set the value to <code>true</code> if you are deploying on a private environment and specify the proxy host, proxy port, and noProxyHosts details.<br>The default value is <code>false</code> .                                                                                                                                                                                                                                                 |
| proxy_host                  | Specify the proxy host name if proxy is enabled.                                                                                                                                                                                                                                                                                                                                                                                                |
| proxy_port                  | Specify the proxy port if proxy is enabled.<br>For example, 3128.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Proxy bypass details</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| no_proxy                    | Specify the host that can be accessed without going through the proxy. If the proxy is enabled, then add the required Foundation REST API, OpenText Documentum Content Management (CM) Client REST API, and OTDS internal service URLs for <code>noproxy</code> inputs.<br><br> <b>Note:</b> These entries should be separated using the pipe operator ( ). |
| <b>OTDS details</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| oauth_client_id             | Specify the OTDS client ID.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| oauth_client_secret         | Specify the OTDS client secret. If Vault is enabled, you must specify the secret key and store the password in the Vault in the following format:<br>OAUTH_CLIENT_SECRET/dcis                                                                                                                                                                                                                                                                   |
| oauth_token_endpoint        | Specify the OTDS token endpoint.<br>For example: <a href="http://otds/token">http://otds/token</a>                                                                                                                                                                                                                                                                                                                                              |
| <b>xPlore details</b>       |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Parameter | Description                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------|
| Fetcher   | Specify the Fetcher URL details.<br>For example: <code>http://&lt;host_name&gt;:&lt;port number&gt;</code>                 |
| Parser    | Specify the Parser URL details.<br>For example: <code>http://&lt;host_name&gt;:&lt;port number&gt;/api/v1/extractor</code> |

5. For the Vault-supported environments, follow the steps documented in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
6. To deploy Content Aviator, do the following:

#### Windows

Run the <Extracted Path>/setup.bat file.

#### Linux

Make sure that you have the execute permission and then run the <Extracted Path>/setup.sh file.

7. To verify the successful installation, do the following:

#### Windows

Run the <Extracted Path>/DCIS/dcis\_status.bat and <Extracted Path>/SaaS-Proxy-Client/proxyclient\_status.bat files.

#### Linux

Run the <Extracted Path>/DCIS/dcis\_status.sh and <Extracted Path>/SaaS-Proxy-Client/proxyclient\_status.sh files.

## 11.5 Logging and tracing

OpenText Documentum CM manages the logging and tracing capabilities of the Content Aviator system and includes the following log files:

- DCIS log file: Displays all the DCIS logs generated in the <Extracted Path>/DCIS/dcis.log file.
- SaaS Proxy Client log file: Displays the SaaS proxy client logs generated in the <Extracted Path>/SaaS-Proxy-Client/logs/app.log file.

For additional traces, you can change the log level in <Extracted Path>/DCIS/application-onprem.properties and restart the services.

## 11.6 Uninstalling Content Aviator components

### Windows

Run the <Extracted Path>/uninstall.bat file.

### Linux

Run the <Extracted Path>/DCIS/dcis\_stop.sh and <Extracted Path>/SaaS-Proxy-Client/proxyclient\_stop.sh files.



**Note:** To remove the extracted Content Aviator folders, you must manually delete the <Extracted Path> folder.

## Chapter 12

# Distributed Content configuration

## 12.1 Network locations

Network locations are a basic building block of a single-repository distributed environment for web-based clients. Network locations identify locations on a network, and, optionally, a range of IP addresses, from which users connect to OpenText Documentum CM web clients. For example, a OpenText Documentum CM installation could include network locations called San Francisco, New York, London, Athens, Tokyo, and Sydney, corresponding to users in those cities. A network location can also identify specific offices, network subnets, or even routers.

Network locations are associated with server configuration objects and Accelerated Content Services configuration objects. The server configuration objects and Accelerated Content Services configuration objects contain information defining the proximity of a Documentum CM Server or Accelerated Content Services server to the network location. Documentum CM Server uses the information in the server configuration objects and Accelerated Content Services configuration objects and their associated network locations to determine the correct content storage area from which to serve content to a web client end user and to determine the correct server to serve the content.

Creating network locations requires superuser privileges. Network locations can be created only in a repository designated as a global registry, and the name of each location must be unique among the set of network locations in the global registry. Network locations should be created in the global registry repository that is defined when Foundation Java API is installed on the Documentum Administrator host. If a network contains multiple global registry repositories, a particular Documentum Administrator instance only recognizes the global registry that was designated during Foundation Java API installation on the Documentum Administrator host. You can connect to a global registry repository without being able to create network locations in that global registry.

Use the **Administration > Distributed Content Configuration > Network Locations** navigation in Documentum Administrator to access the Network Locations list page. From the Network Locations list page, you can create, copy, view, modify, and delete network locations.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains more information on network locations.

### 12.1.1 Creating, viewing, or modifying network locations

Network locations should be created in the global registry repository that is defined when Foundation Java API is installed on the Documentum Administrator host. You must have superuser privileges in the global registry repository to create network locations. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides additional information on network locations.



**Note:** When `localhost` is in the URL used from a browser on the application server host to access an application server, it resolves to 127.0.0.1. Unless 127.0.0.1 is included in a network location, the correct network location is not selected automatically. Therefore, when you create network locations, include the IP address 127.0.0.1 in a network location if you want to:

- Run a browser on the application server host where a WDK application is located.
- Use `localhost` in the URL when accessing the application.
- Automatically select the correct network location.

**Table 12-1: Network location properties**

| Field                              | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network Location Identifier</b> | An identifier that is used by system and network administrators. For example, to identify network locations by network subnets. This field cannot be edited after the network location is created.                                                                                                                                                                                                                                                                                     |
| <b>Subject</b>                     | A description of the network location.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Default Network Location</b>    | Select to display the network location to users whose IP address is not mapped to a particular network location.<br><br>At log-in time, an end user whose IP address is not mapped to a network location sees a set of possible network locations. When selected, this network location is on the list from which the user selects. If there is only one network location with this checkbox selected, that network location is used automatically and the user does not see the list. |

| Field                        | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network Location Name</b> | <p>A descriptive name of the network location. For example, the geographical location of the network, such as Paris, San Francisco. The name is displayed on the login page for OpenText Documentum CM web clients when users must choose a network location. The display name is not the object name. The display name can be modified after the network location is created.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>IP Address Ranges</b>     | <p>The IP address range identified by the network location. Each range must conform to standard IP address conventions. A network location may have multiple IP address ranges. It is recommended that each IP address is mapped to a single network location, but if an IP address maps to multiple physical locations, you may need to map that address to multiple network locations.</p> <p>Type the IP address in one of the following formats:</p> <ul style="list-style-type: none"> <li>• IPv4 address range can be entered by separating the two IP address with a hyphen(-). For example: x.x.x.x-x.x.x.x where x is from 0 to 255.</li> <li>• IPv6 address range can be entered by separating the two IP addresses with a hyphen(-). For example: x:x:x:x:x:x:x-x:x:x:x:x:x or x:x::y (ipv6-address/prefix-length) where the x's are the hexadecimal values of the eight 16-bit pieces of the address and y is a decimal value specifying how many of the leftmost contiguous bits of the address comprise the prefix.</li> </ul> |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying network locations.

### 12.1.2 Copying network locations

To save time retying existing information, you can copy a network location file using the **Save As** option. To copy a network location, you must be connected to the repository known to Foundation Java API on the Documentum Administrator host as a global registry and you must be logged in as a user with superuser privileges.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on copying network locations.

### 12.1.3 Deleting network locations

You must have superuser privileges to delete a network location. Users who connect from a location that was mapped to a deleted network location are not automatically mapped when they connect to a web client. If you selected any network locations to be displayed to users who are not automatically mapped, the users see that list when they log in.

Network locations are used to determine which server provides content files to end users. If the network location that you are deleting is associated with any OpenText™ Documentum™ Content Management Branch Office Caching Services or Accelerated Content Services servers, users at those locations could not receive content in the most efficient manner possible.

When you delete network locations, references to the network locations in existing server configuration objects, Accelerated Content Services configuration objects, OpenText Documentum Content Management (CM) Branch Office Caching Services configuration objects, and Branch Office Caching Services caching jobs are not automatically removed. You must manually remove any references to the deleted network locations.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting network locations.

## 12.2 Accelerated Content Services servers

An Accelerated Content Services server is a lightweight server that is automatically created during a Documentum CM Server installation. The Accelerated Content Services server reads and writes content for web-based client applications using HTTP and HTTPS protocols. Accelerated Content Services servers do not modify object metadata but write content to storage areas.

Each Documentum CM Server host installation has one Accelerated Content Services server that communicates with one Documentum CM Server per repository and the Documentum Message Service server. A single Accelerated Content Services server can serve content from multiple repositories. WDK-based applications can use the Accelerated Content Services server if the Accelerated Content Services server is enabled in the app.xml file of the applications.

Most Accelerated Content Services server properties can be modified using Documentum Administrator. Certain Accelerated Content Services server behavior

is configured the `acs.properties` file on the Accelerated Content Services server host and cannot be modified by Documentum Administrator.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides information on modifying the `acs.properties` file and additional information about the Accelerated Content Services server.

The Accelerated Content Services server is configured on the Accelerated Content Services servers configuration page in the **Administration > Distributed Content Configuration > ACS Servers** node. The Accelerated Content Services Servers configuration page displays information about the Accelerated Content Services server, as described in “[Accelerated Content Services server configurations](#)” on page 181.

**Table 12-2: Accelerated Content Services server configurations**

| Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                          | The name that is assigned to the Accelerated Content Services server during the Documentum CM Server installation. The name cannot be modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Documentum Server</b>             | The name of the Documentum CM Server, the Accelerated Content Services server is associated with.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Content Access</b>                | Specifies how the Accelerated Content Services server can access content. Valid values are: <ul style="list-style-type: none"> <li>• <i>Access all stores</i>: The Accelerated Content Services server can access all stores that are connected to the Documentum CM Server.</li> <li>• <i>Access local stores only</i>: The Accelerated Content Services server can read content from local file stores, but is unable to use Surrogate Get to request content files it does not find in the local file stores.</li> <li>• <i>None (disabled)</i>: The Accelerated Content Services server is disabled.</li> </ul> |
| <b>Projections &amp; Stores from</b> | Specifies the connection broker projections, network locations, and local stores information for the Accelerated Content Services server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Description</b>                   | A description of the Accelerated Content Services server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Field           | Description                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dormancy Status | <p>The current dormancy status of the Accelerated Content Services server. Valid values are:</p> <ul style="list-style-type: none"> <li>• Dormant</li> <li>• Active</li> </ul> <p> <b>Note:</b> The Dormancy Status column is only visible for 7.0 and later versions of repositories.</p> |

## 12.2.1 Viewing or modifying the Accelerated Content Services server configuration properties

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing or modifying the Accelerated Content Services server configuration properties.

**Table 12-3: Accelerated Content Services server configuration properties**

| Field                            | Description                                                                                                                                     |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACS Server Configuration</b>  |                                                                                                                                                 |
| <b>Name</b>                      | The name that is assigned to the Accelerated Content Services server during the Documentum CM Server installation. The name cannot be modified. |
| <b>Associated Content Server</b> | The name of the Documentum CM Server, the Accelerated Content Services server is associated with.                                               |
| <b>Description</b>               | A description of the Accelerated Content Services server.                                                                                       |

| Field                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACS Server Version</b>     | <p>The major and minor version of the Accelerated Content Services server.</p> <p>The Accelerated Content Services server version indicates the underlying repository version.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• 2.1: Specifies that the Accelerated Content Services server is part of a OpenText Documentum CM version 6.5 SPx repository.</li> <li>• 2.2: Specifies that the Accelerated Content Services server is part of a OpenText Documentum CM version 6.6 to 6.6 (Patch 21) repository.</li> <li>• 2.3: Specifies that the Accelerated Content Services server is part of a OpenText Documentum CM version 6.6 (Patch 22) to the latest version.</li> </ul> |
| <b>Dormancy Status</b>        | <p>Indicates the dormancy status of Accelerated Content Services server.</p> <p> <b>Note:</b> The Dormancy Status label is only visible for 7.0 and later versions of repositories.</p>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Content Access</b>         | <p>Specifies how the Accelerated Content Services server can access content. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>Access all stores</i>: The Accelerated Content Services server can access all stores that are connected to the Documentum CM Server.</li> <li>• <i>Access local stores only</i>: The Accelerated Content Services server can read content from local file stores in the repository.</li> <li>• <i>None (disabled)</i>: The Accelerated Content Services server is disabled.</li> </ul>                                                                                                                                                                 |
| <b>ACS Server Connections</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Protocol</b>               | <p>The protocol the Accelerated Content Services server uses. Valid values are http and https. Click <b>Add</b> to add a protocol, or select a protocol from the list and click <b>Edit</b> to modify it or <b>Delete</b> to remove the protocol.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Field           | Description                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Base URL</b> | The base URL for the Accelerated Content Services server. The base URL requires the following format:<br><i>&lt;protocol&gt;://&lt;host&gt;:&lt;port&gt;/ACS/servlet/ACS</i> |

## 12.2.2 Accelerated Content Services projections and stores

Accelerated Content Services projections and stores are configured on the Projections & Stores page.

**Table 12-4: Accelerated Content Services projections and stores properties**

| Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source</b>                        | Specifies where to use projections and stores for the Accelerated Content Services server. Valid values are: <ul style="list-style-type: none"> <li><b>Associated Content Server:</b> The Accelerated Content Services server uses the connection broker projections, network locations, and local stores already configured for Accelerated Content Services.</li> <li><b>Settings entered here:</b> You must enter the Accelerated Content Services server uses connection brokers, network locations, and near stores manually.</li> </ul> If you select this option, an <b>Add</b> button displays in the Connection Broker Projections, Network Location Projections, and Local Stores sections. |
| <b>Connection Broker Projections</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Target Host</b>                   | The host name of the server that hosts the connection broker.<br>Click <b>Add</b> to add a target host, or select a host from the list and click <b>Delete</b> to remove the host.<br>The connection broker is a process that provides client sessions with server connection information. Each Accelerated Content Services server broadcasts information to connection brokers at regular intervals.                                                                                                                                                                                                                                                                                                |
| <b>Port</b>                          | The port number on which the connection broker is listening.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Field                               | Description                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enabled</b>                      | Enables projections to the connection broker.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Network Location Projections</b> |                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Network Location</b>             | Specifies a network location in the global registry of the Documentum CM Server host.<br><br>Click <b>Add</b> to add a network location, or select a location from the list and click <b>Delete</b> to remove the location.<br><br>Network locations identify locations on a network, and, optionally, a range of IP addresses, from which users connect to OpenText Documentum CM web clients. |
| <b>Display Name</b>                 | A name that describes the network location.                                                                                                                                                                                                                                                                                                                                                     |
| <b>Proximity</b>                    | The proximity value for the network location.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Enabled</b>                      | Enables projection to that network location.                                                                                                                                                                                                                                                                                                                                                    |
| <b>Local Stores</b>                 |                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Local Store</b>                  | A local store.<br><br>Click <b>Add</b> to add a store, or select a store from the list and click <b>Delete</b> to remove the store.<br><br>Local stores are defined as near to the Accelerated Content Services server.                                                                                                                                                                         |
| <b>Type</b>                         | Specifies the storage type associated with the local store. This property cannot be modified.                                                                                                                                                                                                                                                                                                   |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing or modifying the Accelerated Content Services projection stores.

### 12.2.3 Designating connection brokers for an Accelerated Content Services server

Connection broker projections are configured in the Connection Broker Projections section of the Accelerated Content Services server configurations page.

**Table 12-5: Accelerated Content Services connection broker projections properties**

| Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Source</b>                        | <p>Specifies where to use projections for the Accelerated Content Services server. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>Associated Content Server:</b> The Accelerated Content Services server uses the connection broker projections, network locations, and local stores already configured for Accelerated Content Services.</li> <li>When this option is selected, you cannot modify the connection broker projections.</li> <li>• <b>Settings entered here:</b> Select this option to designate connection broker projections.</li> <li>If you select this option, an <b>Add</b> button displays in the Connection Broker Projections, Network Location Projections, and Local Stores sections.</li> </ul> |
| <b>Connection Broker Projections</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Target Host</b>                   | <p>The host name of the server that hosts the connection broker.</p> <p>Click <b>Add</b> to add a target host, or select a host from the list and click <b>Delete</b> to remove the host.</p> <p>The connection broker is a process that provides client sessions with server connection information. Each Accelerated Content Services server broadcasts information to connection brokers at regular intervals.</p>                                                                                                                                                                                                                                                                                                                        |
| <b>Port</b>                          | The port number on which the connection broker is listening.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Enabled</b>                       | Enables projections to the connection broker.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on designating connection brokers for an Accelerated Content Services server.

### 12.2.4 Choosing network locations

Use the Choose Network Locations page to designate network locations. The network locations displayed on this page are in the global registry known to Foundation Java API on the Documentum Administrator host.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding or deleting network locations.

## 12.3 Branch Office Caching Services servers

Branch Office Caching Services servers cache content locally. Caching content allow quick access to content. The amount of cached content and the storage time can be configured. Content can also be cached programmatically prior to user requests or through a pre-caching job. A Branch Office Caching Services server can serve content from multiple repositories.

Branch Office Caching Services servers communicate only with Accelerated Content Services servers and OpenText™ Documentum™ Content Management Messaging Service servers, but not directly with Documentum CM Servers. Every Branch Office Caching Services server for OpenText Documentum CM 6 or later repositories is associated with a dm\_bocs\_config object. The installation program for the Branch Office Caching Services server does not create the object at installation time. The Branch Office Caching Services server must be added manually, using the properties on the **BOCS Configuration** page. All Branch Office Caching Services configuration objects for OpenText Documentum CM 6 or later repositories reside in the global registry in the /System/BocsConfig folder.

To create, modify, or view Branch Office Caching Services configuration objects, you must have superuser privileges and be connected to the global repository that is associated with the Foundation Java API installation. If you are not connected to the global repository and click the **BOCS Server** node, the system displays an error message and provides a link to the login page of the global registry repository.

### 12.3.1 Creating, viewing, or modifying Branch Office Caching Services servers

You can create, view, or modify the Branch Office Caching Services configuration object in the global registry repository after the Branch Office Caching Services server is installed on its host. To create, view, or modify Branch Office Caching Services configuration objects, you must have superuser privileges and be connected to the global registry that is associated with the Foundation Java API installation.

**Table 12-6: Branch Office Caching Services server properties**

| Field                          | Value |
|--------------------------------|-------|
| BOCS Server Configuration Info |       |

| Field                      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                | <p>The object name of the Branch Office Caching Services server.</p> <p>The object name cannot be modified for existing Branch Office Caching Services server configuration objects.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>         | <p>Description of the Branch Office Caching Services server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>BOCS Server Version</b> | <p>A numeric string that identifies the set of Distributed Content features with which the Branch Office Caching Services server is compatible. In some cases, a set of features spans multiple product versions. Valid values are:</p> <ul style="list-style-type: none"> <li>• 1: The Content Access options are limited to Read Only and None (disabled).</li> <li>• 2.1: Compatible with Documentum CM Server version 6.5 SPx and 6.6.</li> <li>• 2.2: Compatible with Documentum CM Server version 6.6 to 6.6 (Patch 21). This value is used only when Atmos and Accelerated Content Services connector integration is available.</li> <li>• 2.3: Compatible with Documentum CM Server versions 6.6 (Patch 22) to 16.x. This value is only valid if the actual version of the installed Branch Office Caching Services server is from 6.6 (Patch 22) to the latest version.</li> </ul> |
| <b>Content Access</b>      | <p>Select an access type, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Read and synchronous write:</b> Select this option for the Branch Office Caching Services server to support read and synchronous write.</li> <li>• <b>Read, synchronous, and asynchronous write:</b> Select this option for the Branch Office Caching Services server to support read, synchronous write, and asynchronous write.</li> <li>• <b>None (disabled):</b> The Branch Office Caching Services server is disabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                |
| <b>Network Locations</b>   | <p>Network locations served by the Branch Office Caching Services server.</p> <p>Click <b>Select</b> to access the Choose a Network Location page to select network locations.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Field                          | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Repositories</b>            | Select a repository from which to serve content, as follows: <ul style="list-style-type: none"> <li>• <b>all repositories:</b> Content is served from all repositories.</li> <li>• <b>selected repositories only:</b> Serves content from all repositories that are specified on the Include list. Click <b>Edit</b> to add specific repositories.</li> <li>• <b>all except selected repositories:</b> Serves content from all repositories except the repositories that are specified in the Exclude list.</li> </ul> Click the <b>Edit</b> link to add specific repositories to exclude. |
| <b>Proxy URL</b>               | The Branch Office Caching Services proxy URL. The URL can contain up to 240 characters. The Branch Office Caching Services proxy URL is a message URL that only OpenText Documentum Content Management (CM) Messaging Service uses when Branch Office Caching Services is in push mode.                                                                                                                                                                                                                                                                                                    |
| <b>BOCS Server Connections</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Add</b>                     | Click to access the Branch Office Caching Services server connection page to add a protocol and base URL for the Branch Office Caching Services server.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Edit</b>                    | Select a communication protocol and then click <b>Edit</b> to access the Branch Office Caching Services server connection page to edit a protocol and base URL for the Branch Office Caching Services server.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Delete</b>                  | To delete a Branch Office Caching Services server protocol and base URL, select a communication protocol and then click <b>Delete</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Field                        | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protocol and Base URL</b> | The communication protocols used by the Branch Office Caching Services server to provide content to end users. The HTTP and HTTPS protocols are supported. The base URL must be provided when the Branch Office Caching Services server is created. It is in the form:<br><br><code>&lt;protocol&gt;://&lt;host&gt;:&lt;port&gt;/ACS/servlet/ACS</code><br><br>where <i>protocol</i> is http or https; <i>host</i> is the name of the computer on which the Branch Office Caching Services server is installed; and <i>port</i> is the port designated for communications during the Branch Office Caching Services server installation. |

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on creating, viewing, or modifying Branch Office Caching Services servers.

### 12.3.2 Setting Branch Office Caching Services server security

The Branch Office Caching Services server security properties specifies whether the Branch Office Caching Services server is in push or pull mode and is used to upload a public key from the Branch Office Caching Services server.

The Branch Office Caching Services server configuration object in the global registry contains the public key information and generates an electronic signature for the Branch Office Caching Services server to use when contacting the Messaging Service server. When the Branch Office Caching Services server connects to the Messaging Service server in pull or push mode, it sends its electronic signature to Messaging Service where Messaging Service matches the electronic signature to the public key in the Branch Office Caching Services configuration object. If the Messaging Service server authenticates the Branch Office Caching Services electronic signature, the Branch Office Caching Services server can then pull or push its messages from or to the Messaging Service server respectively.

**Table 12-7: Branch Office Caching Services server security properties**

| Field                         | Value                                                                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pull Mode Enabled</b>      | Specifies whether the Branch Office Caching Services server communicates with the Messaging Service server using the pull mode.<br><br>If this option is not selected, the Branch Office Caching Services server communicates with the Messaging Service server using the push mode. |
| <b>Public Key Installed</b>   | Displays the last updated status for the public key.                                                                                                                                                                                                                                 |
| <b>Upload Public Key File</b> | Click <b>Browse</b> to locate and install the public key file for the Branch Office Caching Services server.                                                                                                                                                                         |

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on setting Branch Office Caching Services server security.

### 12.3.3 Setting Branch Office Caching Services server communication protocols

On the **BOCS Server Connection** page, set the communication protocols used by the Branch Office Caching Services server.

To access the **BOCS Server Connection** page, click **Add** or **Edit** in the **BOCS Server Connections** section of the **BOCS Server Configuration** page.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on setting Branch Office Caching Services server communication protocols.

### 12.3.4 Deleting Branch Office Caching Services servers

You can delete Branch Office Caching Services server configuration objects from a global registry repository.

Deleting the configuration object does not uninstall the Branch Office Caching Services servers; they must be manually uninstalled from the hosts on which they are running. Without the configuration object, the Branch Office Caching Services server cannot provide content from this repository.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on deleting Branch Office Caching Services servers.

## 12.4 Configuring distributed transfer settings

The distributed transfer object is created when the repository is created. The distributed transfer configuration object controls whether reading and writing content through Accelerated Content Services is enabled for the repository and whether Branch Office Caching Services pre-caching is also enabled. Administrators cannot create new distributed transfer objects; however, administrators with superuser privileges can configure the default object.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on configuring distributed transfer settings.

## 12.5 Messaging server configuration

A Messaging Service server is an intermediary server that provides messaging services between an Accelerated Content Services or Branch Office Caching Services server and a web application server. The messaging server configuration object must be created and set up in the global registry using Documentum Administrator. Administrators with superuser privileges only can configure the messaging server configuration object. Administrators with superuser privileges connecting to 6.7 and earlier versions, global registry can only create default messaging server configuration object. If a messaging server configuration object exists, administrator cannot create new objects.



**Note:** You can create multiple messaging server configuration objects using Documentum Administrator 7.0 on 7.0 and later versions of Documentum CM Server and repositories. Use the **File > New > Messaging Server Configuration** in the Messaging Server list page.

Use the **Administration > Distributed Content Configuration > Messaging Server** navigation to access the Messaging Server Configuration list page.

To modify or view the Messaging Service server configuration object, you must be connected to the repository known to Foundation Java API on the Documentum Administrator host as a global registry and you must be logged in as a user with superuser privileges. Administrators logging in to a repository that is not the global registry do not see a Messaging Server Configuration list page. If they click the Messaging Server node, the system displays a message informing administrators that they logged in to a non-global registry repository and the messaging server configuration object is stored only in the global registry repository. The system also shows a link for the administrator to click to navigate to the login page of the global registry repository.

To save time retying existing information, you can copy a messaging server configuration using the **Save As** option. To copy a messaging server, you must be connected to the repository known to Foundation Java API on the Documentum Administrator host as a global registry and you must be logged in as a user with superuser privileges.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on the following:

- Viewing or modifying the messaging server configuration
- Copying a messaging server



# Chapter 13

## User management

### 13.1 Administering users, groups, roles, and sessions

Users, groups, roles, and sessions are managed in the User Management page under the **Administration > User Management** node.

The User Management page contains links to the user management features that can be configured for a repository, as described in “[Users, groups, roles, and sessions](#)” on page 195.

**Table 13-1: Users, groups, roles, and sessions**

| Link          | Description                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Users</b>  | Accesses the Users page. From the Users page you can <ul style="list-style-type: none"><li>• Search for existing user accounts.</li><li>• Create, modify, and delete user accounts.</li><li>• View and assign group memberships for a particular user account.</li><li>• Change the home repository for particular user accounts.</li></ul> <p><a href="#">“Users” on page 196</a> contains more information on user accounts.</p> |
| <b>Groups</b> | Accesses the Groups page. From the Groups page you can <ul style="list-style-type: none"><li>• Search for existing group accounts.</li><li>• Create, modify, and delete group accounts.</li><li>• View and reassign group a particular group account.</li></ul> <p><a href="#">“Groups” on page 211</a> contains more information on group accounts.</p>                                                                           |

| Link                | Description                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Roles</b>        | <p>Accesses the Roles page. From the Roles page you can</p> <ul style="list-style-type: none"><li>• Search for existing roles.</li><li>• Create, modify, and delete roles.</li><li>• View current group memberships and reassign roles.</li></ul> <p><a href="#">“Roles” on page 218</a> contains more information on roles.</p>                                                     |
| <b>Module Roles</b> | <p>Accesses the Modules Roles page. From the Modules Roles page you can</p> <ul style="list-style-type: none"><li>• Search for existing module roles.</li><li>• Create, modify, and delete module roles.</li><li>• View current group memberships and reassign module roles.</li></ul> <p><a href="#">“Modules roles” on page 221</a> contains more information on module roles.</p> |
| <b>Sessions</b>     | <p>Accesses the Sessions page. From the Sessions page you can</p> <ul style="list-style-type: none"><li>• Search for sessions.</li></ul> <p>View session properties and session logs.</p> <p><a href="#">“Sessions” on page 223</a> contains more information on sessions.</p>                                                                                                       |

## 13.2 Users

A repository user is a person or application with a user account that has been configured for a repository. User accounts are created, managed, and deleted on the User node. In a repository, user accounts are represented by user objects. Whenever a new user account is added to a repository, Documentum CM Server creates a user object. A user object specifies how a user can access a repository and what information the user can access.

### 13.2.1 Locating users

Use the search filters on the Users page to locate users.

**Table 13-2: User search filters**

| Field             | Description                                               |
|-------------------|-----------------------------------------------------------|
| User Name         | Filters the search results by user name.                  |
| Default Group     | Filters the search results the name of the default group. |
| User Login Name   | Filters the search results by the login name of the user. |
| User Login Domain | Filters the search results by login domain.               |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on locating users.

### 13.2.2 Creating or modifying users

You must be the installation owner, or have system administrator or superuser privileges to create users. Superusers and system administrators cannot modify their own extended privileges.

Before you create users, determine what type of authentication the server uses. If the server authenticates users against the operating system, each user must have an account on the server host.

If the repository is the governing member of a federation, a new user can be a global user. Global users are managed through the governing repository in a federation, and have the same attribute values in each member repositories within the federation. If you add a global user to the governing repository, that user is added to all the member repositories by a federation job that synchronizes the repositories.

**Table 13-3: User properties**

| Field                    | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>State</b>             | <p>Indicates the user account state in the repository. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>Active</i>: The user is a currently active repository user. Active users are able to connect to the repository.</li> <li>• <i>Inactive</i>: The user is not currently active in the repository. Inactive users are unable to connect to the repository. The user automatically moves to ACTIVE state after auth_deactivation_interval minutes, if auth_deactivation_interval is greater than zero.</li> <li>• The user is automatically assigned to INACTIVE state by Documentum CM Server if the user exceeds max_auth_attemp failure attempts within auth_failure_interval minutes.</li> <li>• <i>Locked</i>: The user is unable to connect to the repository.</li> <li>• <i>Locked and inactive</i>: The user is inactive and unable to connect to the repository. The user moves to locked and inactive states, if a locked user exceeds max_auth_attemp failure attempts within auth_failure_interval minutes.</li> </ul> <p>If the user is a superuser, only another superuser can reset the state.</p> |
| <b>Name</b>              | The user name for the new user. The user name cannot be modified, but can be reassigned to another user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>User Login Name</b>   | <p>The login name used for authenticating a user in repositories.</p> <p>If the user is an operating system user, the user login name must match the operating system name of the user.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>User Login Domain</b> | Identifies the domain in which the user is authenticated. This is typically a Windows domain used for authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Field            | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Source      | <p>Specifies how to authenticate user name and password of a given repository user. Valid values depend on whether the repository runs on a Linux or Windows server.</p> <ul style="list-style-type: none"> <li>• <i>None</i>: The user is authenticated in a Windows domain.</li> <li>• <i>UNIX only</i>: The user is authenticated using the default Linux mechanism, dm_check_password or other external password checking program.</li> <li>• <i>Domain only</i>: The user is authenticated against a Windows domain.</li> <li>• <i>UNIX first</i>: This is used for Linux repositories where Windows domain authentication is in use. The user is authenticated first by the default Linux mechanism; if that fails, the user is authenticated against a Windows domain.</li> <li>• <i>Domain first</i>: This is used for Linux repositories where Windows domain authentication is in use. The user is authenticated first against a Windows domain; if that fails, the user is authenticated by the default Linux mechanism.</li> <li>• <i>OTDS</i>: The user is authenticated against OTDS.</li> <li>• <i>Inline Password</i>: The user is authenticated based on a password stored in the repository. This option is available only when Documentum Administrator is used to create users. It is not available in other applications in which it is possible to create users.</li> </ul> <p> <b>Note:</b> If the value of <b>User Source</b> is <i>None</i> or <i>Domain only</i> then user must have the <b>Allow logon locally</b> privilege to change the password. You can change the user privileges using <b>Administrative Tools</b> in Windows.</p> |
| Password         | <p>The password for the user. Make sure that you follow the password complexity rules. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> contains detailed information about password complexity rules.</p> <p>This field is displayed if Inline Password is selected as the User Source. Type the password, which is then encrypted and stored in the repository.</p> <p>This must be provided manually for users added using an imported LDIF file.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Confirm Password | <p>The password for the user.</p> <p>This field is displayed if Inline Password is selected as the User Source. Enter the same password you entered in the <b>Password</b> field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Description      | A description of the user account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| E-Mail Address   | The email address of the user. This is the email address to which notifications are sent for workflow tasks and registered events.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Field                     | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User OS Name              | The operating system user name of the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Windows Domain            | The Windows domain associated with the user account or the domain on which the user is authenticated. The latter applies if Documentum CM Server is installed on a Linux host and Windows domain authentication is used.                                                                                                                                                                                                                                                                         |
| Home Repository           | The repository where the user receives notifications and tasks.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| User is global            | If the user is created in the governing repository of a federation, select this option to propagate the user account to all members of the federation.                                                                                                                                                                                                                                                                                                                                           |
| Restrict Folder Access To | Specifies which folders the user can access. Click <b>Select</b> to specify a cabinet or folder. Only the selected cabinets and folders display for the user. The other folders do not display but the user can access the folders using the search or advanced search options.<br><br>If no folders or cabinets are specified, the user has access to all folders and cabinets in the repository, depending on the permissions on those cabinets and folders, and depending on folder security. |
| Default Folder            | The default storage place for any object the user creates. This option only displays when you are creating a user. Valid values are: <ul style="list-style-type: none"> <li>• <b>Choose existing folder:</b> Select this option to assign a folder you already created as the default folder for that user.</li> <li>• <b>Choose/Create folder with the user name:</b> Select this option to automatically create a folder with the name of the user as the object name.</li> </ul>              |
| Default Group             | The group that is associated with the default permission set of the user. Click <b>Select</b> to specify a default group.<br><br>When the user creates an object in the repository, it automatically belongs to this group.                                                                                                                                                                                                                                                                      |
| Default Permission Set    | The permission set that assigns the default permissions to objects the user creates. Click <b>Select</b> to specify a default permission set.                                                                                                                                                                                                                                                                                                                                                    |
| Db Name                   | The user name of the user in the underlying RDBMS. The DB Name is only required if the user is a repository owner or a user who registers RDBMS tables.                                                                                                                                                                                                                                                                                                                                          |

| Field                      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Privileges</b>          | <p>The privileges that are assigned to the user.</p> <p>User privileges authorize certain users to perform activities in the repository. Select one of the privileges from the drop-down list, as follows:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Create Type</li> <li>• Create Cabinet</li> <li>• Create Cabinet and Type</li> <li>• Create Group</li> <li>• Create Group and Type</li> <li>• Create Group and Cabinet</li> <li>• Create Group, Cabinet, and Type</li> <li>• System administrator</li> <li>• Superuser: If you grant superuser privileges to a user, add that user manually to the group called admingroup. If you revoke the superuser privileges of a user, remove the user from the admingroup.</li> </ul>                                                                                                                                                                                           |
| <b>Extended Privileges</b> | <p>Specifies the auditing privileges for the user. Superusers and system administrators cannot modify their own extended privileges.</p> <ul style="list-style-type: none"> <li>• <i>None</i>: The user cannot configure auditing, view audit trails, or purge audit trails.</li> <li>• <i>Config audit</i>: The user can configure auditing.</li> <li>• <i>Purge audit</i>: The user can purge existing audit trails.</li> <li>• <i>Config and Purge Audit</i>: The user can configure auditing and purge existing audit trails.</li> <li>• <i>View Audit</i>: The user can view audit trails.</li> <li>• <i>Config and View Audit</i>: The user can configure auditing and view existing audit trails.</li> <li>• <i>View and Purge Audit</i>: The user can view existing audit trails and purge them.</li> <li>• <i>Config, View, and Purge Audit</i>: The user can configure auditing and view and purge existing audit trails.</li> </ul> |

| Field                                          | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Client Capability</b>                       | <p>Describes the expertise level of the user.</p> <p>The client capability setting is used by OpenText Documentum CM client products to determine which functionality to deliver to the user. Documentum CM Server does not recognize or use the client capability setting. The OpenText Documentum CM client documentation contains the information on the client features available with each setting.</p> <p>Choose a user type from the list:</p> <ul style="list-style-type: none"><li>• Consumer</li><li>• Contributor</li><li>• Coordinator</li><li>• System Administrator</li></ul> |
| <b>Alias Set</b>                               | The default alias set for the user. Click <b>Select</b> to specify an alias set.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Disable Workflow</b>                        | Indicates whether a user can receive workflow tasks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Disable Authentication Failure Checking</b> | If selected, user can exceed the number of failed logins specified in the Maximum Authentication Attempts field of the repository configuration object.                                                                                                                                                                                                                                                                                                                                                                                                                                     |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating or modifying user accounts.

### 13.2.3 Creating global users

A *global user* is a repository user who is found in all members of a repository federation and whose attribute values are the same in all of the repositories. Global users are managed through the governing repository. If you add a global user to the governing repository, that user is added to all the member repositories by a federation job that synchronizes the repositories.

To create a global user, connect to the governing repository of a federation and create the user there. On the New User - Info page, select **User is global** to make the user global.

Connect to the governing repository to modify the attributes of a global user.

Global users can also have local attributes, which you can modify in a local repository.

### 13.2.4 Setting default permissions for folders and cabinets

When you create a new user, you assign the user a default folder. Documentum Administrator allows you to select between assigning an existing folder as the default folder or creating a folder with the name of user. If you have Documentum Administrator create the folder for a new user and you can control the permissions assigned to folder.

#### To set default permissions for folders:

1. Create a alias set called UserPropertiesConfiguration.
2. Assign ownership of the UserPropertiesConfiguration alias set to the repository owner.

This is the user whose account is used for database access (dm\_dbo).
3. Create two aliases in UserPropertiesConfiguration.
  - DefaultFolderAcl

Point this alias to the permission set to be applied to the new folder created for new users.
  - DefaultFolderAclDomain

Point this alias to the user who owns the permission set you use for the DefaultFolderAcl alias.

When you add a user, Documentum Administrator applies the permission set you designate to the new folder. If a new user is not present as an accessor in the permission set, the user is granted write permission on the folder. The permission set for the folder is then modified to a system-generated permission set, but it otherwise has the permissions from the permission set you created.

You can use Documentum Administrator to create a default folder for an existing user and permissions on the set are applied if you have created the necessary alias set and aliases.

If the UserPropertiesConfiguration alias set does not exist and a superuser creates the user, the user owns the folder and has delete permission. If a system administrator creates the user, the user is not the owner of the default folder, but the user has change owner permission on the folder as well as write permission.

### 13.2.5 Importing users

You can create repository users from information contained in an input file. Before you begin importing users, determine the following:

- Authentication type

If the server authenticates users against the operating system, each user must have an account on the server host.

- Groups and ACLs

If you specify the attributes `user_group` (the default group of user) and `acl_name` (the default permission set of user), any groups and permission sets must already exist before you import the users.

- Passwords

If you are creating a user who is authenticated using a password stored in the repository, the password cannot be assigned in the input file. You must assign the password manually by modifying the user account after the user has been imported..

**Table 13-4: Import user properties**

| Field         | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>State</b>  | Indicates the state of user in the repository. Select one of the following: <ul style="list-style-type: none"><li>• <i>Active</i>: The user is a currently active repository user. Active users are able to connect to the repository.</li><li>• <i>Inactive</i>: The user is not currently active in the repository. Inactive users are unable to connect to the repository.</li></ul> If the user is a superuser, only another superuser can reset the state. |
| <b>Source</b> | The name of an input file. Click <b>Browse</b> to browse to the location of the LDIF file containing information for creating the new users.                                                                                                                                                                                                                                                                                                                    |

| Field                  | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>User Source</b>     | <p>Specifies how to authenticate user name and password of a given repository user. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>None</i>: Windows only. This means the user is authenticated in a Windows domain.</li> <li>• <i>UNIX only</i>: The user is authenticated using the default Linux mechanism, <code>dm_check_password</code> or other external password checking program. This option only displays on Linux hosts.</li> <li>• <i>Domain only</i>: The user is authenticated against a Windows domain. This option only displays on Linux hosts.</li> <li>• <i>UNIX first</i>: This is used for Linux repositories where Windows domain authentication is in use. This option only displays on Linux hosts.</li> </ul> <p>The user is authenticated first by the default Linux mechanism. If the authentication fails, the user is authenticated against a Windows domain.</p> <ul style="list-style-type: none"> <li>• <i>Domain first</i>: This is used for Linux repositories where Windows domain authentication is in use. This option only displays on Linux hosts.</li> </ul> <p>The user is authenticated first against a Windows domain; if that fails, the user is authenticated by the default Linux mechanism.</p> |
| <b>Description</b>     | A description of the user account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>E-Mail Address</b>  | The email address of the user. This is the email address to which notifications are sent for workflow tasks and registered events.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Windows Domain</b>  | (Windows only) The domain name associated with the Windows account of new user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Home Repository</b> | The repository where the user receives notifications and tasks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>User is global</b>  | If the user is created in the governing repository of a federation, select this option to propagate the user account to all members of the federation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default Folder</b>  | The default storage place for any object the user creates. Click <b>Select</b> to assign a folder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Field                | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Group</b> | <p>The group that is associated with the default permission set of the user. Click <b>Select</b> to specify a default group.</p> <p>When the user creates an object in the repository, it automatically belongs to this group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Default ACL</b>   | <p>The permission set that assigns the default permissions to objects the user creates. Click <b>Select</b> to specify a default permission set.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Db Name</b>       | <p>The user name of the user in the underlying RDBMS. The DB Name is only required if the user is a repository owner or a user who registers RDBMS tables.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Privileges</b>    | <p>The privileges that are assigned to the user.</p> <p>User privileges authorize certain users to perform activities in the repository. Select one of the privileges from the drop-down list, as follows:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Create Type</li> <li>• Create Cabinet</li> <li>• Create Cabinet and Type</li> <li>• Create Group</li> <li>• Create Group and Type</li> <li>• Create Group and Cabinet</li> <li>• Create Group, Cabinet, and Type</li> <li>• System Administrator</li> <li>• Superuser: If you grant superuser privileges to a user, add that user manually to the group called <code>admingroup</code>. If you revoke the superuser privileges of a user, remove the user from the <code>admingroup</code>.</li> </ul> |

| Field                                                  | Value                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Client Capability</b>                               | Indicates what expertise level of the user. This option is for informative purposes only and is not associated with any privileges. Documentum CM Server does not recognize or enforce these settings.<br><br>Choose a user type from the list: <ul style="list-style-type: none"><li>• Consumer</li><li>• Contributor</li><li>• Coordinator</li><li>• System Administrator</li></ul> |
| <b>Alias Set</b>                                       | The default alias set for the user. Click <b>Select</b> to specify an alias set.                                                                                                                                                                                                                                                                                                      |
| <b>If user exists, then overwrite user information</b> | Select this option if a user already exists in the repository and you want to replace existing information with the imported information.                                                                                                                                                                                                                                             |
| <b>If user exists, then ignore information</b>         | Select this option if a user already exists in the repository and you want to retain the existing information.                                                                                                                                                                                                                                                                        |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on importing new users.

### 13.2.5.1 Import file format

You can create repository users from information contained in an input file.

Each imported user starts with the header object\_type:dm\_user. Follow the header with a list of attribute\_name:attribute\_value pairs. The attributes user\_name and user\_os\_name are required. In addition, the following default values are assigned when the LDIF file is imported:

**Table 13-5: Default values for new users**

| Argument          | Default   |
|-------------------|-----------|
| user_login_name   | username  |
| privileges        | 0 (None)  |
| folder            | /username |
| group             | docu      |
| client_capability | 1         |

Each *attribute\_name:attribute\_value* pair must be on a new line. For example:

```
object_type:dm_user
user_name:Pat Smith
user_group:accounting
acl_domain:smith
acl_name:Global User Default ACL
object_type:dm_user
user_name:John Brown
```

If the ldif file contains umlauts, accent marks, or other extended characters, store the file as a UTF-8 file, or users whose names contain the extended characters are not imported.

The attributes you can set through the LDIF file are:

```
user_name
user_os_name
user_os_domain
user_login_name
user_login_domain
user_password
user_address
user_db_name
user_group_name
user_privileges (set to integer value)
default_folder
user_db_name
description
acl_domain
acl_name
user_source (set to integer value)
home_docbase
user_state (set to integer value)
client_capability (set to integer value)
globally_managed (set to T or F)
alias_set_id (set to an object ID)
workflow_disabled (set to T or F)
user_xprivileges (set to integer value)
failed_auth_attempt (set to integer value)
```

You can specify as many of the attributes as you wish, but the attribute\_names must match the actual attributes of the type.

The attributes may be included in any order after the first line (object\_type:dm\_user). The Boolean attributes are specified using T (for true) or F (for false). Use of true, false, 1, or 0 is deprecated.

Any ACLs that you identify by acl\_domain and acl\_name must exist before you run the file to import the users. Additionally, the ACLs must represent system ACLs. They cannot represent private ACLs.

Any groups that you identify by user\_group\_name must exist before you run the file to import the users.

Documentum CM Server creates the default folder for each user if it does not already exist.

### 13.2.6 Deleting users

You can remove users from the repository, but OpenText recommends making users inactive or reassigning them rather than deleting them from the repository.

When you delete a user, the server does not remove the user's name from objects in the repository such as groups and ACLs. Consequently, when you delete a user, you must also remove or change all references to that user in objects in the repository.

You can delete a user and then create a user with the same name. If you add a new user with the same name as a deleted user and have not removed references to the deleted user, the new user inherits the group membership and object permissions belonging to the deleted user.

You cannot delete the repository owner, installation owner, or yourself.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on deleting users.

### 13.2.7 Reassigning objects to another user

If you want to delete a user from the repository, make the user inactive, or rename a user, you can assign objects owned by that user to another user. For example, to change the user name of a particular user, you have to create a new user and assign the objects that belonged to the old user name to the new user.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on reassigning objects to another user.

### 13.2.8 Changing the home repository of a user

The home repository is where users receive tasks and notifications in their inboxes.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on changing the home repository of a user.

### 13.2.9 Activating or deactivating a user account

Changing a user account from active to inactive is an alternative to deleting the user from the repository. If the account is a superuser account, only another superuser can reset the account.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on changing a user from active to inactive or inactive to active.

### 13.2.10 Viewing groups, workflows, alias sets, permission sets, and documents of a user

You can determine the groups to which a user belongs.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing the groups, workflows, permission sets, alias sets, or documents of a user.

### 13.2.11 Viewing or deleting change home repository logs

You can view or delete the logs generated by changing the home repository of user.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing or deleting change home repository logs.

### 13.2.12 Viewing user reassign logs

You can view or delete the logs generated by reassigning objects of user to another user.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing the user reassign logs.

### 13.2.13 Reassigning reports

This page displays reassign logs, including group and user reassign logs.

### 13.2.14 Managing user profile picture

Documentum CM Server supports the managing of user profile pictures. It provides the ability to associate the user profile picture with the user object (dm\_user). You can add, modify, retrieve, and remove a user profile picture using OpenText Documentum CM clients (for example, Foundation Java API).



#### Notes

- All users have permissions to update or remove their own profile pictures only.
- This feature is not available in the **User Management** node in Documentum Administrator.

The format (for example, PNG) of the user profile picture must comply with the Documentum CM Server-supported image formats where the MIME type of the dm\_format object must be `image/*`. The size of the user profile picture must not exceed 5 MB.

Documentum CM Server creates `user_image`, a location object with a directory named `user_images` under the default data directory for the repository. The user profile picture is stored by converting the `r_object_id` sequence to the directory structure (two digits each) with last two digits as filename. For example, if `r_object_id` of user is `1100000180000000`, then the user profile picture is stored as follows:

```
path: configured with location as 'user_image'
file structure: \80\00\00\00.<format>
```

In a multi-server distributed setup, you must modify the location to UNC path or NFS/CIFS share so that all Documentum CM Server instances can access the user profile picture. In addition, Documentum CM Server provides audit events that can be configured for tracking all operations related to the user profile picture.

The Foundation Java API events for managing the user profile picture are `dm_user_updatepicture`, `dm_user_removepicture`, and `dm_user_retrievepicture`. “[Foundation Java API events](#)” on page 615 contains more information.

## 13.3 Groups

A group represents multiple repository users, and can contain groups, users, or roles. By default, a group is owned by the user who creates the group. Groups can be public or private. By default, groups created by a user with Create Group privileges are private, while groups created by a user with system administrator or superuser privileges are public.

A group can be a *dynamic* group. A dynamic group is a group, of any group class, whose list of members is considered a list of potential members.

To create or modify groups, you must have privileges as shown in the following table:

**Table 13-6: Privileges for creating or modifying groups**

| Privilege    | Create                                                                     | Modify                                                                               | Delete                                                                                                          |
|--------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Create Group | Can create group or assign ownership to a group to which the user belongs. | Can add or delete members and assign ownership to a group to which the user belongs. | Can delete groups the user owns, including groups where a group is owner and the user is a member of the group. |

| Privilege            | Create                                                                     | Modify                                                                                                                                             | Delete                                                                                                                                          |
|----------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| System administrator | Can create group or assign ownership to a group to which the user belongs. | Can update the group the system administrator owns, including groups where a group is owner and the system administrator is a member of the group. | Can delete groups the system administrator owns, including groups where a group is owner and the system administrator is a member of the group. |
| Superuser            | Can create a group and assign ownership to a different user or group.      | Can update group administrator, owner, or members of a group.                                                                                      | Can delete any group.                                                                                                                           |

A group can own SysObjects and permission sets.

The name assigned to a group must consist of characters that are compatible with the Documentum CM Server **OS code** page.

If you create a role as a domain, it is listed on the groups list, not the roles list.

To jump to a particular group, type the first few letters of its object name in the **Starts with** box and click **Search**. To view a list of all groups beginning with a particular letter, click that letter. To view a different number of groups than the number currently displayed, select a different number in the **Show Items** list.

To view the members of a group, click the group name.

### 13.3.1 Dynamic groups

A dynamic group is a group, of any group class, whose list of members is considered a list of potential members. A dynamic group is created and populated with members similar to any other group. Whether or not a group is dynamic is part of the groups definition. It is recorded in the `is_dynamic` attribute and can be changed after the group is created. (In this application, `is_dynamic` is the field labeled **Dynamic Group**.)

When a session is started, whether Documentum CM Server treats a user in a dynamic group as an actual member is dependent on two factors:

- The default membership setting in the group object
- Whether the application from which the user is accessing the repository requests that the user be added or removed from the group

You can use dynamic groups to model role-based security. For example, suppose you define a dynamic group called `EngrMgrs`. Its default membership behavior is to assume that users are not members of the group. The group is granted the privileges to change ownership and change permissions. When a user in the group accesses the

repository from a secure application, the application can issue the session call to add the user to the group. If the user accesses the repository from outside your firewall or from an unapproved application, no session call is issued and Documentum CM Server does not treat the user as a member of the group. The user cannot exercise the change ownership or change permissions permits through the group.

### 13.3.2 Privileged groups

Installing Documentum CM Server installs a set of privileged groups. Members of privileged are allowed to perform privileged operations even though the members do not have the privileges as individuals. The privileged groups are divided into two sets.

The first set of privileged groups are used in applications or for administration needs. With two exceptions, these privileged groups have no default members when they are created. You must populate the groups. The following table describes these groups:

**Table 13-7: Privileged groups**

| Group                           | Description                                                                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dm_browse_all                   | Members of this group can browse any cabinets and folders in the repository, folders except the rooms that were created using Documentum Collaborative Services.<br><br>The dm_browse_all_dynamic is a member of this group by default.   |
| dm_browse_all_dynamic           | This is a dynamic role group whose members can browse any object in the repository. The dm_browse_all_dynamic group is a member of the dm_browse_all group.                                                                               |
| dm_escalated_allow_save_on_lock | Used internally for OpenText™ Documentum™ Content Management Retention Policy Services.<br><br>Created and managed by superusers only. Members of this group can modify and save changes to an object that is checked out by other users. |

| Group                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dm_retention_managers | <p>Members of this group can:</p> <ul style="list-style-type: none"> <li>• Own retainer objects (representing retention policies)</li> <li>• Add and remove a retainer from any SysObject.</li> <li>• Add and remove content in a retained object</li> <li>• Change the containment in a retained virtual document</li> </ul> <p>This is a non-dynamic group.</p>                                                                                                                                                               |
| dm_retention_users    | <p>Members of this group can add retainers (retention policies) to SysObjects.</p> <p>This is a non-dynamic group.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |
| dm_superusers         | <p>Members of this group are treated as superusers in the repository.</p> <p> <b>Note:</b> Adding an user to the dm_superusers privilege group does not offer superuser privileges to that user until a particular Foundation Java API API is called. Also, calling that API offers the privileges to the user only for that session and it is not permanent.</p> <p>The dm_superusers_dynamic group is a member of this group by default.</p> |
| dm_superusers_dynamic | <p>A dynamic role group whose members are treated as superusers in the repository. The dm_superusers_dynamic group is a member of the dm_superusers group.</p>                                                                                                                                                                                                                                                                                                                                                                  |
| dm_sysadmin           | <p>Members of this group are treated as users with system administrator user privileges.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| dm_create_user        | <p>Member of this group have Create User user privilege.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| dm_create_type        | <p>Member of this group have Create Type user privilege.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| dm_create_group       | <p>Member of this group have Create Group user privilege.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| dm_create_cabinet     | <p>Member of this group have Create Cabinet user privilege.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

The second set of privileged groups are privileged roles that are used internally by Foundation Java API. You cannot add or remove members from these groups. The groups are:

- dm\_assume\_user
- dm\_datefield\_override
- dm\_escalated\_delete
- dm\_escalated\_full\_control
- dm\_escalated\_owner\_control
- dm\_escalated\_full\_control
- dm\_escalated\_relate
- dm\_escalated\_version
- dm\_escalated\_write
- dm\_internal\_attrib\_override
- dm\_user\_identity\_override

### 13.3.3 Locating groups

You can locate groups in a repository.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on locating groups.

### 13.3.4 Viewing group memberships

You can view where a group is used.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing group memberships.

### 13.3.5 Creating, viewing, or modifying groups

You can create a group or view and modify group properties on the Info tab of the New Group and Group properties pages.

**Table 13-8: Group properties**

| Field             | Value                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------|
| Name              | The name of the repository group.                                                                            |
| Group Native Room | The native room of group. This field appears only if the rooms feature of Collaborative Services is enabled. |

| Field                  | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E-Mail Address</b>  | <p>The email address for the new group.</p> <p>If no value is entered in this field, the group email address defaults to the group name.</p>                                                                                                                                                                                                                                                                                                                                                        |
| <b>Owner</b>           | <p>The name of a repository user who has the Create Group privilege and who owns this group.</p> <p>If you are a superuser, you can select the owner. Otherwise, you can set this to a group of which you are a member.</p>                                                                                                                                                                                                                                                                         |
| <b>Administrator</b>   | <p>Specifies a user or group, in addition to a superuser or the group owner, who can modify the group. If this is null, only a superuser and the group owner can modify the group.</p> <p>Only a superuser and the group owner can change the administrator of a group.</p>                                                                                                                                                                                                                         |
| <b>Alias Set</b>       | The default alias set for the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Group is Global</b> | Displayed only in the governing repository of a federation and the group must be a global group.                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Description</b>     | A description of the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Private</b>         | <p>Defines whether the group is private. If not selected, the group is created as a public group.</p> <p>A group with Private enabled can be updated only by a user who is the owner of the group or is listed as the group administrator of the group.</p> <p>A group with Private not enabled can be updated by a user with system administrator privileges as well as by the group owner or administrator.</p> <p>A superuser can update any group, regardless if Private is enabled or not.</p> |

| Field            | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dynamic</b>   | Indicates if the group is a dynamic group. A dynamic group is a group, of any group class, whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic group comprise of the set of users who are allowed to use the group; but a session started by one of those users will behave as though it is not part of the group until it is specifically requested by the application. |
| <b>Protected</b> | Indicates if the group is protected against adding or deleting members. Use of a protected dynamic group is limited to applications running with a Foundation Java API installation that has been configured as privileged through the Documentum Administrator client rights administration.<br><br>The Protected checkbox is enabled only when Dynamic Group is selected.                                                                                                                               |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying groups.

### 13.3.6 Adding users, groups, or roles to a group

A group can contain users, other groups, or roles. You can add users, groups, or roles to a group.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding users to a group.

### 13.3.7 Removing users from a group

You can remove users from a group.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on removing users from a group.

### 13.3.8 Deleting groups

You can delete a group if you are the owner of group, a superuser, a member of the group that owns the group to be deleted, or identified in the group\_admin attribute of group, either as an individual or as a member of a group specified in the attribute. However, to preserve repository consistency, do not remove groups from the repository. Instead, remove all members of the group and leave the group in the repository, or reassign all objects owned by the group to another group or user and then delete the group.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting a group.

### 13.3.9 Reassigning the objects owned by a group

You can reassign the objects owned by a group to another group.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on reassigning a group.

### 13.3.10 Viewing group reassign logs

You can view or delete the logs generated by reassigning the members of a group to another group.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing group reassign logs.

## 13.4 Roles

A role is a type of group that contains a set of users or other groups that are assigned a particular role within a client application domain.

If you create a role as a domain, it is listed in the groups list, not the roles list.

### 13.4.1 Creating, viewing, or modifying roles

You can create, view, or modify roles.

**Table 13-9: Role properties**

| Field             | Value                                                                                                           |
|-------------------|-----------------------------------------------------------------------------------------------------------------|
| Name              | The name of the repository role.                                                                                |
| Group Native Room | The native room for the role. The field appears only if the rooms feature of Collaborative Services is enabled. |

| Field                        | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>E-Mail Address</b>        | The email address for the new role. This is typically the email address of the owner of role.<br><br>If no value is entered in this field, the role email address defaults to the role name.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Owner</b>                 | The name of a repository user who has the Create Group privilege and who owns this role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Administrator</b>         | Specifies a user or group, in addition to a superuser or the role owner, who can modify the role. If this is null, only a superuser and the role owner can modify the role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Alias Set</b>             | The default alias set for the role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Role Is Global</b>        | If the role is being created in the governing repository of a federation, select to propagate the attributes of role to all members of the federation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Description</b>           | A description of the role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Private</b>               | Defines whether the role is private. If not selected, the role is created as a public role.<br><br>A role with Private enabled can be updated only by a user who is the owner of the role or is listed as the roll administrator. A role with Private not enabled can be updated by a user with system administrator privileges as well as by the role owner or administrator. A superuser can update any role, regardless if Private is enabled or not.<br><br>By default, roles created by users with System Administration or superuser privileges are public, and roles created by users with a lower user privilege level are private. |
| <b>Create role as domain</b> | Select to create a dm_group object with group_class as domain.<br><br>This field only appears on the New Role - Info page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Field            | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Dynamic</b>   | Indicates if the role a dynamic role. A dynamic role is a role whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic role comprise of the set of users who are allowed to use the role; but a session started by one of those users will behave as though it is not part of the role until it is specifically requested by the application. |
| <b>Protected</b> | Indicates if the role is protected against adding or deleting members. Use of a protected dynamic role is limited to applications running with a Foundation Java API installation that has been configured as privileged through the Documentum Administrator client rights administration.<br><br>The Protected checkbox is enabled only when Dynamic Role is selected.                                                                                                   |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating roles.

### 13.4.2 Adding users, groups, or roles to a role

You can add users, groups, or roles to a role.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding users, groups, or roles to a role.

### 13.4.3 Reassigning roles

If you plan to delete a role, consider reassigning the users and other objects belonging to the role. You can reassign the users and other objects.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on reassigning a role.

### 13.4.4 Deleting roles

Roles are a type of group. It is therefore recommended that you do not delete a role. Instead, remove all members of the role and leave the role in the repository. You can also reassign the members of the role to another role.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting a role.

## 13.5 Modules roles

Module roles are required by applications that run privileged escalations and they behave the same as roles with respect to memberships. Module roles are dm\_group objects with group\_class set to module role. Any user, group, or dynamic group can be a member of a module role.

By default, module roles are dynamic. A dynamic module role is a role whose list of members is considered a list of potential members. User membership is controlled on a session-by-session basis by the application at runtime. The members of a dynamic module role comprise of the set of users who are allowed to use the module role; but a session started by one of those users will behave as though it is not part of the module role until it is specifically requested by the application. Administrators should not modify module roles unless they are configuring a client that requires privileged escalations.

### 13.5.1 Creating, viewing, or modifying module roles

You can create new module roles.

**Table 13-10: Module role properties**

| Field             | Value                                                                                                                                               |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Name              | The name of the repository module role.                                                                                                             |
| Group Native Room | The native room for the module role. The field appears only if the rooms feature of Collaborative Services is enabled.                              |
| E-Mail Address    | The email address for the module role.<br><br>If no value is entered in this field, the module role email address defaults to the module role name. |
| Owner             | The name of a repository user who has the Create Group privilege and who owns this module role.                                                     |

| Field                        | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Administrator</b>         | Specifies a user or group, in addition to a superuser or the module role owner, who can modify the module role. If this is null, only a superuser and the module role owner can modify the module role.                                                                                                                                                                                                                                                                                            |
| <b>Alias Set</b>             | The default alias set for the module role.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Module Role is Global</b> | If the module role is being created in the governing repository of a federation, select to propagate the attributes of module role to all members of the federation.                                                                                                                                                                                                                                                                                                                               |
| <b>Description</b>           | A description of the module role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Private</b>               | Defines whether the module role is private. If not selected, the module role is created as a public module role.<br><br>A module role with Private enabled can be updated only by a user who is the owner of the role or is listed as the roll administrator. A module role with Private not enabled can be updated by a user with system administrator privileges as well as by the role owner or administrator. A superuser can update any module role, regardless if Private is enabled or not. |
| <b>Protected</b>             | Select to restrict the module role to be used only by applications running on a privileged client.                                                                                                                                                                                                                                                                                                                                                                                                 |

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on creating, viewing, or modifying module roles.

### 13.5.2 Reassigning module roles

If you plan to delete a module role, consider reassigning the users and other objects belonging to the module role. You can reassign the users and other objects.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on reassigning module roles.

### 13.5.3 Deleting module roles

Module roles are a type of group. It is therefore recommended that you do not delete a module role. Instead, remove all members of the module role and leave the module role in the repository. You can also reassign the members of the module role to another module role.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting module roles.

## 13.6 Sessions

A repository session is opened when an end user or application establishes a connection to a server. Each repository session has a unique ID.

During any single API session, an external application can have multiple repository sessions, each with a different repository or server or both.

A repository session is terminated when the end user explicitly disconnects from the repository or the application terminates.

You can use Documentum Administrator to monitor repository sessions only. It cannot monitor any other sessions (for example, eConnector for JDBC sessions).

The Sessions page lists sessions in the current repository. For each session, the name, OpenText Documentum CM Session ID, Database Session ID, Client Host, Start Time, time Last Used, and State are displayed. To view all sessions or user sessions, make a selection from the drop-down list. To view a different number of sessions, select a new number from the **Show Items** drop-down list. To view the next page of sessions, click the > button. To view the previous page of sessions, click the < button. To jump to the first page of sessions, click the << button. To jump to the last page, click>>.

### 13.6.1 Viewing user sessions

You can view user sessions and details of user sessions. User session information that can be viewed includes the root process start time, root process ID, session ID, client library version, and how the user is authenticated.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing user sessions.

### 13.6.2 Viewing user session information

You can view information about user sessions.

**Table 13-11: Session information**

| Field                          | Description                                                                |
|--------------------------------|----------------------------------------------------------------------------|
| <b>Root Process Start Date</b> | The last start date for the server to which the session is connected       |
| <b>Root Process ID</b>         | The process ID of the server on its host                                   |
| <b>User Name</b>               | The session user                                                           |
| <b>Client Host</b>             | The host from which the session is connected                               |
| <b>Session ID</b>              | The ID of the current repository session                                   |
| <b>Database Session ID</b>     | The ID of the current database session                                     |
| <b>Session Process ID</b>      | The operating system ID of the current session process                     |
| <b>Start Time</b>              | The time the session was opened                                            |
| <b>Last Used</b>               | The time of the last activity for the session                              |
| <b>Session Status</b>          | The status of the current session                                          |
| <b>Client Library Version</b>  | The DMCL version in use                                                    |
| <b>User Authentication</b>     | The authentication type                                                    |
| <b>Shutdown Flag</b>           | An internal flag                                                           |
| <b>Client Locale</b>           | The preferred locale for repository sessions started during an API session |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing user session information.

### 13.6.3 Viewing user session logs

You can view user session logs. Session logs provide information about the actions performed in a session.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing user session logs.

#### 13.6.4 Killing user sessions

You can kill user sessions.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on killing user sessions.



# Chapter 14

## Security and authentication

### 14.1 Object permissions

Access to folders and documents in a repository is subject to security restrictions of an organization. All content in the repository is associated with object permissions, which determines the access users have to each object in the repository such as a file, folder, or cabinet and governs their ability to perform specific actions. There are two categories of object permissions:

- Basic: Required for each object in the repository
- Extended: Optional

Basic permissions grant the ability to access and manipulate content of an object. The seven basic permission levels are hierarchical and each higher access level includes the capabilities of the preceding access levels. For example, a user with Relate permission also has Read and Browse.

**Table 14-1: Basic permissions**

| Basic permission | Description                                                                                                                                                                                                                                         |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None             | No access to the object is permitted.                                                                                                                                                                                                               |
| Browse           | Users can view the properties of object but not the content of object.                                                                                                                                                                              |
| Read             | Users can view both the properties and content of the object.                                                                                                                                                                                       |
| Relate           | Users can use the preceding list of permissions and additionally add annotations to the object.                                                                                                                                                     |
| Version          | Users can use the preceding list of permissions. In addition, users can modify the content of object and check in a new version of the item (with a new version number). Users cannot overwrite an existing version or edit the properties of item. |
| Write            | Users can use the preceding list of permissions. In addition, users can edit object properties and check in the object as the same version.                                                                                                         |
| Delete           | Users can use all the preceding list of permissions. In addition, users can delete objects.                                                                                                                                                         |

Extended permissions are optional, grant the ability to perform specific actions against an object, and are assigned in addition to basic permissions. The six levels of extended permissions are not hierarchical, so each must be assigned explicitly. Only system administrators and superusers can grant or modify extended permissions.

**Table 14-2: Extended permissions**

| Extended permission | Description                                                                                                                                                                                                   |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Execute Procedure   | Superusers can change the owner of an item and use Execute Procedure to run external procedures on certain object types. A procedure is a Docbasic program stored in the repository as a dm_procedure object. |
| Change Location     | Users can move an object from one folder to another in the repository. A user also must have Write permission to move the object. To link an object, a user also must have Browse permission.                 |
| Change State        | Users can change the state of an item with a lifecycle applied to it.                                                                                                                                         |
| Change Permission   | Users can modify the basic permissions of an object.                                                                                                                                                          |
| Change Ownership    | Users can change the owner of the object. If the user is not the object owner or a superuser, they also must have Write permission.                                                                           |
| Delete Object       | Users can only delete the object. For example, you may want a user to delete documents but not read them. This is useful for Records Management applications where discrete permissions are common.           |
| Change Folder Links | Users can link or unlink an object to the folder in the repository.                                                                                                                                           |

When a user tries to access an object, Documentum CM Server first determines if the user has the necessary level of basic permissions. If not, extended permissions are ignored.

Permission sets (also known as access control lists, or ACLs) are configurations of basic and extended permissions assigned to objects in the repository that lists users and user groups and the actions they can perform. Each repository object has a permission set that defines the object-level permissions applied to it, including who can access the object. Depending on the permissions, users can create new objects; perform file-management actions such as importing, copying, or linking files; and start processes, such as sending files to workflows.

Each user is assigned a default permission set. When a user creates an object, the repository assigns the default permission set of user to that object. For example, if

the default permission set gives all members of a department Write access and all other users Read access, then those are the access levels assigned to the object.

Users can change access levels of object by changing the permission set of an object. To do this, the user must be the owner of object (typically the owner is the user who created the object) or they must have superuser privileges in the repository of object.

When a user modifies a permission set, it is saved as a permission set assigned to them. They can then apply the permission set to other objects in the repository.

The ability to modify permission sets depends on the user privileges in the repository:

- Users with superuser privileges can modify any permission set in the repository. They can designate any user as the owner of a permission set, and change the owner of a permission set. This permission is usually assigned to the repository administrator.
- Users with system administrator privileges can modify any permission set owned by them or by the repository owner. They can designate themselves or the repository owner as the owner of a permission set they created and can change whether they or the repository owner owns the permission set. This permission is usually assigned to the repository administrator.
- Users with any privileges less than the superuser or system administrator privileges are the owner only of the permission sets they create. They can modify any permission set they own, but cannot change the owner of the permission set.

If you designate the repository owner as the owner of a permission set, that permission set is a System (or Public) permission set. Only a superuser, system administrator, or the repository owner can edit the permission set. If a different user is the owner of the permission set, it is a Regular (or Private) permission set. It can be edited by the owner, a superuser, system administrator, or the repository owner.

A user with Write or Delete permission can change which permission set is assigned to an object.

Security protects the information in each repository using object permissions to control access to cabinets, folders, documents, and other objects. Object permissions determine what actions users can perform on objects. Permissions can be added, removed, modified, or replaced, and set differently for different users.

If you use Documentum Web Publisher and if the user does not assign the default permission set, the Documentum CM Server assigns a default permission set according to the setting in the default\_acl property in the server configuration object.

## 14.2 Changing default operating system permits on public directories and files (Linux only)

On Linux, Documentum CM Server assigns default operating system permissions to newly created files and directories. For example, when Foundation Java API creates directories on the client machines or writes files to directories on the client machines, it assigns default operating system permissions to those directories and files.

Internally, Content Cerver refers to permissions with the symbolic names dmOSFSAP\_Public, dmOSFSAP\_Private, dmOSFSAP\_Public ReadOnly, dmOSFSAP\_PrivateReadOnly, and dmOSFSAP\_PublicOpen. The dmOSFSAP\_PublicOpen permissions assigned to public directories and files can be modified using the umask key in the server.ini file. Setting umask affects all public directories and files created after the key is set. By default the dmOSFSAP\_PublicOpen permissions are 777 for directories and 666 for files.

[“umask” on page 68](#) contains more information on unmask key.

## 14.3 Folder security

Folder security is an additional level of security that supplements the existing repository security. Implementing this security option further restricts allowable operations in a repository. Folder security prevents unauthorized users from adding documents to, removing documents from, or changing contents of secured folders. When folder security is enabled, a user must have Write permission or Change Folder Links permission for the:

- Target folder to create, import, copy, or link an object into the folder.
- Source folder to move or delete an object from a folder.

Folder security only pertains to changing the contents in a folder. For example, a user with Browse permission on a folder can still check out and check in objects within the folder.

If you use Documentum Web Publisher, and if folder security is used in a repository, any content files in the WIP state must have the same permission as the folder. To use the same folder permission, the administrator must make sure that the lifecycle in WIP state does not apply any set ACL action. For example:

```
WIP - folder acl  
Staging - WP "Default Staging ACL"  
Approved - WP "Default Approved ACL"
```

The following table lists the actions affected by folder security:

**Table 14-3: Permissions required under folder security**

| Action                               | Requires at least Write or Change Folder Links permission for:                                    |
|--------------------------------------|---------------------------------------------------------------------------------------------------|
| Create an object                     | Cabinet or folder in which you create the new object                                              |
| Import file(s) or folder             | Cabinet or folder to which you import the file(s) or folder                                       |
| Move an object                       | Both the cabinet or folder from which you remove the object and the destination folder or cabinet |
| Copy an object                       | Destination cabinet or folder                                                                     |
| Link an object                       | Destination cabinet or folder                                                                     |
| Unlink an object                     | Cabinet or folder from which you unlink the object                                                |
| Delete one version of a document     | The primary folder of document                                                                    |
| Delete all versions of a document    | The primary folder of document                                                                    |
| Delete unused versions of a document | The primary folder of document                                                                    |

Consult the repository administrator to determine if folder security is enabled in the repository.

## 14.4 Additional access control entries

When the value of `macl_security_disabled` is set to FALSE, additional access control entries are available. Set up the additional access control entries on the Permissions page under the Security node. The access control entries described in the following table are independent of each other, not hierarchical, and must be explicitly assigned:

**Table 14-4: Additional access control entries**

| Access control entry | Effect of the entry                                                                                                                                                                                                                                                                                                                                            |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Restriction   | An access restriction entry denies a user the right to the base object-level permission level specified in the entry. For example, if a user would otherwise have Delete permission as a member of a particular group, an access restriction might limit the user to, at most, Version permission. The user would therefore lose Write and Delete permissions. |

| Access control entry | Effect of the entry                                                                                                                                                                                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Extended Restriction | An extended restriction entry denies a user or the members of a specified group the specified extended object-level permission. For example, if a user would otherwise have Change Permission rights as a member of a particular group, an extended restriction would remove that right.                 |
| Required Groups      | A required group entry requires a user requesting access to an object governed by the permission set to be a member of the group identified in the entry. If there are entries for multiple groups, the user must be a member of all the groups before Documentum CM Server allows access to the object. |
| Required Group Set   | A required group set entry requires a user requesting access to an object governed by the permission set to be a member of at least one group in the set of groups.                                                                                                                                      |

## 14.5 Default alias sets

The Documentum CM Server adds two default aliases to a permission set:

- *dm\_owner*: Represents the owner of the permission set.
- *dm\_world*: Represents all repository users.



### Notes

- You cannot delete dm\_owner or dm\_world aliases from a permission set.
- dm\_owner and dm\_world are just containers used by server to determine the permissions defined for owners and other users in the repository. This is internal to Foundation Java API and server and any end user application should not use them to set permits for ACLs.

## 14.6 Access evaluation process

When a user who is not the owner of the object or a superuser requests access to an object, Documentum CM Server evaluates the entries in the permission set of the object, as follows:

1. Checks for a basic access permission or extended permission entry that gives the user the requested access level (Browse, Read, Write, and so forth)



**Note:** Users are always granted Read access if the user owns the document, regardless of whether there is an explicit entry granting Read access or not.

2. Checks for no access restriction or extended restriction entries that deny the user access at the requested level.

A restricting entry, if present, can restrict the user specifically or can restrict access for a group to which the user belongs.

3. If there are required group entries, the server checks that the user is a member of each specified group.
4. If there are required group set entries, the server checks that the user is a member of at least one of the groups specified in the set.

If the user has the required permission, with no access restrictions, and is a member of any required groups or groups sets, the user is granted access at the requested level.

When a user is the object owner, Documentum CM Server evaluates the entries in the permission set of object in the following manner:

1. Checks if the owner belongs to any required groups or a required group set.  
If the owner does not belong to the required groups or group set, then the owner is allowed only Read permission as their default base permission, but is not granted any extended permissions.
2. Determines what base and extended permissions are granted to the owner through entries for dm\_owner, the owner specifically (by name), or through group membership.
3. Applies any restricting entries for dm\_owner, the owner specifically (by name), or any groups to which the owner belongs.
4. The result constitutes the base and extended permissions of owner.
  - If there are no restrictions on the base permissions of the owner and the dm\_owner entry does not specify a lower level, the owner has Delete permission by default.
  - If there are restrictions on the base permission of the owner, the owner has the permission level allowed by the restrictions. However, an owner will always have at least Browse permission; they cannot be restricted to None permission.
  - If there are no restrictions on the extended permissions of owner, they have, at minimum, all extended permissions except delete\_object by default. The owner may also have delete\_object if that permission was granted to dm\_owner, the user specifically (by name), or through a group to which the owner belongs.
  - If there are restrictions on the extended permissions of owner, then the extended permissions of owner are those remaining after applying the restrictions.

When Documentum CM Server evaluates the access of superuser to an object, the server does not apply AccessRestriction, ExtendedRestriction, RequiredGroup, or RequiredGroupSet entries to the superuser. A base permission of superuser is

determined by evaluating the AccessPermit entries for the user, for dm\_owner, and for any groups to which the user belongs. The superuser is granted the least restrictive permission among those entries. If that permission is less than Read, it is ignored and the superuser has Read permission by default.

The extended permissions of a superuser are all extended permits other than delete\_object plus any granted to dm\_owner, the superuser by name, or to any groups to which the superuser belongs. This means that the extended permissions of superuser may include delete\_object if that permit is explicitly granted to dm\_owner, the superuser by name, or to groups to which the superuser belongs.

## 14.7 Permission sets

Permission sets are displayed on the Permission Sets page under the **Administration > Security** node. The Permission Sets page displays all permission sets that are configured for the repository.

**Table 14-5: Permissions Sets page**

| Field       | Description                                                                                                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | The object name of the permission set.                                                                                                                                                                                                 |
| Owner       | The user or group that owns the permission set.                                                                                                                                                                                        |
| Class       | Specifies set how the permission set is used: <ul style="list-style-type: none"><li>• <i>Regular</i>: The permission set can only be used by the owner.</li><li>• <i>Public</i>: The permission set can be used by any user.</li></ul> |
| Description | A description of the permission set.                                                                                                                                                                                                   |

## 14.8 Authenticating in domains

For domain authentication on Windows, Documentum CM Server authenticates user names and passwords within a domain. The user domain is stored in the user\_os\_domain property of the user object. A default domain is defined for all users in the repository in the user\_auth\_target key of the server.ini file.

Whether the server uses the user-specific domain or the default domain for authentication depends on whether the server is running in domain-required mode. By default, the Documentum CM Server installation procedure installs a repository in no-domain required mode. If a Windows configuration has only users from one domain accessing the repository, the no-domain required mode is sufficient. If the users accessing the repository are from varied domains, using domain-required mode provides better security for the repository.

### 14.8.1 No-domain required mode

In no-domain required mode, users are not required to enter a domain name when they connect to the repository. In this mode, a user name must be unique among the user\_os\_name values in the repository.

The server authenticates users depending on the user\_os\_domain property value. The property can contain an asterisk (\*), a blank, or a domain name.

- If user\_os\_domain contains an asterisk or blank, Documentum CM Server authenticates the user with the user name and the domain specified in the connection request. If no domain is included in the connection request, the server uses the domain defined in the user\_auth\_target key in the server.ini file.
- If user\_os\_domain contains a domain name, Documentum CM Server authenticates against the domain identified in the user\_os\_domain property.

### 14.8.2 Domain-required mode

In domain-required mode, users must enter a domain name when they connect to the repository. The domain value is defined when the user is created and is stored in the user\_login\_domain property in the user object.

In domain-required mode, the combination of the login name and domain must be unique in the repository. It is possible to have multiple users with the same user login name if each user is in a different domain.

Trusted logins do not require a domain name even if the repository is running in domain-required mode.

## 14.9 Principal authentication

Some applications require authenticating users with external authentication mechanisms that are not accessible to Documentum CM Server. For these cases, Documentum CM Server supports principal authentication and principal mode for privileged Foundation Java API clients (trusted clients). Principal mode is a Foundation Java API mechanism that allows trusted clients to log in to Documentum CM Server without having to go through another password authentication process.

Privileged DFC provides a client rights domain that is implemented using a client rights domain object (dm\_client\_rights\_domain). The client rights domain contains the Documentum CM Servers that share the same set of client rights objects (dm\_client\_rights). The client rights domain is configured in a global repository that acts as a governing repository. Multiple repositories can be grouped together under the global repository to share the Privileged DFC information. The global repository propagates all changes in the client rights objects to the repositories that are members of the domain.

Privileged DFC is configured using the Documentum Administrator interface.

## 14.9.1 Client rights domains

A client rights domain contains the Documentum CM Servers that share the same set of client rights objects. The client rights domain is configured in a global repository that acts as a governing repository. Multiple repositories can be grouped together under the global repository to share the Privileged DFC information.

Privileged DFC is the term used to refer the Foundation Java API instances that can invoke escalated privileges or permissions for a particular operation. For example, privileged DFC can request to use a privileged role for an application to perform an operation that requires higher permissions or a privilege.

A client rights domain is a group of repositories that share the same client rights. The group of repositories in a client rights domain is typically governed by a global repository (global registry). The following rules and restrictions apply to a client rights domain and repository members of that domain:

- A client rights domain can only be configured in a global repository.
- Only a global repository can be a governing repository.
- A global repository can only have one client rights domain.
- A global repository cannot be the governing repository and also a member repository of the client rights domain.
- A repository can only be a member of one client rights domain.
- The global repository must have access to all member repositories in the client rights domain.
- Changes to the client rights in the governing repository are automatically propagated to all member repositories in the same domain.

### 14.9.1.1 Creating a client rights domain

Creating a clients right domain requires superuser privileges and the repository on which you are creating a client rights domain must be a global registry.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on creating a client rights domain.

### 14.9.1.2 Enabling or disabling a client rights domain

Any modifications to a client rights domain require superuser privileges.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on enabling or disabling a client rights domain.

### 14.9.1.3 Deleting a client rights domain

Deleting a clients rights domain requires superuser privileges. Deleting a client rights domain also deletes associated member repository entries.

Deleting a client rights domain automatically starts dm\_PropagateClientRights job, which removes the associated member repository entries. The job execution can take approximately 2 to 4 minutes and until the job has completed successfully, any member repository of the deleted client rights domain cannot be associated with another client rights domain.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting a client rights domain.

### 14.9.1.4 Adding member repositories

Adding a repository to a client rights domain requires superuser privileges.

**Table 14-6: Member repository properties**

| Field                         | Description                                                                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Member Repository Name</b> | The name of the repository. The repository cannot be the governing repository (global registry).                                    |
| <b>Login Name</b>             | The login name of the repository user. The user must have system administrator privileges and be a member of the dm_sysadmin group. |
| <b>Password</b>               | The password of the repository user.                                                                                                |
| <b>User Login Domain</b>      | The name of the login domain for the user. Optional property.                                                                       |
| <b>Application Alias Name</b> | The application name for the Foundation Java API instance. Optional property.                                                       |

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding member repositories.

#### 14.9.1.5 Viewing repository memberships

Viewing a member repository or modifying repository login information in a client rights domain requires superuser privileges.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing repository memberships.

#### 14.9.1.6 Removing a member repository from a client rights domain

Removing a member repository from a client rights domain requires superuser privileges. Removing a member repository also removes the client rights entries from the member repository.

Removing a member repository automatically starts dm\_PropagateClientRights job, which removes the client rights entries from the member repository. The job execution can take approximately 2 to 4 minutes and until the job has completed successfully, the member repository cannot be associated with another client rights domain.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on removing repository memberships.

### 14.10 Privileged clients

Privileged DFC is the term used to refer Foundation Java API instances that are recognized by Documentum CM Servers as privileged to invoke escalated privileges or permissions for a particular operation. In some circumstances, an application needs to perform an operation that requires higher permissions or a privilege than is accorded to the user running the application. In such circumstances, a Privileged DFC can request to use a privileged role to perform the operation. The operation is encapsulated in a privileged module invoked by the Foundation Java API instance. Supporting Privileged DFC is a set of privileged groups, privileged roles, and the ability to define TBOs and simple modules as privileged modules. The privileged groups are groups whose members are granted a particular permission or privileged automatically.

Each installed Foundation Java API has an identity, with a unique identifier extracted from the PKI credentials. The first time an installed Foundation Java API is initialized, it creates its PKI credentials and publishes its identity to the global registry known to the Foundation Java API. In response, a client registration object and a public key certificate object are created in the global registry. The client registration object records the identity of the Foundation Java API instance. The public key certificate object records the certificate used to verify that identity.

In Documentum Administrator, the Privileged DFC clients are managed on the **Privileged Clients** page. To access the **Privileged Clients** page, select **Administration > Client Rights Management > Privileged Clients**.

The **Privileged Clients** page provides the following information:

**Table 14-7: Privileged Clients page information**

| Field                 | Description                                                                                                                                                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Client Name</b>    | The name of the Foundation Java API client.                                                                                                                  |
| <b>Client ID</b>      | A unique identifier for the Foundation Java API client.                                                                                                      |
| <b>Host Name</b>      | The name of the host on which the Foundation Java API client is installed.                                                                                   |
| <b>Approved</b>       | Indicates if the given the Foundation Java API client is approved to perform privilege escalations.                                                          |
| <b>Manage Clients</b> | The Manage Client button displays the <b>Manage Client</b> page, which lists all the Foundation Java API clients that are registered in the global registry. |

### 14.10.1 Adding Privileged DFC clients

The **Manage Clients** page displays the list of the Foundation Java API clients created in the repository. When you select one or more Foundation Java API clients as a **Privileged DFC** client, a Foundation Java API client object is created in the logged in repository and displayed on the **Privileged Clients** page. The public key certificate is copied to the local repository.



#### Notes

- To add a **Privileged DFC** client, you must be logged in as a superuser and you must be the owner of the `dm_acl_superusers` ACL or the install owner.
- If the OpenText Documentum CM Foundation Classes client does not have the global registry information configured, that is valid `dfc.globalregistry.repository`, `dfc.globalregistry.username` and `dfc.globalregistry.password`, then it will not be displayed in the list of OpenText Documentum CM Foundation Classes clients.

**Table 14-8: Manage Clients page information**

| Field                | Description                                                                |
|----------------------|----------------------------------------------------------------------------|
| <b>Client Name</b>   | The name of the Foundation Java API client.                                |
| <b>Client ID</b>     | A unique identifier for the Foundation Java API client.                    |
| <b>Host Name</b>     | The name of the host on which the Foundation Java API client is installed. |
| <b>Creation Date</b> | The creation date of the Foundation Java API client.                       |

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on adding Privileged DFC clients.

## 14.10.2 Configuring privileged client trusted login and trusted server privileges

Privileged Client trusted login and trusted server privileges are configured on the Privileged Client Properties page.

**Table 14-9: Privileged client properties**

| Field                           | Value                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Client Name</b>              | The name of the Foundation Java API client.                                                                                                                                                     |
| <b>Client ID</b>                | The unique identifier for the Foundation Java API client.                                                                                                                                       |
| <b>Host Name</b>                | The name of the host on which the Foundation Java API client is installed.                                                                                                                      |
| <b>Client Privilege</b>         | Indicates whether the Foundation Java API client is approved to perform privilege escalations.                                                                                                  |
| <b>Trusted Login</b>            | Specifies whether the client is allowed to create sessions for users without user credentials.<br><br>Select this option to enable the client to create sessions for users without credentials. |
| <b>Trusted Server Privilege</b> | Specifies whether the Foundation Java API client is part of a trusted Documentum CM Server domain. If this option is enabled, the client has direct access to the repositories on the server.   |
| <b>Is globally managed</b>      | Select to propagate the Privileged DFC information by domain. Optional property.                                                                                                                |
| <b>Application Name</b>         | The application name for the Foundation Java API instance. Optional property.                                                                                                                   |

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on enabling or disabling trusted login and trusted server privileges.

### 14.10.3 Approving or denying privileged clients

Foundation Java API client privilege escalations are approved or denied on the **Privileged Clients** page.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on approving or denying privileged clients.

### 14.10.4 Deleting a Foundation Java API client and certificate

You can delete a Foundation Java API client and the certificate.



**Note:** You cannot delete a certificate that is also used by another Foundation Java API client.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting a Foundation Java API client and certificate.

## 14.11 Administrator access sets

The administrator access functionality enables access to administration nodes based on roles. The nodes, such as Basic Configuration, User Management, Job Management, and Audit Management, provide access to different repository and server functions.

In Documentum Administrator, the administrator access sets are managed on the Administrator Access Sets page. To access the Administrator Access Sets page, select **Administration > Administrator Access**.



**Note:** Administrator Access functionality is available only on OpenText Documentum CM 6 and later repositories.

Administrator access set definitions reside in the global registry. The access sets do not conflict with Documentum CM Server privileges. Object level and user level permissions and permission sets take precedence over administrator access sets. In general, administrator access sets control node access as follows:

- Users are not assigned an administrator access set and do not have superuser privileges, cannot access administration nodes.
- Users who are assigned an administration access set, but do no have superuser privileges, can only access the nodes that are enabled in their administration access set.
- Users with superuser privileges and at least coordinator client capabilities are not affected by administrator access sets. These users always have access to the entire administration node.

- The Groups node is always enabled for users with Create Group privileges.
- The Types node is always enabled for users with Create Type privileges.

The list of available roles is retrieved from the repository to which the administrator is connected. To ensure that administrator access sets function correctly across an application, the roles associated with the administrator access sets must exist in all repositories. If the same role name exists in both the global repository and a non-global repository, the user of the role would see the nodes as per the administrator access specified in the global repository. Even if the user is able to see the nodes, the user can perform operations only with sufficient privileges.



**Note:** The following Administration nodes are currently not available for the administrator access set functionality:

- **Work Queue Management**
- **Distributed Content Configuration**
- **Privileged Clients**

The User Management chapter provides information about setting up roles.

#### 14.11.1 Creating, viewing, or modifying administrator access sets

Only users with superuser privileges and Coordinator client capabilities or greater can create, view, or modify administrator access sets.

**Table 14-10: Administrator access set properties**

| Field       | Value                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name        | Name of the administrator access set. The administrator access set name must be unique. After creating and saving an administrator access set, the name cannot be modified. |
| Description | Description of the administrator access set.                                                                                                                                |

| Field | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nodes | <p>Select one or more node options to designate the nodes that users with this administrator access set can access. At least one node must be selected for an administrator access set. The available node options are:</p> <ul style="list-style-type: none"><li>• Basic Configuration</li><li>• LDAP Server Configuration</li><li>• Java Method Servers</li><li>• User Management</li><li>• Audit Management</li><li>• Jobs and Methods</li><li>• Content Objects</li><li>• Storage Management</li><li>• Content Delivery</li><li>• Index Management</li><li>• Content Intelligence</li><li>• Transformation Services</li><li>• Resource Management</li></ul> |

| Field                | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Assigned Role</b> | <p>Indicates the role assigned to the administrator access set. If the role does not exist in the connected repository, the role is displayed in a red font.</p> <p>To select or modify a role, click <b>Select</b> to select a role on the Choose a role page. The assigned role must be unique for an administrator access set or an error message displays, prompting the user to select a different role.</p> <p>The list of available roles is retrieved from the repository to which the administrator is connected. To ensure that administrator access sets function correctly across an application, the roles associated with the administrator access sets must exist in all repositories. If an assigned role is missing in a connecting repository, the administrator access set does not apply for the missing role. Documentum Administrator displays a message notifying the user when an assigned role is missing.</p> <p>Administrator access sets can be created without assigning a role, and they can contain an inactive or missing role. This is useful during the initial setup of your system.</p> |

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on creating, viewing, or modifying administrator access sets.

### 14.11.2 Deleting administrator access sets

Only users with superuser privileges and Coordinator client capabilities or greater can delete administrator access sets.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on deleting administrator access sets.

## 14.12 Managing authentication plug-ins, signatures, and encryption keys

### 14.12.1 Using authentication plug-ins

Documentum CM Server supports authentication plug-ins that are implemented as DLLs or shared libraries, depending on the operating system hosting the plug-in. You can write and install custom modules.

#### 14.12.1.1 Plug-in scope

You can use a plug-in to authenticate users connecting to a particular repository or to any repository in the installation. All plug-in modules are installed at the root of the base directory or one of the subdirectories. If they are installed at the root of the base directory, they are loaded for all repositories in the installation. If the plug-ins are installed in repository-specific subdirectories, they are only loaded for those specific repositories.

A default %DOCUMENTUM%\dba\auth (\$DOCUMENTUM/dba/auth) base directory is created automatically during Documentum CM Server installation. For every repository, there is a subdirectory under the base directory specific to that repository. There also is a location object, called auth\_plugin, that points to the base directory and sets the auth\_plugin\_location property in the server configuration object to the name of the location object.

When a Documentum CM Server starts, it loads the plug-ins found in its repository-specific directory first and then those located in the base directory. If two or more plug-ins loaded by the server have the same identifier, only the first one loaded is recognized. The remaining plug-ins with the same name are not loaded.

#### 14.12.1.2 Identifying a plug-in

There are two ways to identify an authentication plug-in:

- Include the plug-in identifier in the connection request arguments.
- Set the User Source property of a user account to the plug-in identifier of the module.

When Documentum CM Server receives a connection request, it checks whether a plug-in identifier is included in the arguments. If not, the server examines the User Source property of the user account to determine which authentication mechanism to use.

To use a plug-in to authenticate users for connection requests issued by an application, the application must prepend the plug-in identifier to the password argument before sending the connection request to the DMCL.

When you want to use a plug-in to authenticate a particular user regularly, set the User Source property of that user account to the plug-in identifier.

#### 14.12.1.2.1 Defining a plug-in identifier

Plug-in identifiers are defined as the return value of the dm\_init method in the interface of the plug-in module. A plug-in identifier must conform to the following rules:

- It must be no longer than 16 characters.
- It cannot contain spaces or non-alphanumeric characters.
- It cannot use the prefix dm\_. (This prefix is reserved for OpenText Documentum CM.)

For example, the following are valid identifiers:

- myauthmodule
- authmodule1
- auth4modul

To include a plug-in identifier in a connection request, the application must prepend the following syntax to the password argument:

```
DM_PLUGIN=plugin_identifier/
```

Plug-in identifiers are accepted in all methods that require a password.

#### 14.12.1.3 Implementing a custom authentication plug-in

You can write and install custom authentication plug-ins. On Windows, the plug-in must be a DLL. On Linux, the plug-in must be a shared library.

Authentication plug-ins that require root privileges to authenticate users are not supported. If you want to write a custom authentication mechanism that requires root privileges, use a custom external password checking program.



##### Caution

This section outlines the basic procedure for creating and installing a custom authentication plug-in. OpenText Documentum CM provides standard support for plug-ins that are created and provided with the Documentum CM Server software, as part of the product release. For assistance in creating, implementing, or debugging custom rules, contact OpenText Global Technical Services for service and support options to meet your customization needs.

##### To implement a custom authentication plug-in:

1. Write the plug-in, as described in “[Writing the authentication plug-in](#)” on page 247.
2. Install the plug-in, as described in “[Plug-in scope](#)” on page 245.

3. Enable the plug-in, as described in “[Identifying a plug-in](#)” on page 245.
4. Restart Documentum CM Server to load the new plug-in.

#### 14.12.1.3.1 Writing the authentication plug-in

To write an authentication plug-in, you must implement the following interface:

```
dm_init(void *inPropBag, void *outPropBag)
dm_authenticate_user(void *inPropBag, void *outPropBag)
dm_change_password(void *inPropBag, void *outPropBag)
dm_plugin_version(major, minor)
dm_deinit(void *inPropBag, void *outPropBag)
```

The inPropBag and outPropBag parameters are abstract objects, called property bags, used to pass input and output parameters. The methods have the following functionality:

- dm\_init

The dm\_init method is called by Documentum CM Server when it starts up. The method must return the plug-in identifier for the module. The plug-in identifier should be unique among the modules loaded by a server. If it is not unique, Documentum CM Server uses the first one loaded and logs a warning in the server log file.

- dm\_authenticate

The dm\_authenticate\_user method performs the actual user authentication.

- dm\_change\_password

The dm\_change\_password method changes the password of a user.

- dm\_plugin\_version

The dm\_plugin\_version method identifies the version of the interface. Version 1.0 is the only supported version.

- dm\_deinit

The dm\_deinit method is called by Documentum CM Server when the server shuts down. It frees up resources allocated by the module.

the dmauthplug.h header file contains detailed comments about each of the interface methods. The header file resides in the %DM\_HOME%\install\external\_apps\authplugins\include\dmauthplug.h (\$DM\_HOME/install/external\_apps/authplugins/include/dmauthplug.h) directory. All authentication plug-ins must include this header file.

Additionally, all plug-ins must link to the dmauthplug.lib file in the %DM\_HOME%\install\external\_apps\authplugins\include (\$DM\_HOME/install/external\_apps/authplugins/include) directory.

#### 14.12.1.3.2 Internationalization

An authentication plug-in can use a code page that differs from the Documentum CM Server code page. To enable that, the code page must be passed in the output property bag of the dm\_init method. If the code page is passed, Documentum CM Server translates all parameters in the input property bag from UTF-8 to the specified code page before calling the dm\_authenticate\_user or dm\_change\_password methods. The server also translates back any error messages returned by the plug-in. A list of supported code pages is included in the header file, dmauthplug.h.

#### 14.12.1.4 Tracing authentication plug-in operations

Plug-ins are responsible for writing their own trace files. The trace level is determined by the DM\_TRACE\_LEVEL parameter in the input property bag. The initial value of the parameter is taken from the server start up flag - otrace\_authentication. However, if a user issues a SET\_OPTIONS administration method that changes the trace authentication level, the new level will be reflected in the plug-in tracing.

The suggested location of the trace file is defined by the DM\_LOGDIR\_PATH parameter in the dm\_init method.

### 14.12.2 Implementing signature support

Documentum CM Server provides administration tasks that support using an electronic signature feature in applications. There are three options for electronic signatures:

- Electronic signatures using addESignature

Electronic signatures are implemented through Documentum CM Server and provide rigorous accountability. This option requires OpenText Documentum Content Management (CM) Trusted Content Services. “[Customizing electronic signatures](#)” on page 250 contains the information on using and customizing electronic signature support. Electronic signatures are supported on all supported operating systems.

- Electronic signatures using addDigitalSignature

Electronic signatures are implemented in client applications, using third-party software. “[Supporting electronic signatures](#)” on page 253 contains the instructions on supporting electronic signatures.

- Simple signoffs

Simple signoffs are the least rigorous way to enforce an electronic signature requirement. “[Customizing simple signoffs](#)” on page 254 contains the instructions on using and customizing simple signoffs.

### 14.12.2.1 Using electronic signatures

The default signature template is a form field based PDF template. You must have Adobe Acrobat installed on your system to use this template. Documentum CM Server version 6.6 and later supports publishing only static information on the signature template. Static information, such as a company logo, can be converted to a form field based template using Adobe LiveCycle Designer.

 **Note:** OpenText recommends that you backup any existing custom templates before upgrading to a new template.

**SIGNATURE PAGE**

Document Name :

Document Title :

Document Version :

| Date (GMT)           | Signed by            |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |
| Justification        | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| Justification        | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| Justification        | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| Justification        | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| Justification        | <input type="text"/> |

**Figure 14-1: Signature page**

### 14.12.2.2 Customizing electronic signatures

There are a variety of options for customizing the default signature template for electronic signatures:

- Adding or removing properties from the template page
- Changing the property delimiters on the page
- Changing the look of the template by adding, removing, or rearranging elements on the page or changing the font and point size of the properties
- Defining separate templates for different document types
- Configuring the number of signatures allowed on a version of a document and whether the signature page is added to the front or end of the content.

A signature in non-PDF format requires a custom signature creation method. A custom method can use a custom signature page template, but it is not required. The signature can be in any form that the method implements.

#### 14.12.2.1 Configuring the number of allowed signatures

By default, each signature page can have six signatures. Additional signatures are configured using the esign.signatures.per.page property in the esign.properties file. The esign.properties file resides in the %DM\_JMS\_HOME%\shared\lib\configs.jar directory.

The following table describes configuration parameters in the esign.properties file:

**Table 14-11: Configuration parameters in esign.properties file**

| Property                                | Description                                                                                                                                                            |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| esign.server.language=en                | Indicates the locale of Documentum CM Server.                                                                                                                          |
| esign.server.country=US                 | Indicates the country code.                                                                                                                                            |
| esign.date.format = MM/dd/yyyy HH:mm:ss | Indicates the date format on the signature page. If the date format is not provided in the esign.properties file, the date format of the Documentum CM Server is used. |
| esign.signatures.per.page               | Indicates the number of signatures per signature page.                                                                                                                 |

#### 14.12.2.2.2 Creating custom signature creation methods and associated signature page templates

If you do not want to use the default functionality, you must write a signature creation method. Using a signature page template is optional.

This section outlines the basic procedure for creating and installing a user-defined signature creation method. OpenText Documentum CM provides standard support for the default signature creation method and signature page template installed with the Documentum CM Server software. For assistance in creating, implementing, or debugging a user-defined signature creation method or signature page template, contact OpenText Global Technical Services for service and support options to meet your customization needs.

**To create a custom signature-creation method:**

1. Write the method program.
2. Create a dm\_method object that references the method program.

Use the following guidelines when writing the method:

- The method should check the number of signatures currently defined for the object to ensure that adding another signature does not exceed the maximum number of signatures for the document.
- The method must return 1 if it completes successfully or a number greater than 1 if it fails. The method cannot return 0.
- If the trace parameter is passed to the method as T (TRUE), the method should write trace information to standard output.

To use the custom method, applications must specify the name of the method object that represents the custom method in the addESignature arguments. The following table describes the parameters passed by the addESignature method:

**Table 14-12: Parameters passed by the addESignature method**

| Parameter | Description                                |
|-----------|--------------------------------------------|
| docbase   | Name of the repository.                    |
| user      | Name of the user who is signing.           |
| doc_id    | Object ID of the document.                 |
| file_path | The name and location of the content file. |

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| signature_properties   | <p>A set of property and value pairs that contain data about the current and previous signatures. The information can be used to fill in a signature page. The set includes:</p> <ul style="list-style-type: none"> <li>• sig.requester_0...&lt;n&gt;</li> <li>• sig.no_0...&lt;n&gt;</li> <li>• sig.user_id_0...&lt;n&gt;</li> <li>• sig_user_name_0...&lt;n&gt;</li> <li>• sig.reason_0...&lt;n&gt;</li> <li>• sig.date_0...&lt;n&gt;</li> <li>• sig.utc_date_0...&lt;n&gt;</li> </ul> <p>The number at the end of each parameter corresponds to the number of the signature to which the information applies.</p> |
| application_properties | User-defined set of property names and values specified in the Addsignature command line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| trace                  | If tracing is turned on for SysObjects, this parameter is passed as T (TRUE).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| passThroughArgument1   | User-defined information specified in the addESignature command line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| passThroughArgument2   | User-defined information specified in the addESignature command line.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

If you decide to create a new signature template page, you can define the format, content, and appearance of the page. You can store the template as primary content of an object or as a rendition. For example, you can create an XML source file for your template and generate an HTML rendition that is used by the custom signature creation method. If you store the template as a rendition, set the template page modifier to dm\_sig\_template. Setting the page modifier to dm\_sig\_template ensures that the Rendition Manager administration tool does not remove the template rendition.

#### 14.12.2.3 Publishing dynamic information

Documentum CM Server supports publishing dynamic information on custom signature templates at the page level. The dynamic information is passed through the app\_properties parameter while executing the addESignature method.

Custom field names in custom signature templates must be added with a Ecustf\_ prefix, using the following syntax:

```
'ECustF_Attribute_name1 = ''attr1_value'
```

#### 14.12.2.4 Tracing electronic signature operations

You can trace the addESignature method and the default signature creation method by setting the trace level for the DM\_SYSOBJECT facility to 5 (or higher).

The tracing information for the addESignature and verifyESignature methods is recorded in the session log file. The tracing information for the signature creation method is recorded in the server log file.

If you are using a custom signature creation method, trace messages generated by the method written to standard out are recorded in the server log file if tracing is enabled.



**Note:** When tracing is enabled, the addESignature method passes the trace parameter set to T (TRUE) to the signature creation method.

Set the DM\_DEBUG\_ESIGN\_METHOD environment variable to 1 to log additional information about electronic signatures generated by addESignature to the repository log file. You must restart Documentum CM Server after setting this variable.

#### 14.12.2.5 Setting the Java memory allocation

To avoid performance issues while adding signatures to the document for files greater than 30 MB, it is recommended to increase the JVM memory according to availability. For example, set the value as -Xms1024m -Xmx1024m in the Java Method Server startup file.

#### 14.12.2.3 Supporting electronic signatures

Digital signatures, such as electronic signoffs, are a way to enforce accountability. Digital signatures are obtained using third-party client software and embedded in the content. The signed content is then stored as primary content or a rendition of the document. For example, you can implement digital signing using based on Microsoft Office XP, in which case the signature is typically embedded in the content file and stored in the repository as primary content for the document.

The implementation and management of electronic signatures is almost completely within the context of the client application. The only system administration task is registering the dm\_adddigsig event for signature by Documentum CM Server. This is an optional task. When an application issues the addDigitalSignature

method to record a digital signoff in an audit trail entry, that entry can itself be signed by the Documentum CM Server. To configure signing by the server, an explicit registration must be issued for the dm\_adddigisignature event. “[Audit properties](#)” on page 294 contains the information on how Documentum CM Server signatures on audit entries are implemented and how to configure their use.

#### 14.12.2.4 Regenerating audit signatures

If there is a change in the time zone in the Documentum CM Server host, run the following command to recalculate the audit signature: `apply,c,NULL,REGENERATE_AUDIT_SIGNATURE,FROM_DATE,S,<from_date>,TO_DATE,S,<to_date>,DATE_FORMAT,S,<format>,TRACE,B,<T/F>`



**Note:** The FROM\_DATE, TO\_DATE, and FORMAT commands are mandatory arguments. TRACE is an optional argument with the default value as `<false>`. If enabled, trace messages are written to the repository log. The supported date formats are mentioned in *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)*.

For example:

```
apply,c,NULL,REGENERATE_AUDIT_SIGNATURE,FROM_DATE,S,'03/20/2015',
TO_DATE,S,'04/03/2015',FORMAT,S,'mm/dd/yyyy',TRACE,B,T

apply,c,NULL,REGENERATE_AUDIT_SIGNATURE,FROM_DATE,S,'01/04/2014',
TO_DATE,S,'02/10/2014',FORMAT,S,'mm/dd/yyyy'
```

#### 14.12.2.5 Customizing simple signoffs

Simple signoffs are implemented using a `IDfPersistentObject.signoff` method and a signature validation program. OpenText Documentum CM provides a default signature validation program that authenticates a user based on the user authentication name and password passed as arguments in the signoff method. If the authentication succeeds, Documentum CM Server creates an audit trail entry of event type `dm_signoff` that records what was signed, who signed it, and some information about the context of the signing. The audit trail entry is not signed by Documentum CM Server.

You can customize the simple signoff feature by:

- Creating an alternate validation program that uses the user authentication name and password to validate the user.
- Passing data other than a password through `password` argument of `signoff` and creating a custom validation method to authenticate the user with that data.  
For example, you can pass some biometric data and then validate that using a custom validation program.
- Use an argument in a registration method to force Documentum CM Server to sign the `dm_signoff` events or to add additional information to the entries.



**Note:** OpenText Documentum CM provides standard support for the default signature validation method installed with the Documentum CM Server software. For assistance in creating, implementing, or debugging custom rules, contact OpenText Global Technical Services for service and support options to meet your customization needs.

#### 14.12.2.5.1 Customizing the signature validation program

Use the following procedure to create and implement a customized simple signoff:

**To use a custom signature validation program:**

1. Create a custom signature validation program.

The program must accept two arguments: the user name and the signature data passed using the user-password argument of the signoff method. If the personal data is binary, you can use the uuencode program to convert the data to a string. Data passed in the user-password argument cannot be longer than 127 bytes.

The validation program must return 0 if it succeeds; otherwise, it must return 1.

2. Create a location object that identifies where the program is installed.
3. Modify the signature\_chk\_loc property in the server configuration object to point to the location object created in [step 2](#).

The signature\_chk\_loc property identifies the location of the signature validation program to Documentum CM Server.

#### 14.12.2.5.2 Registering for notification

Users can register the dm\_signoff event so that when the signoff method is executed, the server sends mail notifications to users. You do not need to register a separate audit event, because the server always generates an audit trail for signoff executions.

#### 14.12.2.5.3 Querying the audit trail for signoffs

To return a collection of document objects signed by a specific user within a certain time frame, use the following DQL statement:

```
SELECT "audited_obj_id" FROM "dm_audittrail" WHERE
"event_name" = 'dm_signoff' AND
"user_name" = 'tom' AND
substr ("audited_obj_id", 1, 2) = '09' AND
"time_stamp" >= DATE('01/01/1998', 'dd/mm/yy') AND
"time_stamp" <= DATE(TODAY)
```

To find everyone who signed off a specific object whose ID is xxx, use the following DQL statement:

```
SELECT "user_name" FROM "dm_audittrail" WHERE
"audited_obj_id" = 'xxx' AND
"event_name" = 'dm_signoff'
```

### 14.12.3 Managing encryption keys

Each Documentum CM Server software installation contains one master key, called the Administration Encryption key, or AEK. The AEK is always stored locally in the Documentum CM Server installation.

#### 14.12.3.1 AEK

Starting with the 7.2 release, the creation of AEK is performed during the creation of the repository. Prior to 7.2, there was only one AEK in each Documentum CM Server software installation. It will be created and installed during the Documentum CM Server software installation procedure or when an existing repository was upgraded. The AEK is used to encrypt:

- The repository keys
- OpenText Documentum CM passwords, such as those used by Documentum CM Server to connect to the RDBMS or other repositories

The AEK is itself encrypted using a default passphrase provided by OpenText Documentum CM. You can change the passphrase to a custom passphrase using a utility provided by OpenText Documentum CM. Using a custom passphrase is recommended. [“Using dm\\_crypto\\_change\\_passphrase” on page 265](#), has instructions for changing the passphrase.

The AEK is installed in the following location:

On Windows:

```
%DOCUMENTUM%\dba\secure\aekey
```

On Linux:

```
$DOCUMENTUM/dba/secure/aekey
```

The file is a read only file. The name of the file depends on the `keyname` parameter.

Documentum CM Server and all server processes and jobs that require access to the AEK use the following algorithm to find it:

1. If a location is explicitly passed, look for the AEK in that location.
2. If the AEK is not found in the specified location or a location is not passed, use the location defined in the `DM_CRYPTO_FILE` environment variable.
3. If the `DM_CRYPTO_FILE` environment variable is not defined, assume that the location is `%DOCUMENTUM%\dba\secure\<keyname>` (`$DOCUMENTUM/dba/secure/<keyname>`). If `keyname` is not specified, `aekey` is assumed to be the name of the key.

Starting with the 7.2 release, the creation of AEK can be performed during the creation of the repository. During repository creation or upgrade, option is provided to create or upgrade key or to use existing key.

You can choose to maintain your existing key. If you need to use the AEK key before creating the repository, create a key using the dm\_crypto\_create tool. Starting with the 7.2 release, changing of the AEK is supported.

#### **14.12.3.1.1 Sharing the AEK or passphrase**

If there are multiple OpenText Documentum CM products installed on one host, the products can use different AEKs or the same AEK.

On the same host, all keys have to use the same passphrase. If you want that passphrase to be a custom passphrase, perform the following procedure after you install the Documentum CM Server software:

**To implement the same passphrase for multiple products:**

1. Shut down Documentum CM Server if it is running.
2. Run the dm\_crypto\_change\_password to change the passphrase to a custom passphrase.  
“[Using dm\\_crypto\\_change\\_passphrase](#)” on page 265 contains the instructions.
3. Run the dm\_crypto\_boot utility using the -all argument.  
“[Using dm\\_crypto\\_boot](#)” on page 259 contains the instructions.
4. Restart Documentum CM Server.
5. Install the remaining products on the host machine.

#### **14.12.3.1.2 AEK and distributed sites**

If your repository is a distributed repository, all servers at all sites must be using the same AEK. The installer handles the copying of AEK key.

In multiple-repository distributed sites, you should use the same AEK key.

#### **14.12.3.1.3 Backing up the AEK**

It is strongly recommended that you back up the AEK file separately from the repository and content files. Backing up the AEK and the data it encrypts in different locations helps prevent a dictionary-based attack on the AEK.

### 14.12.3.2 Repository encryption keys

A repository encryption key is created for a repository when the repository is created. The key or its ID is encrypted using the AEK and stored in the `i_crypto_key` property of the repository configuration object. This property cannot be changed after the repository is created.

Documentum CM Server uses the repository encryption key to create the signature on audit trail entries. The server also uses the repository encryption key to encrypt file store keys.

A repository created to use local key management stores the encrypted key in the repository configuration object.

### 14.12.3.3 Encryption utilities

The utilities that are used to manage the AEK are:

- `dm_crypto_boot`

Use this utility if you are protecting the AEK with a custom passphrase. Use it to:

- Install an obfuscated AEK or passphrase in the shared memory of host machine after you define a custom passphrase.
- Reinstall an obfuscated AEK or passphrase in the shared memory of host machine if you stop and restart a server host machine.
- (Windows only) Reinstall an obfuscated AEK or passphrase in the shared memory of host machine if you log off the host machine after you stop Documentum CM Server.
- Clean up the shared memory used to store the obfuscated AEK and passphrase.

It is not necessary to use this utility if you are protecting the AEK with the default, OpenText Documentum CM passphrase. [“Using dm\\_crypto\\_boot” on page 259](#) contains more details and instructions on using the utility.

- `dm_crypto_create`

This utility is run automatically, during the Documentum CM Server installation process, to create and install the AEK. You can use this utility to determine if an AEK exists at a specified location and can be decrypted with a specified passphrase. [“Using dm\\_crypto\\_create” on page 260](#) contains the instructions.

- `dm_encrypt_password`

The `dm_encrypt_password` utility is used for encrypting passwords. [“Using dm\\_encrypt\\_password” on page 261](#) contains the instructions.

- `dm_crypto_change_passphrase`

The `dm_crypto_change_passphrase` utility changes the passphrase used to encrypt an AEK. [“Using dm\\_crypto\\_change\\_passphrase” on page 265](#) contains the instructions.



**Note:** When you run the utilities from command prompt or other Windows utility, make sure that the application is launched as administrator using **Run as Administrator**. If it is not done, Windows restricts the access to the shared memory and other system resources.

#### 14.12.3.4 Using dm\_crypto\_boot

The dm\_crypto\_boot utility obfuscates the AEK or the passphrase used to decrypt the AEK and puts the obfuscated AEK or passphrase in shared memory. The utility is only used when you are protecting the AEK with a custom passphrase. It is not necessary if you are using the default passphrase. If you are protecting the AEK with a custom passphrase, you must run the utility in the following situations:

- When you stop and restart the host machine

After you stop a host machine, run this utility after restarting the host and before restarting the product or products that use the AEK.

- After you install the Documentum CM Server software and before you install the remaining products

You can also use this utility to clean up the shared memory region used to store the AEK.

To run this utility, you must be a member of the dmadmin group and you must have access to the AEK file.

The syntax for the utility is:

```
dm_crypto_boot  
[-keyname <keyname>] [-location <location> | -all]  
[-passphrase <passphrase>] [-remove] [-noprompt]
```

The available arguments are:

- **-passphrase <passphrase>**: The -passphrase argument identifies the passphrase used to encrypt the AEK. If you do not include the argument or if you include the argument keyword but not its value, the utility prompts for the passphrase. If the user is prompted for a passphrase, the passphrase is not displayed on screen when it is typed in.
- **-keyname <keyname>**: This is the name of the key. By default, the name is CSaek.

You must include either the -location or -all argument. Use -location if only one product is accessing the AEK. Using -location installs an obfuscated AEK in shared memory. The -location argument identifies the location of the AEK key. Make sure that you provide the complete path of the file along with the AEK file name when using the -location argument. If you do not include the argument, the utility looks for the location defined in DM\_CRYPTO\_FILE. If that environment variable is not defined, the utility assumes the location %DOCUMENTUM%\dba\secure\aeck.key (Windows) or \$DOCUMENTUM/dba/secure/aeck.key (Linux).

Use the -all argument if there are multiple products on the host machine that use the same passphrase for their AEKs and also to use AES\_256\_CBC algorithm with a custom passphrase. If you include -all, the utility obfuscates the passphrase and writes it into shared memory instead of the AEK. Each product can then obtain the passphrase and use it to decrypt the AEK for their product.

To clean up the shared memory used to store the obfuscated AEK or passphrase, execute the utility with the -remove argument. You must include the -passphrase argument if you use -remove.

The -help argument returns help information for the utility. If you include -help, you cannot include any other arguments.

#### 14.12.3.5 Using dm\_crypto\_create

You can run the dm\_crypto\_create utility with the -check argument to determine whether an AEK exists at a specified location and whether a particular passphrase can be used to decrypt it. Make sure that you follow the password complexity rules while creating a password-based AEK key. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules. The syntax is:

```
dm_crypto_create
[-keyname <keyname>]
[-location <location>]
[-passphrase <passphrase>]
[-remote] [-key_id key_id]
[-noprompt]
[-check]
[-algorithm <algorithm>]
[-dsis_url <DSIS URL>]
[-secret_id <ID of the new password>]
[-dsis_daemon_token <DSIS authentication token>]
[-vault]
[-help]
```

By default, the AEK key is created in %DOCUMENTUM%\dba\secure in Windows and \$DOCUMENTUM/dba/secure in Linux. However, if you want to create the AEK key in a different location, use the -location argument using the dm\_crypto\_create utility. The -location argument identifies the location of the AEK key. Make sure that you provide the complete path of the file along with the AEK file name when using the -location argument. If you do not include the -location argument, the utility looks for the AEK key in the location defined in DM\_CRYPTO\_FILE. If that environment variable is not defined, the utility assumes the location %DOCUMENTUM%\dba\secure\aeck.key (Windows) or \$DOCUMENTUM/dba/secure/aeck.key (Linux).

The available arguments are:

- -keyname <keyname>: This is the name of the key. By default, the name is CSaek.
- -location <location>: This is the location of the administration key file.
- -passphrase <passphrase>: This identifies the passphrase whose use you wish to check. If you do not include the -passphrase argument, the utility assumes the default passphrase but prompts you for confirmation. Consequently, if you are checking the default passphrase and wish to avoid the confirmation request,

include the `-noprompt` argument. The `-passphrase` and `-noprompt` arguments are mutually exclusive.

- Starting with the 7.2 release, the utility is enhanced to provide the option for specifying the algorithm used for generating encryption keys. The following optional argument is introduced:
  - `-check`: If the AEK file exists and decryption succeeds, the utility returns 0. If the AEK file exists but decryption fails, the utility returns 1. If the AEK file is already existing at the specified location, the utility returns 2. If the AEK file does not exist at the specified location, the utility returns 3.
  - `-algorithm <algorithm>`: This option allows to specify the algorithm that has to be used for generating the AEK key. By default, `AES_128_CBC` is used. Valid values are:
    - `AES_128_CBC`
    - `AES_192_CBC`
    - `AES_256_CBC`
  - `-dsis_url <DSIS URL>`: Optional argument (DSIS URL) to be provided to create new AEK key in the Vault-based environment. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.
  - `-secret_id <ID of the new password>`: Optional argument (ID of the new password) to create new AEK key in the Vault-based environment. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.
  - `-dsis_daemon_token <DSIS authentication token>`: Optional argument (for DSIS authentication token) to create new AEK key in the Vault-based environment. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.
  - `-vault`: Optional argument to enable Vault.
  - `-help`: This returns the help information for the utility. If you include `-help`, including any other arguments is not possible.

#### 14.12.3.6 Using dm\_encrypt\_password

Documentum CM Server and many of the internal jobs that manage repository operations use passwords stored in files in the installation. These passwords are stored in encrypted format by default. The passwords are encrypted using the AEK during Documentum CM Server installation or job creation. “[Password files encrypted by default](#)” on page 262, lists the password files whose content is encrypted by default. All the files are found in `%DOCUMENTUM%\dba\config\<repository_name>` (`$DOCUMENTUM/dba/config/<repository_name>`). You must be the installation owner to access or edit these files.

**Table 14-13: Password files encrypted by default**

| <b>File</b>          | <b>Description</b>                                                                                                                                                                                                                                                                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dbpasswd.txt         | This file contains one line with the database password used by Documentum CM Server to connect to the RDBMS. This is password for the repository owner.                                                                                                                                  |
| <docbase_name>.cnt   | The file contains one line with the password used by an object replication job and the distributed operations to connect to the repository as a source or target repository.<br><br>If this file is present, the dm_operator.cnt file is not.                                            |
| dm_operator.cnt      | The file contains one line with the password used by an object replication job and the distributed operations to connect to repositories.<br><br>If this file is present, <docbase_name>.cnt files are not used.                                                                         |
| federation.cnt       | Contains the information, including passwords, used by a governing repository server to connect to member repositories. The file is stored with the governing repository.<br><br>The format of the content of file is:<br><br><member_repository_name>:<user_name>:<password>:[<domain>] |
| ldap_<object_id>.cnt | Contains the password used by Documentum CM Server to bind to an LDAP server.                                                                                                                                                                                                            |

#### 14.12.3.6.1 Using encryptPassword

Use encryptPassword to encrypt any password that you want to pass in encrypted form to the one of the following methods:

- IDfSession.assume
- Authenticate in IDfSessionManager, IDfSession, or IDfClient
- A method to obtain a new or shared session.
- IDfPersistentObject.signoff
- IDfSession.changePpassword

Passwords encrypted with encryptPassword cannot be decrypted explicitly by an application or user. There is no method provided to perform decryption of passwords encrypted with encryptPassword. Foundation Java API decrypts those

passwords internally when it encounters the password in the arguments of one of the preceding methods.

Passwords encrypted with encryptPassword are prefixed with DM\_ENCR\_PASS.

The Javadocs contains more information on using this method.

#### 14.12.3.6.2 Using clear text passwords

If you do not want to use an encrypted password for a particular operation, use a text editor to edit the appropriate file listed in “[Password files encrypted by default](#)” on page 262. Remove the encrypted password and replace it with the clear text password.

#### 14.12.3.6.3 Changing an encrypted password

If you find it necessary to change one of the encrypted passwords described in “[Password files encrypted by default](#)” on page 262, use the dm\_encrypt\_password utility to do so. This utility takes non-encrypted password, encrypts it, and writes it to a specified file. If the file is one of the password files maintained by Documentum CM Server, the utility replaces the current encrypted password in that file with the new password. You must be the repository owner to use this utility.

To encrypt or change a password in a password file maintained by repository, use the following syntax:

For password-based AEK key:

```
dm_encrypt_password
[-location <AEK_location>]
-keyname <keyname>
[-passphrase <passphrase>]
-docbase <repository name>
-remote <remote repository name>
-operator
-rdbms
-encrypt <password>
```

To create or change an encrypted password in a file that you have created, use the following syntax:

For password-based AEK key:

```
dm_encrypt_password
[-location <AEK_location>]
-keyname <keyname>
[-passphrase <passphrase>]
-file <file_name>
-encrypt <password>
```

The arguments have the following definitions:

| Argument           | Description                    |
|--------------------|--------------------------------|
| -keyname <keyname> | Specifies the name of AEK key. |

| Argument                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -location <AEK_location>         | Identifies the location of the AEK file to be used to encrypt the password. If this argument is not set, the environment variable DM_CRYPTO_FILE must be set.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| -passphrase <passphrase>         | <p>Specifies the passphrase used to protect the AEK file.</p> <p>If the argument is included without a passphrase, the utility prompts for a passphrase.</p> <p>If the argument is not included, the utility attempts to use the default passphrase. (The default passphrase can be defined when the dm_crypto_boot utility is run to set up the AEK.)</p> <p>If a default passphrase is not defined, the utility checks the shared memory location, based on the location argument or the default location, for an AEK or passphrase. If neither is found in shared memory, the utility exits with an error.</p> |
| -file <file_name>                | <p>Identifies the file on which to operate.</p> <p>Do not include this argument if you include the -docbase argument.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| -encrypt <password>              | Defines the password to encrypt. If specified, the password is encrypted and written to the file identified in the -file argument. If unspecified, the utility encrypts the first line found in the file and writes it back to the file.                                                                                                                                                                                                                                                                                                                                                                          |
| -docbase <repository name>       | <p>Identifies the repository for which the password is being encrypted.</p> <p>Do not include this argument if you include the -file argument.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| -remote <remote repository name> | <p>Identifies the file to operate on as %DOCUMENTUM%\dba\config\&lt;repository_name&gt;\&lt;remote_repository_name&gt;</p> <p>You must include the -docbase argument if you include -remote.</p>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| -operator                        | <p>Identifies the file to operate on as %DOCUMENTUM%\dba\config\&lt;repository_name&gt;\dm_operator.cnt</p> <p>You must include the -docbase argument if you include -operator.</p>                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Argument | Description                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -rdbms   | Identifies the file to operate on as %DOCUMENTUM%\dba\config\<repository_name>\dbpasswd.txt<br><br>You must include the -docbase argument if you include -rdbms. |

For example, executing the utility with the following command line replaces the database password used by the Documentum CM Server in the engineering repository to connect with the RDBMS:

```
dm_encrypt_password keyname CSAek -docbase engineering -passphrase jdoe -rdbms
                     -encrypt 2003password
```

The AEK location is not identified, so the utility reads the location from the DM\_CRYPTO\_FILE environment variable. The passphrase jdoe is used to decrypt the AEK. The utility encrypts the password 2003password and replaces the current RDBMS password in dbpasswd.txt with the newly encrypted password.

This example identifies a user-defined file as the target of the operation.

```
dm_encrypt_password keyname CSAek -passphrase jdoe
                     -file C:\engineering\specification.enc -encrypt devpass
```

The AEK location is not identified, so the utility reads the location from the DM\_CRYPTO\_FILE environment variable. The password jdoe is used to decrypt the AEK. The utility encrypts the password devpass and writes the encrypted value to the file C:\engineering\specification.enc.

#### 14.12.3.7 Using dm\_crypto\_change\_passphrase

Use dm\_crypto\_change\_passphrase to change the passphrase used to encrypt the AEK in the installation. Installing the Documentum CM Server software installs the AEK encrypted using a default passphrase. Use this utility, also, if business rules or a security breach require you to change the passphrase. All OpenText Documentum CM products that use the affected AEK must be stopped before running the utility.



**Note:** This utility must be used only for the password-based AEK key. Make sure that you follow the password complexity rules for new passphrases. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

The syntax is:

```
dm_crypto_change_passphrase [-keyname <keyname>] [-location <location>]
                            -passphrase <old_passphrase>
                            -newpassphrase <new_passphrase> //use only in an environment where Vault is not enabled
                            -dsis_url <DSIS URL> //optional argument to be provided to move the existing AEK key to the Vault-based environment (see OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD))
                            -dsis_daemon_token <DSIS authentication token> //optional argument to be provided to move the existing AEK key to the Vault-based environment (see OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD))
```

```
-secret_id <ID of the new password> //optional argument to be provided to move the
existing AEK key to the Vault-based environment (see OpenText Documentum Content
Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD))
[-noprompt][-help]
```

For more information about enabling Vault, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

The -location argument identifies the location of the AEK whose passphrase you wish to change. If you do not include the argument, the utility looks for location defined in DM\_CRYPTO\_FILE. If that environment variable is not defined, the utility assumes the location %DOCUMENTUM%\dba\secure\aekey (Windows) or \$DOCUMENTUM/dba/secure/aekey (Linux).

The -passphrase argument identifies the current passphrase associated with the AEK. The -newpassphrase argument defines the new passphrase you wish to use to encrypt the AEK. Both phrases interact in a similar manner with the -noprompt argument. The behavior is described in “[Interaction of dm\\_crypto\\_change\\_passphrase arguments](#)” on page 266.

**Table 14-14: Interaction of dm\_crypto\_change\_passphrase arguments**

|                                                        | <b>-noprompt included</b>                                     | <b>-noprompt not included</b>                                                               |
|--------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <i>-passphrase argument not included</i>               | Utility assumes the OpenText Documentum CM default passphrase | Utility assumes the OpenText Documentum CM default passphrase                               |
| <i>-passphrase keyword is included but no value</i>    | Utility assumes the OpenText Documentum CM default passphrase | Utility assumes the OpenText Documentum CM default passphrase                               |
| <i>-newpassphrase argument not included</i>            | Utility assumes the OpenText Documentum CM default passphrase | Utility assumes the OpenText Documentum CM default passphrase, but prompts for confirmation |
| <i>-newpassphrase keyword is included but no value</i> | This combination is not supported                             | Utility prompts for a new passphrase                                                        |

You must include a value for at least one of the passphrases. You cannot be prompted for both values or allow both values to default.

To illustrate the use of this utility, here are some examples.

The command in the following example changes the passphrase for the Documentum CM Server host AEK from the default to custom\_pass1. The -passphrase argument is not included and the -noprompt is included, so the utility assumes that the current passphrase is the default passphrase.

**Example:**

```
dm_crypto_change_passphrase -location %DOCUMENTUM%\dba\secure\aekey
-newpassphrase custom_pass1 -noprompt
```

The command in the following example changes the passphrase from one custom passphrase to another:

**Example:**

```
dm_crypto_change_passphrase -location %DOCUMENTUM%\dba\secure\aekey  
-passphrase genuine -newpassphrase glorious
```

The command in the following example changes the passphrase from a custom passphrase to the default passphrase:

**Example:**

```
dm_crypto_change_passphrase -location %DOCUMENTUM%\dba\secure\aekey  
-passphrase custom_pass1 -noprompt
```

The new passphrase is set to the default passphrase. It is not necessary to include the -newpassphrase argument. The utility assumes that the new passphrase is the default if the argument is not present and the -noprompt argument is present.

The command in the following example moves the password of the password-based AEK key to the Vault-based environment. You must move the new AEK password to the Vault-based environment before running the command.

**Example:**

```
dm_crypto_change_passphrase -keyname CSaek -passphrase Password@1234567  
-dsis_url http://localhost:8200/dsis  
-dsis_daemon_token 8780392627541981234  
-secret_id AEK_PASSWORD/CSaek
```

The -help argument returns help information for the utility. If you include -help, you cannot include any other arguments.

## 14.12.4 Managing the login ticket key

The login ticket key is used to generate and validate login tickets and application access control tokens. The key is installed automatically when a repository is created. Each repository has one login ticket key.

A repository created to use local key management stores the encrypted login ticket key in the repository. There is no difference using the EXPORT\_TICKET\_KEY, IMPORT\_TICKET\_KEY, and RESET\_TICKET\_KEY methods for either type of repository.

#### 14.12.4.1 Exporting and importing a login ticket key

If you are using global login tickets or global application access control tokens, both the repository generating the ticket or token and the repository accepting the ticket or token must be using the same login ticket key. When you install a repository, the installation configures a login ticket key for the repository. However, each key is unique. Consequently, to use global login tickets or tokens, you must export a login ticket key from one repository among those that will be exchanging global login tickets or tokens and import that key into the other repositories exchanging global tickets or tokens.

To export a login ticket key, use the EXPORT\_TICKET\_KEY administration method, as described in ["EXPORT\\_TICKET\\_KEY" on page 332](#). To import the key, use IMPORT\_TICKET\_KEY, as described in ["IMPORT\\_TICKET\\_KEY" on page 332](#). These methods are also available as Foundation Java API methods (exportTicketKey and importTicketKey) in the IDfSession interface.

You must restart Documentum CM Server after importing a login ticket key to make the new login ticket key take effect.

#### 14.12.4.2 Resetting a login ticket key

Resetting a login ticket key replaces the current login ticket key with a newly generated key. You need to reset a login ticket key if the current key is compromised. If you reset the login ticket key, the server of repository does not accept any login tickets generated using the old key.

To reset a login ticket key, execute the RESET\_TICKET\_KEY method. You can also use the Foundation Java API method, resetTicketKey, in the IDfSession interface.

You must restart Documentum CM Server after resetting a login ticket key.

### 14.12.5 Configuring application access control token use

Application access control (AAC) tokens are a security feature that you can use to control access to a repository based on who is requesting access, the application or host from which the request is issued, or some combination of these factors.

AAC tokens are enabled at the server level, to give you flexibility in designing your security. For example, you can set up a server that requires a token to service users outside a firewall and another server that does not require a token for users inside the firewall.

Tokens are used in addition to user names and passwords (or login tickets) when issuing a connection request. They are not a substitute for either. If a server requires a token and the user making the connection request is not a Superuser, the connection request must be accompanied by a token. Only Superusers can connect to a repository through a server requiring a token without a token.

*OpenText Documentum Content Management - Server Fundamentals Guide* (EDCCS250400-GGD) contains complete information about tokens and how they are implemented and used.

### **14.12.5.1 Enabling AAC token use by a server**

Use Documentum Administrator to enable the use of application access control tokens by a particular server. If use is enabled, non-Superuser users cannot access the repository through that server unless the constraints specified in the token are satisfied. Whether a server has AAC token use enabled is recorded in the application\_access\_control property of its server config object.

#### **14.12.5.1.1 Enabling machine-only AAC tokens**

An application access control token can be created to be valid only when sent from a particular host machine. This token authentication mechanism is dependent on knowledge of the machine ID of host. If you are using such tokens, you must set the dfc.machine.id key in the dfc.properties file used by client applications on that host so that Foundation Java API can include that when sending the application token to Documentum CM Server. Set the key to the machine ID of host.

### **14.12.5.2 Enabling token retrieval by the client library**

You can configure client library behavior to allow the client library to automatically retrieve a token from storage and append that token to connection request of an application if a token is required and none is provided in the connection request. If retrieval is enabled, the client library searches for a token file whose name matches the name of the repository specified in the connection request. If such a token file is found, the token it contains is appended to the connection request. If such a token file is not found, the client library appends the token from the token file named default.tkn, if one is available.

This feature helps ensure that the appropriate token is provided when an application is run from different machines and that older applications can connect to a server that requires an AAC token for connection.

#### **To enable token retrieval:**

1. Generate the token files using dmtkgen.  
For instructions on using the utility, refer to “[Generating tokens for storage](#)” on page 270.
2. Configure the retrieval behavior in the dfc.properties file.
  - a. Set dfc.tokenstorage.enable to true.
  - b. Set dfc.tokenstorage.dir to the desired token storage directory.

The dfc.tokenstorage.enable key is a Boolean key that controls whether the client library can retrieve tokens from storage. If it is set to true, the client library will attempt to retrieve a token from storage for use when a connect request without a

token is issued to a server requiring a token. If the key is set to false, the client library does not retrieve tokens from storage.

The dfc.tokenstorage.dir key tells the client library where to find the token files generated by the dmtkgen utility. Any tokens that you generate using dmtkgen must be placed in this location. If they are not, the client library will not find them.

When you install Foundation Java API on a client host machine for the first time, the installation sets the dfc.tokenstorage.enable key to false and the dfc.tokenstorage.dir to <user-selected drive>:\Documentum\apptoken. If you upgrade or reinstall Foundation Java API, the procedure will not reset those keys if you have changed them.

When you install Documentum CM Server for the first time on a host machine, the process also installs Foundation Java API. The Foundation Java API installation process sets the dfc.tokenstorage.enable key in the dfc.properties file on the server host to false and the dfc.tokenstorage.dir to %Documentum%\apptoken (\$DOCUMENTUM/apptoken). However, when the Documentum CM Server installer runs, it resets the tdfc.tokenstorage.enable key to true. The dfc.tokenstorage.dir is not reset.

The dfc.properties file on the server host is used by the internal methods to connect to repositories. The dfc.tokenstorage.enable and dfc.tokenstorage.dir settings in this dfc.properties file affect methods associated with dm\_method objects. Replication and federation methods are not affected by the settings in this dfc.properties file because these jobs execute as a Superuser.



**Note:** *OpenText Documentum Content Management - Server Fundamentals Guide (EDCCS250400-GGD)* contains the additional information about how internal methods are affected by this setting.

If you are installing an upgrade to Documentum CM Server or a previous Foundation Java API installation occurred and a dfc.properties file already exists on the host machine with these keys set, installing Documentum CM Server and a new Foundation Java API does not overwrite their values.

#### 14.12.5.3 Generating tokens for storage

Use the dmtkgen utility to generate application access control tokens to be stored on host machines. The utility is found in %DM\_HOME%\bin (\$DM\_HOME/bin). Each execution of the utility creates one token file in XML format. The file is an ASCII file. The file contains the token and the information used to generate the token. Here is a sample of the file format:

```
<token>
<docbase>mytestdb</docbase>
<user>me</user>
<scope>global</scope>
<timeout>40000</timeout>
<appidhash>hash_of_application_id</appidhash>
<machineonly>T</machineonly>
<tokendata>DM_TOKEN=tokenstring</tokendata>
</token>
```

“[dmtkgen utility arguments](#)” on page 271, lists the arguments accepted by this utility.

**Table 14-15: dmtkgen utility arguments**

Argument	Description
<code>-u username</code>	User as whom the utility is running This is a required argument.
<code>-p password</code>	Password for the user identified in <i>username</i> This is a required argument.
<code>-d domain</code>	Domain of the user identified in <i>username</i> This argument is required only if a domain is required to authenticate the user.
<code>-b repository_name</code>	Name of the repository to which to connect to create the token. This is a required argument.
<code>-a user group name</code>	Name of the user or group who can use this token. If a group is specified, all members of the group can use this token. This is an optional argument. If unspecified, then all users can use the token.
<code>-s scope</code>	Scope of the generated token. Valid values are <ul style="list-style-type: none"> <li>• docbase Specifying docbase restricts the use of token to the repository identified in the output name of the file.</li> <li>• global Specifying global allows the token to be used to connect to any repository having the same login ticket key as the repository in which the token was generated.</li> </ul> This is an optional argument. The default is global.
<code>-t timeout</code>	Validity period for the generated token. The value is interpreted in minutes. This is an optional argument. The default is one year, expressed in minutes.

Argument	Description
<code>-i application_identifier</code>	<p>User-defined application identifier representing the application for which this token is valid.</p> <p>This is an optional argument. If unspecified, the token is valid for all applications.</p>
<code>-m machine_only</code>	<p>Boolean flag indicating whether the token is valid only when used on the machine on which the token was generated. T means the token may only be used from the machine on which it was generated. F means that the token may be sent from any machine.</p> <p>This is an optional argument. The default is F.</p>
<code>-o output_file</code>	<p>The name of the generated XML token file. You can specify a full file path or only the file name.</p> <p>The file name must be either:</p> <p><code>default.tkn</code></p> <p>or</p> <p><code>repository_name.tkn</code></p> <p>This is an optional argument. It defaults to <code>repository_name.tkn</code> where <code>repository_name</code> is the repository identified in the <code>-b</code> argument. If you include a name but not a file path, the file is stored in the current directory.</p> <p>The implementation imposes a naming constraint on global tokens. Refer to <a href="#">“Naming the output file” on page 272</a>, for information.</p>

#### 14.12.5.3.1 Naming the output file

Token files are retrieved by repository name. If the client library is looking for a token in storage for a particular connection request, it searches for a token whose name is the name of the requested repository in the connection request. If the library cannot find a token whose name matches the repository name in the connection request, it searches for a token file called `default.tkn`. Because of this token file search algorithm, if you create a global token file for use across multiple repositories, you must name the file `default.tkn`.

#### 14.12.5.4 Storing tokens generated by dmtkgen

The client library looks for the stored tokens in the location identified by the `dfc.tokenstorage.dir` key in the `dfc.properties` file of client. After you generate the token file, you can copy the file to that location for each client machine where the token will be used. Because the generated file is an ASCII file, you can copy the file across operating systems. For example, if it was generated on a Windows host machine, you can copy it to a UNIX host machine. Similarly, if it was generated on a UNIX host machine, you can copy it to a Windows host machine.

If the location specified in `dfc.tokenstorage.dir` is visible to the machine on which you generate the token, you can specify the location in the `-o` argument and the token file will be saved to the correct location automatically.

The `dfc.tokenstorage.dir` key is set automatically when the Foundation Java API is installed. For more information about its setting, refer to “[Enabling token retrieval by the client library](#)” on page 269.

## 14.13 Configuring two-man oversite

The two-man oversite feature provides the capability of sending notifications to a set of users for all the default critical events that occurs in Documentum CM Server. Users with extended privileges only can add other users to the `dm_critical_event_receiver_role` role and manage the user list. All users that are added to the `dm_critical_event_receiver_role` role receive notifications without any exceptions.

Documentum CM Server creates an inbox item with details such as name of the event, time of occurrence, user, message, and so on that you can view in `Inbox` of Documentum Administrator.

To enable the two-man oversite feature, set the value of `TWO_MAN_OVERSITE_FEATURE_FLAG` (`r_module_name`) to 1.

During the Documentum CM Server installation, a set of default critical events are registered automatically with an empty `dm_critical_event_receiver_role` role. The following events are added to the list of critical events at the time of Documentum CM Server installation:

- `dm_critical_event_reciever_role`: `dm_save` for `dm_group` only for this role
- `dm_audit`
- `dm_purgeaudit`
- `dm_unaudit`
- `dm_save`: `dm_user`,  
`dm_acl`, `dm_scope_config`, `dm_display_config`, `dm_docbase_config`, `dm_server_config`, `dm_cache_config`, `dmc_mq_config`, `dm_sysprocess_config`, `dm_jms_config`
- `dm_destroy`: `dm_user`, `dm_acl`, `dm_scope_config`, `dm_display_config`,  
`dm_docbase_config`, `dm_server_config`, `dm_cache_config`, `dmc_mq_config`,  
`dm_sysprocess_config`, `dm_jms_config`

- dm\_kill

The `dm_critical_event_receiver_role` role is governed using the `DM_PRIV_CONFIG_CRITICAL_EVENT` environment variable with a value set to 1.

The *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* contains information about the privileges and the values added for the `user_xprivileges` user type property.

# Chapter 15

## Logging and tracing

### 15.1 Introduction

OpenText Documentum CM supports tracing and logging facilities for both Documentum CM Server and Foundation Java API operations. The logging facilities record information generated automatically by Documentum CM Server or Foundation Java API, including error, warning, and informational messages. Logging errors, warnings, and informational messages occurs automatically.

The tracing facility records information that is explicitly requested by user or an application. Enabling or disabling tracing requires system administrator or superuser privileges.

### 15.2 Documentum CM Server logging and tracing

Documentum CM Server logging and tracing provides information about Documentum CM Server operations. Documentum CM Server records logging information and tracing information, with a few exceptions, in the following files:

- Repository log file

Contains information about root server activities. This file is also sometimes referred as the Documentum CM Server log file.

- Session log files

Contains all informational, warning, error, and fatal error messages and, by default, all SQL commands generated from DQL commands.

Session log files are stored in the %DOCUMENTUM%\dba\log  
\\<hex\_repository\_id>\<username> (\$DOCUMENTUM/dba/log/  
<hex\_repository\_id>/<username>) directory, where <hex\_repository\_id> is the repository ID expressed as a hexadecimal value and <username> is the account under which the session is running. The session log name is the session ID. The server creates a separate session log for each new connection.

Sessions that are connected to the primary Documentum CM Server create their session logs under the primary server and sessions that are connected to one or more remote Content Server create their session logs under the remote server(s). Because sessions are assigned using a round-robin method, look in both places for session logs.

Some features, such as jobs, record tracing and logging information in log files specific to those features. The sections that describes those features contain more details about the associated log files.

### 15.2.1 Tracing from the startup command line

A variety of tracing operations can be initiated from the Documentum CM Server startup command line. To start tracing at server start-up, specify the trace flags for the options with the -o option on the command line. The name of the option must immediately follow the -o. No space is allowed between the -o and the option name. On Windows, add the -o option to the command line by editing the Documentum CM Server service entry.

The following table describes the trace flags for the -o option at server start-up:

**Table 15-1: Server start-up trace options**

Option name	Description
crypto_trace	Cryptography information.
debug	Session shutdown, change check, launch and fork information.
docbroker_trace	Connection broker information.
i18n_trace	Session locale and client code page usage.
lock_trace	Windows locking information.
net_ip_addr	IP addresses of client and server for authentication.
nettrace	Turns on RPC tracing (traces Netwise calls, SSL, connection ID, client host address, and client host name).
ossl_trace	SSL communication information.
rptctrace	Turns on tracing of RPC calls.
sqltrace	SQL commands sent to the underlying RDBMS for subsequent sessions, including the repository session ID and the database connection ID for each SQL statement.  This option is turned on by default when a server starts.
ticket_trace	Traces import and export operations for login ticket keys and operations using single-use login tickets.
trace_authentication	Detailed authentication information.
trace_complete_launch	Linux process launch information.
trace_workflow_agent	Trace messages generated by the workflow agent.

The generated trace information is recorded in the repository log file.

To stop tracing from the command line, you must remove the trace flag from the server command line and then stop and restart the server.

## 15.2.2 Using the `setServerTraceLevel` method

The `setServerTraceLevel` method is defined for the Foundation Java API `IDfSession` interface. The method takes two arguments, a trace level, defined as an integer value, and a facility name. The following table describes the trace levels for the `setServerTraceLevel` method:

**Table 15-2: Trace level severity values**

Severity level	Meaning
0	No messages, tracing is turned off. Use this value to turn off tracing for the specified facility.
1	Level 1 trace messages
2	Level 2 trace messages
3	Level 3 trace messages
4	Level 4 trace messages
8	Dump and load object information
10	Timing information

The severity levels are additive. For example, if you specify tracing level 10, you also receive all the other messages specified by the lower levels in addition to the timing information.



**Note:** The severity levels are also applicable for `-Ftrace_level` and `-Ltrace_level` arguments.

The following table describes the facilities for the `setServerTraceLevel` method:

**Table 15-3: Valid facilities for `setServerTraceLevel`**

Facility	Description
ALL	Traces all available trace facilities.
DM_CONTENT	Traces content operations. The information is recorded in the session log file.
DM_DUMP	Traces dump operations. The information is recorded in the session log file.
DM_LOAD	Traces load operations. The information is recorded in the session log file.

Facility	Description
DM_QUERY	Traces query operations. The information is recorded in the session log file.
SQL_TRACE	Traces generated SQL statements. The information is recorded in the session log file.  Tracing for this facility is turned on by default. Turning it off is not recommended by OpenText Global Technical Services.
DM_SYSOBJECT	Traces SysObject operations. The information is recorded in the session log file.

### 15.2.3 Using the SET\_OPTIONS method

The SET\_OPTIONS administration method controls wide range of Documentum CM Server tracing options, including tracing Centera and NetApp SnapLock storage area operations, digital shredding operations, and connection broker information. [“SET\\_OPTIONS” on page 347](#) contains a complete list of the trace options for the SET\_OPTIONS method.

The method can be executed from Documentum Administrator or using the DQL EXECUTE statement or an IDfSession.apply method.

Turning tracing on and off using SET\_OPTIONS affects only new sessions. Current sessions are not affected.

### 15.2.4 Examples of server tracing

The following example describes a section from the server log for DM\_LOAD tracing:

```
Fri Aug 14 16:02:27 1998 569000 [DM_LOAD_I_PROGRESS]info:  
"For load object 310007b680000101 in phase 2, processed 54 of 66 objects;  
last object processed was 090007b680000238"  
Fri Aug 14 16:02:27 1998 710000 [DM_LOAD_I_PROGRESS]info:  
"For load object 310007b680000101 in phase 2, processed 55 of 66 objects;  
last object processed was 060007b680000118"  
Fri Aug 14 16:02:27 1998 720000 [DM_LOAD_I_PROGRESS]info:  
"For load object 310007b680000101 in phase 2, processed 56 of 66 objects;  
last object processed was 270007b680000165"
```

The following example describes a log file section for query tracing. The example assumes that the following query is issued:

```
SELECT "user_os_name" FROM "dm_user" WHERE "user_name"='zhan'
```

The corresponding server log:

```
Fri Aug 14 15:31:29 1998 608000 [DM_QUERY_T_SELECT_COMPLETE]info:  
"SELECT statement semantic checking and setup is complete."  
Fri Aug 14 15:32:20 1998 942000 [DM_QUERY_T_SYNTAX_BEGIN]info:  
"Begin syntactic parse (call yacc)."  
Fri Aug 14 15:32:20 1998 942000 [DM_QUERY_T_SYNTAX_COMPLETE]info:
```

```
"Syntactic parse is complete."
Fri Aug 14 15:32:20 1998 942000 [DM_QUERY_T_SELECT_BEGIN]info:
"Begin SELECT statement."
Fri Aug 14 15:32:20 1998 942000 [DM_QUERY_T_SQL_SELECT]info:
"SELECT statement generated by the query is:
select all dm_user.user_os_name from dm_user_sp dm_user where
(dm_user.user_name='zhan').
Begin Database processing."
Fri Aug 14 15:32:22 1998 434000 [DM_QUERY_T_SELECT_COMPLETE]info:
"SELECT statement semantic checking and setup is complete."
```

### 15.2.5 Determining active tracing options

To determine whether a particular Documentum CM Server tracing option is enabled, use an `IDfSession.isServerTraceOptionSet` method with the name of the option as the method argument. For example, to determine if the `docbroker_trace` tracing option is enabled, specify the option name as the method argument.

You cannot specify a facility name with the `isServerTraceOptionSet` method.

## 15.3 Foundation Java API logging

Foundation Java API logging and the location of the log file is controlled by the `log4j2.properties` file. The default location is  `${user.dir}/documentum/logs/documentum.log`.

The standard Java documentation contains the information on the configurable logging options.

To record debug information generated by specific packages or classes, OpenText recommends you to use the Foundation Java API trace file, rather than the `log4j` log file, as described in “[Directing categories to the trace file](#)” on page 287.

## 15.4 Foundation Java API tracing

Foundation Java API supports a set of tracing configuration options for the Foundation Java API operations, such as tracing for individual users, individual threads, and methods. The trace file format can be configured as well, such as timestamps within the file and how to record method entrances and exits.

All Foundation Java API tracing is configured in the `dfc.properties` file. The entries are dynamic. Adding, removing, or changing a tracing key entry is effective immediately without having to stop and restart Foundation Java API or the application.

### 15.4.1 Enabling Foundation Java API tracing

Foundation Java API tracing options are configured in the dfc.properties file.

#### To enable Foundation Java API tracing:

1. Open the dfc.properties file in a text editor.
2. Modify the tracing properties by changing the key values, as desired.
3. Change the dfc.tracing.enable key to true to start tracing:

```
dfc.tracing.enable=true
```

Trace log file names have the following format:

```
<file_prefix>[.<identifier>].<timestamp>.log
```

Where file\_prefix is a string that is prepended to the beginning of the name of each trace file generated by Foundation Java API and timestamp records when the file was created. An identifier is included in the file name only if you are generating log files for individual users or threads. The identifier is the user name, if the logs are generated for individual users or the thread name, if logs are generated for individual threads.

Enabling tracing creates a logger and a logging appender that record the entries in the trace log file. The logging appender determines the name, location, and format of the trace file. “[Logging appender options](#)” on page 280 contains more information.

### 15.4.2 Logging appender options

The logging appender controls various trace file options, such as the name, location, and format of the trace file. The following table describes the appender options:

**Table 15-4: Logging appender configuration options**

Key	Option	Description
dfc.tracing.date_format	Date format for timestamp	Defines a date format if dfc.tracing.timing_style, in dfc.properties, is set to date. <a href="#">“Defining the trace file timestamp format” on page 282</a> contains more information.
dfc.tracing.dir	Location of file	The directory where the trace file is stored. The default location is \${dfc.data.dir}/logs. Valid values for this property are any valid directory path.

Key	Option	Description
dfc.tracing.file_creation_mode	Creation mode	Controls whether trace information is logged in one file or multiple files. “Defining file creation mode” on page 281 contains more information.
dfc.tracing.file_prefix	File name prefix	Defines the base name of the trace file. The default value is dfctrace.
dfc.tracing.max_backup_index	Maximum number of backups for the file	A positive integer value that defines the number of backup files the logger retains for the log file. When the maximum number is reached, the oldest backup is destroyed when a new backup is created.  The default value is 1.
dfc.tracing.max_file_size	Maximum file size	An integer value that defines the maximum size of a trace file before it is rolled over. Valid values are any string accepted by log4j as MaxFileSize.  If no unit of measure is specified, the integer value is interpreted as bytes.  The default size is 100 MB.

### 15.4.3 Defining file creation mode

The dfc.tracing.file\_creation\_mode key controls whether the log entries are recorded in one or several log files. By default all Foundation Java API trace entries are recorded in one log file. The following table describes all valid values for dfc.tracing.file\_creation\_mode key:

**Table 15-5: Valid values for the dfc.tracing.file\_creation\_mode key**

Value	Description
standard	All log entries are recorded in one log file. This is the default.

Value	Description
thread	<p>Foundation Java API creates a log file for each thread in the following format:</p> <p><i>&lt;file_prefix&gt;. &lt;threadname&gt;. &lt;timestamp&gt;.log</i></p> <p>Tracing by thread is only recommended in combination with the dfc.tracing.thread_name_filter key.</p>
user	<p>Foundation Java API creates a log file for each user in the following format:</p> <p><i>&lt;file_prefix&gt;. &lt;username&gt;  default. &lt;timestamp&gt;.log</i></p> <p>If the a user cannot be determined for a particular call, the trace is logged in a separate default log file.</p> <p>Tracing by user is only recommended in combination with the dfc.tracing.user_names_filter key.</p>

#### 15.4.4 Defining the trace file timestamp format

Each entry in a log file has a timestamp. If the file is recorded in compact mode, there are two columns for the timestamp. The first column records the entry time and the second column records the duration of the method call, the difference between method entry and method exit time. If the log file is recorded in standard mode, there is one column for the timestamp in the entry. The value recorded is either the entry time or the exit time, depending on whether the log entry is recording the method entry or exit.

By default, timestamps are expressed in seconds. You can configure the timestamp display using the dfc.tracing.timing\_style key. The following table describes the valid values for dfc.tracing.timing\_style:

**Table 15-6: Valid values for dfc.tracing.timing\_style**

Value	Description
nanoseconds	<p>The timestamp value is expressed in nanoseconds.</p> <p>Whether the timestamp values are actually returned in nanoseconds depends on the underlying operating system. The values cannot be correlated to absolute time.</p>
milliseconds	The timestamp value is expressed in milliseconds.

Value	Description
milliseconds_from_start	The timestamp is recorded as the number of milliseconds from the start of the JVM process.
seconds	<p>The timestamp value is displayed as the number of seconds from the start of the process. The value is a float.</p> <p>This is the default timing style.</p>
date	<p>The timestamp value is displayed as a date string. The default format is:</p> <p>yyyy/MM/dd-HH:mm:ss.S</p> <p>(The Javadocs contains the information for the <code>SimpleDateFormat</code> class.)</p> <p>The date setting is only used if <code>dfc.tracing.mode</code> is set to standard. If you set <code>dfc.tracing.timing_style</code> to date and the mode is compact, the timing style defaults to milliseconds.</p> <p>If the timing style is set to date, you can also set <code>dfc.tracing.date_format</code> key and <code>dfc.tracing.date_format_width</code> key to define an alternate date format, as described in “<a href="#">Defining the date format</a>” on page 283.</p>

#### 15.4.4.1 Defining the date format

There are three keys that determine the date format in a trace file:

- `dfc.tracing.timing_style`

If the key value is **date**, the date format and column width can be specified in the `dfc.tracing.date_format` and `dfc.tracing.date_column_width` keys.

- `dfc.tracing.date_format`

Specifies a date format that is different from that default format. The specified format specify must conform to the syntax supported by the Java class `java.text.SimpleDateFormat`.

- `dfc.tracing.date_column_width`

This key specifies the column width as a positive integer value. The default column width is 14. If the format specified in `dfc.tracing.date_format` is wider than 14 characters, modify the column width to the required number of characters.

## 15.4.5 Configuring method tracing

The following keys control method tracing:

- dfc.tracing.max\_stack\_depth

This key controls the depth of tracing into the Foundation Java API call stack.

The default value for this key is 1, meaning only the first method call in a Foundation Java API stack is traced. A value of -1 means that all levels of method calls are traced.

- dfc.tracing.mode

This key controls how the method entry and exit is recorded in the log file. Valid values are:

- **compact**: Foundation Java API adds one line to the file that records both entry and exit and return value for a method. The methods are logged in the order of method entrance. Foundation Java API buffers the log entries for a sequence of method calls until the topmost method returns.
- **standard**: Foundation Java API creates one line in the file for a method entry and one line for a method exit. The log entries for exit record the return values of the methods.

The default value is compact.

- dfc.tracing.method\_name\_filter[n]

This key specifies tracing for packages, classes, and methods. The key is a repeating key, that allows multiple entries in the dfc.properties file. Each entry has one value, specifying a package, class or method. Similar to repeating repository properties, each dfc.tracing.method\_name\_filter entry is referenced using a square-bracketed integer, with the first entry beginning with zero. For example:

```
dfc.tracing.method_name_filter[0]=<value>
dfc.tracing.method_name_filter[1]=<value>
dfc.tracing.method_name_filter[2]=<value>
```

Where <value> is one or more string expressions that identify what to trace. The syntax of the expression is:

```
([<qualified_classname_segment>][*]|*)[.[<method_name_segment>][*]()]
```

For example, the value **com.documentum.fc.client.DfPersistentObject** traces all methods on DfPersistentObject and any lower level calls made within the context of those methods

### 15.4.6 Tracing users by name

The dfc.tracing.user\_name\_filter key traces users. The key is a repeating key that allows multiple entries in the dfc.properties file. Each entry specifies one regular expression that identifies the user or users to trace. Each dfc.tracing.user\_name\_filter entry is referenced using an integer in brackets, the first entry beginning at zero.

For example:

```
dfc.tracing.user_name_filter[0]=<expression>
dfc.tracing.user_name_filter[1]=<expression>
dfc.tracing.user_name_filter[2]=<expression>
```

The expression is a regular expression, using the syntax for a regular expression as defined in the Java class java.util.regex.Pattern. Foundation Java API traces activities of the users whose login names (dm\_user.user\_login\_name) match the specified expression. The log entries contain the user name. By default, dfc.tracing.user\_name\_filter key empty, which means that all users are traced.

The tracing output does not necessarily include all Foundation Java API calls made by a particular user. For some calls, it is not possible to identify the user. For example, most methods on the DfClient interface are unrelated to a specific session or session manager. Consequently, when tracing is constrained by user, these method calls are not traced.

When tracing by user, Foundation Java API cannot identify the user until one of the following occurs:

- A method call on an object that derives from IDfTypedObject (if the session associated with that object is not an API session).
- A method call that takes an IDfSession or IDfSessionManager.
- A method call that returns an IDfSession or IDfSessionManager.
- An IDfSessionManager method call that sets or gets an IDfLoginInfo object.

### 15.4.7 Tracing threads by name

To trace specific threads, set the dfc.tracing.thread\_name\_filter key. The key is a repeating key, which means you can put multiple entries for the key into the file. Each entry has one value, identifying a thread or threads to be traced. Each dfc.tracing.thread\_name\_filter entry is referenced using an integer in brackets, the first entry beginning at zero.

For example:

```
dfc.tracing.thread_name_filter[0]=<expression>
dfc.tracing.thread_name_filter[1]=<expression>
dfc.tracing.thread_name_filter[2]=<expression>
```

Each dfc.tracing.thread\_name\_filter entry is set to a regular expression that identifies a thread or threads you want to trace. The regular expression must use the syntax for a regular expression defined in the Java class java.util.regex.Pattern.

The key is not set by default, which means that all methods in all traced threads are traced by default. Setting the key is primarily useful for standalone Foundation Java API-based applications that may spawn Foundation Java API worker threads.



**Note:** You can use `dfc.tracing.file_creation_mode` to further sort the entries for each thread into separate files. “[Defining file creation mode](#)” on page 281 contains more information.

#### 15.4.8 Including the session ID

By default, log entries contain the user name associated with the logged operation. To include a session ID with each entry, enable the `dfc.tracing.include_session_id` key by setting the Boolean value to `true`. By default, the key is disabled. Enabling the key instructs Foundation Java API tracing to add the session ID and the identity hash code of the associated session manager to the log entries. The session ID has the format `s<n>`, where `s` is an abbreviation for session and `<n>` is the session number.

#### 15.4.9 Tracing RPC calls

There are two keys that control RPC call tracing:

- `dfc.tracing.include_rpc_count`

This Boolean key instructs Foundation Java API to add an additional column to each log file entry that records the current RPC call count for the associated session. The logged value is N/A if Foundation Java API cannot determine the session. If the mode is set to compact, the logged RPC count is the count at the time the method exits. The default value for the key is false.

- `dfc.tracing.include_rpcls`

This Boolean key instructs Foundation Java API to include a separate line in the trace file for each executed RPC call. The default value for this key is false.

#### 15.4.10 Including stack trace for exceptions

By default, the Foundation Java API tracing facility only logs exception names and messages. Typically, the stack trace can be determined from the trace file. To obtain an exact stack trace for an exception, enable the `dfc.tracing.print_exception_stack` key by setting the key value to `true`.

If the key is enabled, the tracing facility logs the entire stack trace for the exception. The stack trace is recorded immediately following the line that logs the exit of the method that caused the exception. The trace is indented and prefixed with exclamation marks.

The default value for this key is false.

### 15.4.11 Setting verbosity

The dfc.tracing.verbosity key determines what set of classes are traced. By default, the key is disabled (false) and traces a standard set of classes. When enabled (true) the key traces an additional set of low-level classes. Tracing these classes greatly increases the number of entries in the trace file and can noticeably slow down the system. Turning on verbose mode is only recommended when suggested by Support.

### 15.4.12 Directing categories to the trace file

In a log4j2.properties file, categories can be defined as the target of logging operations. For Foundation Java API, a category specification would typically be a class or package. However, it is recommended to record that information in the trace file generated by the dfc.properties tracing facility, especially, when tracing a Foundation Java API class or package at the DEBUG level.

The following dfc.properties keys can be used to redirect the trace:

- dfc.tracing.log.category

This key specifies the category that are traced. The key is a repeating key that can have multiple entries in the dfc.properties file. Each entry has one value that specifies a category. Each dfc.tracing.log.category entry is referenced using an integer in brackets, with the first entry beginning at zero. For example:

```
dfc.tracing.log.category[0]=<class_or_package_name>
dfc.tracing.log.category[1]=<class_or_package_name>
```

- dfc.tracing.log.level

This key specifies the level of tracing. The dfc.tracing.log.level key defaults to DEBUG if not specified.

- dfc.tracing.log.additivity

This key is the additivity setting for the category. The dfc.tracing.log.additivity key defaults to false if not specified.

The dfc.tracing.log.level and dfc.tracing.log.additivity keys are also repeating keys, and the values across one index position in the entries for the keys are the settings for category identified at the corresponding index position in dfc.tracing.log.category.

### 15.4.13 Log file entry format

The log files store trace information in the following format:

```
<timestamp> [<method_duration>] [<threadname>]
<username>|<sessionID>|<session_mgr_id> (RPCs=<count>) [<entry_exit_designation>]
<stack_depth_indicator>
<qualified_class_name>@<object_identity_hash_code>. <method>(<method_arguments>
==><return_value>|<exception>)
```

The following table describes the entries in a log file:

**Table 15-7: Log entry components**

Component	Description
timestamp	The timestamp of the entry. The format depends on the tracing configuration, as defined in the dfc.tracing.timing_style key.
method_duration	The total length of time to execute the method. This value is only included if the dfc.tracing.mode key value is <b>compact</b> .
threadname	Name of the thread associated with the entry.
username	Name of the user associated with the entry.
sessionID	Identifies the session associated with the entry. This entry is only included if the dfc.tracing.include_session_id key enabled (true).
session_mgr_id	The hash code identity of the session manager associated with the entry. This entry is only included if the dfc.tracing.include_session_id key is enabled (true).
RPCs=<count>	Total number of RPC calls at the time the entry was logged. This is only included if dfc.tracing.include_rpc_count is set to true.

Component	Description
entry_exit_designation	Keyword that identifies source of the log entry. The keyword is only included if the dfc.tracing.mode key value is <b>standard</b> . Valid values are: <ul style="list-style-type: none"> <li>• ENTER: The entry records a method entry.</li> <li>• EXIT: The entry records a method exit.</li> <li>• !EXC!: The entry records a call that results in an exception.</li> <li>• RPC_ENTER: The entry records an RPC call entry.</li> <li>• RPC_EXIT: The entry records an RPC call exit.</li> </ul>
stack_depth_indicator	Indicates the depth of call stack tracing. The stack depth indicator is a series of dots (for example, ...).
qualified_class_name	Fully qualified name of the class being traced.
object_identity_hash_code	Hash code of the object on which the method is being called. If the method is static, this element does not appear in the log entry.
method	Name of the traced method.
method_arguments	Arguments to the specified method.
return_value	The value returned by the method. This entry is included if the dfc.tracing.mode value is <b>compact</b> or if the entry records the method exit.
exception	The exception name and message, if any, of the exception thrown by the method.

The values in each column in an entry are separated by spaces, not tabs.

#### 15.4.14 Trace file examples

The following examples describe trace files generated by various combinations of property settings. Due to space limitations on the page, the individual entries are line-wrapped in these examples.

##### ➡ Example 15-1: Settings are: dfc.tracing.enable=true

```
1158701543173 <user1> [Thread-0] [ENTER]
.....com.documentum.fc.client.DfTypedObject@28821120.getData()
1158701543173 <user1> [Thread-0] [EXIT]
.....com.documentum.fc.client.DfTypedObject@28821120.getData==>
com.documentum.fc.client.impl.TypedData@150ed68
```



- **Example 15-2: Settings are: dfc.tracing.enable=true; dfc.tracing.timing\_style=millis\_from\_start**

```
1141125 <user4> [Thread-5] [EXIT]
.....com.documentum.fc.client.impl.session.Session@4889213
.incrementReferenceCountIfNonZero ==> 2
```



- **Example 15-3: Settings are: dfc.tracing.enable=true; dfc.tracing.thread\_name\_filter=Thread[45]**

```
1158718491103 <user4> [Thread-4] [ENTER]
.....com.documentum.fc.client.DfTypedObject@25700470.getData()
1158718491103 <user4> [Thread-4] [EXIT]
.....com.documentum.fc.client.DfTypedObject@25700470.getData
==> com.documentum.fc.client.impl.typeddata.ITypedData@618b08
1158718491150 <user5> [Thread-5] [ENTER]
.....com.documentum.fc.impl.util.io.MessageChannel@15999328.readSocket
==> <void>
1158718491166 [Thread-5] [EXIT]
.....com.documentum.fc.impl.util.io.MessageChannel@15999328
.readLength ==> 18
```



- **Example 15-4: Settings are: dfc.tracing.enable=true; dfc.tracing.include\_rpc\_count=true; dfc.tracing.include\_session\_id=true**

```
1158702906324 <user5/s4/SM@25116828> [Thread-6] [ENTER] (RPCs=3269)
...com.documentum.fc.client.impl.connection.docbase.DocbaseConnection
@17535609.waitForCorrectTransactionContext()
```



# Chapter 16

## Audit management

### 16.1 Auditing

Auditing is a security feature for monitoring events that occur in a repository or application. Auditing an event creates an audit trail, a history in the repository of the occurrence of the event. Audit information can be used to:

- Analyze patterns of access to objects.
- Monitor when critical documents change or when the status of a critical document changes.
- Monitor the activity of specific users.
- Record all occurrences of a particular event on a given object or given object type.
- Record all occurrences of a particular event in the repository, regardless of the object to which it occurs.
- Record all workflow-related events in the repository.
- Record all occurrences of a particular workflow event for all workflows started from a given process definition.
- Record all executions of a particular job.
- Record all events in the repository.
- Record all transaction tracking events that are enabled for tracking in Audit Trail. By default, the TRANSACTION\_TRACKING\_FEATURE module is disabled. To enable the module, perform the following tasks:
  1. Add TRANSACTION\_TRACKING\_FEATURE as r\_module\_name attribute in the dm\_docbase\_config object.
  2. Configure the corresponding value in r\_module\_mode for same index where TRANSACTION\_TRACKING\_FEATURE is configured. Valid values are:
    - 0: Disable the transaction tracking
    - 1: Enable the transaction tracking

When you enable the transaction tracking, a prefix called [TRANSACTION\_TRACKING\_EVENTS] is added in the event\_description column. However, when you disable the transaction tracking, the prefix is not logged.

- Record all session-related information of the occasional users that are part of the dm\_occasional\_user\_role role.

- Record end user tracking information that includes IP address and geographical location of end user, Client host, Client ID, and Client name for contextual awareness and security monitoring.



**Note:** Make sure that the dm\_connect and dm\_logon\_failure events are registered for auditing.

Auditing is managed on the Audit Management page under the **Administration > Audit Management** node.



**Note:** Audit management requires extended user privileges.

## 16.2 Tracking external user transactions

All user transactions that are part of the dm\_external\_users group are tracked in the dm\_extuser\_transaction registered database table. All the data logged into the dm\_extuser\_transaction registered database table can only be viewed by users that are part of the dm\_extuser\_data\_access group. Only superuser can add or remove users from both the dm\_external\_users and dm\_extuser\_data\_access groups. In addition, only superuser can purge all data logged in the dm\_extuser\_transaction registered database table.

The list of audit events tracked for external user is as follows:

Activity	Event
Content upload	dm_setfile
Content download	dm_getfile
Renditions	dm_removecontent, dm_addrendition, dm_removerrendition
Workflow	dm_startedworkitem, dm_selectedworkitem, dm_completedworkitem, dm_delegatedworkitem, dm_changedactivityinstancestate, dm_createworkflow, dm_startworkflow, dm_finishworkflow, dm_abortworkflow, dm_changestateworkflow, dm_changeworkflowsupervisor, dm_wf_resolve_failure, dm_wf_autodelegate_failure, dm_addpackage, dm_removepackage, dm_repeatworkitem, dm_pauseworkitem, dm_resumeworkitem, dm_retryfailedworkitem, dm_faultedworkitem, dm_suspendedworkqueuetask, dm_unsuspendedworkqueuetask, dm_suspendworkitem, dm_unsuspendworkitem

Activity	Event
Save	dm_save
Destroy	dm_destroy

For more information about additional audit trial type properties for external user transactions, see *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)*.

## 16.3 Audit events

An *event* is something that happens to an object in the repository or an operation defined as an event by a user-written application. There are two types of events:

- *System events*

System events are events that Documentum CM Server recognizes and can audit automatically. For example, checking in a document can be an audited system event.

Documentum CM Server provides automatic auditing for any system event. When an audited system event occurs, Documentum CM Server automatically generates the audit trail entry. OpenText Documentum CM provides a large set of system events that are associated with API methods, lifecycles (business policies), workflows, and jobs. For a complete list of auditable system events, see “[System events](#)” on page 615.

- *Application events*

Application events are events that are recognized and audited by client applications. For example, a user opening a particular dialog can be an audited application event. To audit application events, an application must recognize when the event occurs and create the audit trail entry programmatically. Application events are not recognized by Documentum CM Server.

## 16.4 Audit trails

An *audit trail* is a recorded history of event occurrences that have been marked for auditing. Each occurrence is recorded in one *audit trail record*. The server stores audit trail records as objects in the repository. Depending on the event, the objects are dm\_audittrail, dm\_audittrail\_acl, or dm\_audittrail\_group objects. Auditing an event stores pertinent data in the audit trail object, such as when the event occurred and what object was involved.

Audit trail entries are generated after auditing is set up and can consume considerable space in the repository. Therefore audit trail entries should be removed from the repository periodically.

## 16.5 Audit properties

Object properties are audited if the properties are registered for auditing. After the properties are registered, the property name and new value are recorded in the attribute\_list property of the audit trail entry. Old property values are only included automatically if the audit\_old\_values property in the repository configuration object is enabled. The property name and old value are recorded in the attribute\_list\_old property of the audit trail entry. The audit\_old\_values property is enabled by default. If the audit\_old\_values property is disabled, the audit trail entry does not record changes to properties unless they are specifically registered for auditing when the event is registered.

Aspect attributes can also be audited. Aspect attribute audits record the aspect attribute changes attached to an object along with the object type attributes.

Auditing is available for aspect attributes attached to SysObject, user, group, and acl objects, and any of their associated subtypes. Auditing aspect attributes requires that auditing is also enabled for the object type or subtype.



**Note:** For repositories created on RDBMS with a page size of less than 8K, the audit\_old\_values property is always disabled and cannot be enabled.

## 16.6 Events audited by default

Documentum CM Server audits the following events by default:

- dm\_audit and dm\_unaudit  
All executions of methods that register or unregister events for auditing.
- dm\_signoff  
All executions of a IDfPersistentObject.signoff method.
- dm\_adddigisignature  
All executions of an addDigitalSignature method. By default, audit trail entries created for the dm\_adddigisignature event are not signed by Documentum CM Server. To sign those entries, register the event explicitly for auditing and set the argument to require signing.
- dm\_addesignature and dm\_addesignature\_failed  
All executions, successful or unsuccessful of an addESignature method. The audit trail entries for the dm\_addesignature event are signed by Documentum CM Server automatically.
- dm\_purgeaudit  
Removal of an audit trail entry from the repository. A dm\_purgeaudit event is generated whenever a destroy method is executed to remove an audit trail entry from the repository or a PURGE\_AUDIT administration method is executed. All dm\_purgeaudit events are audited.
- User login failure

- dm\_default\_set

A default set of events on objects of type dm\_document and its subtypes. This event is registered against the repository configuration object, and Documentum CM Server audits the events in the set for dm\_document type and its subtypes. The following describes the events that are included in this set for the dm\_docbase\_config object type:

dm_archive	dm_checkin	dm_restore
dm_assemble	dm_checkout	dm_save
dm_bp_attach	dm_destroy	dm_setfile
dm_bp_demote	dm_freeze	dm_signoff
dm_bp_promote	dm_link	dm_unfreeze
dm_bp_resume	dm_lock	dm_unlink
dm_bp_suspend	dm_mark	dm_unlock
dm_branch	dm_prune	

- TRANSACTION\_TRACKING\_FEATURE

When you enable the TRANSACTION\_TRACKING\_FEATURE module, the events described in the following table are audited:

**Table 16-1: Events audited by the TRANSACTION\_TRACKING\_FEATURE module**

Object type	Audited events
dm_document	<ul style="list-style-type: none"> <li>- dm_save</li> <li>- dm_saveasnew</li> <li>- dm_fetch</li> <li>- dm_destroy</li> <li>- dm_link</li> <li>- dm_getfile</li> </ul>
dm_folder and dm_cabinet	<ul style="list-style-type: none"> <li>- dm_save</li> <li>- dm_saveasnew</li> <li>- dm_fetch</li> <li>- dm_destroy</li> <li>- dm_link</li> </ul>
dm_user	<ul style="list-style-type: none"> <li>- dm_save</li> <li>- dm_destroy</li> <li>- dm_connect</li> <li>- dm_disconnect</li> </ul>
dm_group	<ul style="list-style-type: none"> <li>- dm_save</li> <li>- dm_destroy</li> </ul>

- dm\_occasional\_user\_role

All the occasional users that are members of the dm\_occasional\_user\_role, dm\_connect, and dm\_disconnect events are audited.

### 16.6.1 Disabling or modifying default auditing

With the exception of user login failure and the dm\_default\_set events, default auditing cannot be disabled because there are no default registry objects for these events. Turning off auditing of the dm\_default\_set event for the repository configuration type turns off auditing of all events represented by the dm\_default\_set event.

Default auditing can be modified by registering against the events audited by default. Documentum CM Server creates the audit trail entry based on the criteria that are defined for the event and target. When the registration is removed, Documentum CM Server returns to creating the default audit trail entry for the event and target.

## 16.7 Auditing by object type

Auditing by object type creates audit trails for events for all objects of a particular type. You can select the types, restrict the set of objects on which audit trails are created, and select the events.

You can set audits only for one object type at a time. Complete these instructions for each object type you audit.

You must have Config Audit privileges to use this function.

**Table 16-2: Object auditing properties**

Field	Description
<b>Application Code</b>	Enter the application code to audit only objects with a particular application code.  The application code is a property set by the client application that creates the object. For example, an application sets the application code to the value Internal. To audit objects of the type you selected with application code Internal, type <i>Internal</i> in the Application Code field.  You cannot enter a value in the field if you previously selected a dm_user, dm_acl, or dm_group object type.

Field	Description
<b>Lifecycle</b>	<p>Records objects that are attached to a lifecycle. Click <b>Select Lifecycle</b> to access the <b>Choose a lifecycle</b> page.</p> <p>Select the correct lifecycle and then click <b>OK</b>.</p>
<b>State</b>	<p>Records only those objects attached to the lifecycle and in a particular state. Select a state from the drop-down list.</p>
<b>Attributes</b>	<p>Records the values of particular properties of the object in the audit trail. Click <b>Select Attributes</b> to access the <b>Choose an attribute</b> page.</p> <p>Select the properties whose values you want to record, click <b>&gt;</b>, then click <b>Add</b>. To remove any properties, select them on the right-hand side of the page and click <b>&lt;</b>.</p> <p>Click <b>OK</b> when you are finished.</p>
<b>Has signature manifested</b>	<p>Select to sign the audit trail.</p>
<b>Include all subtypes</b>	<p>Select to include all subtypes of the audited object type.</p>
<b>Authentication required</b>	<p>Select to require authentication for custom (user-defined) events that are audited.</p>
<b>Add</b>	<p>Click to access the <b>Choose an event</b> page and select the events you want to register.</p> <p>Select one or more events to audit and click <b>&gt;</b> to move the events to the Selected Items column. To remove any events, select them in the Selected Items column and click <b>&lt;</b>.</p> <p>Click <b>OK</b> when you are finished.</p> <p>To unregister any events, select them in the Event Name list and click <b>Remove</b>.</p>

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding, modifying, or deleting auditing by object type.

## 16.8 Auditing by object instance

Auditing by object instance creates audit trails for events for a particular object in the repository. You can set audits only for one object type at a time.

Aspect attributes can be audited if they are attached to SysObject, user, group, and acl objects, and any of their associated subtypes. Auditing aspect attributes requires that the related aspect type is registered for auditing.

You must have Config Audit privileges to audit object instances.

**Table 16-3: Object instance auditing properties**

Field	Description
<b>Attributes</b>	Records the values of particular properties of the object in the audit trail. Click <b>Select Attributes</b> to access the <b>Choose an attribute</b> page.  Select the properties whose values you want to record, click >, then click <b>Add</b> . To remove any properties, select them on the right-hand side of the page and click <.  Click <b>OK</b> when you are finished.
<b>Add</b>	Click to access the <b>Choose an event</b> page and select the events you want to register.  Select one or more events to audit and click > to move the events to the Selected Items column. To remove any events, select them in the Selected Items column and click <. Click <b>OK</b> when you are finished.  To unregister any events, select them in the Event Name list and click <b>Remove</b> .

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding, modifying, or deleting auditing by object instance.

## 16.9 Auditing by events selected for all objects in the repository

You can add or remove auditing events for all objects in the repository.

You must have Config Audit privileges to use this function.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding or removing auditing by events.

## 16.10 Search audit

The Search Audit feature lets you search and view audit trails. You must have View Audit extended privileges to search for and view existing audit trails.

**Table 16-4: Audit search properties**

Field	Description
<b>Search By</b>	Indicates whether to use the criteria specified on the search page or a DQL query to search for the audit trail.  Do one of the following: <ul style="list-style-type: none"> <li>• Select the <b>Search criteria defined below</b> option and enter the search criteria.</li> <li>• Select the <b>DQL</b> option and enter a DQL query in the <b>Where Clause</b> field. Click <b>OK</b> to display the query results.</li> </ul>
<b>Events</b>	Restricts the search by events. Click <b>Select</b> and select one or more events and click <b>OK</b> .
<b>Object Name</b>	Restricts the search by object names. Select <b>Begins With</b> , <b>Contains</b> , or <b>Ends With</b> and type in a string.
<b>Versions</b>	Restricts the search by version. Type in a version.
<b>Look In</b>	Restricts the search to a particular folder. Click <b>Select Folder</b> and select the folder.
<b>Audit Dates</b>	Restricts the search by time. Click <b>Local Time</b> or <b>UTC</b> , then type or select a beginning date in the <b>From</b> field and an ending date for the search in the <b>Through</b> field.
<b>Type</b>	Restricts the search to a particular type. Click <b>Select Type</b> and select the type. To include subtypes of the type, click <b>Include Subtype</b> .

Field	Description
<b>Lifecycle</b>	Restricts the search to objects attached to a lifecycle. Click <b>Select Lifecycle</b> and select a lifecycle.
<b>Application Code</b>	Restricts the search to objects with an application code. Type the application code. To restrict the search to those audit trails that are signed, select <b>Has Signature</b> .
<b>Controlling Application</b>	Restricts the search to objects with a controlling application. Type the name of the application.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on searching and viewing audit trails.

## 16.11 Audit policies

An audit policy ensures that only the users or groups that are specified in the purge policy can delete an audit record. If an unauthorized user or group attempts to delete the audit record, Documentum CM Server throws an error message. If there are multiple policies for same user, the policy with the highest permissions is in effect.

Audit policies specify which user, group, or role can purge audit trails. You must be an Install Owner to access and manage audit policies. Other users can only view the list of audit policies.

Audit policies are managed on the Audit Policies page. Select **Administration > Audit Management** to display the Audit Management page, then click the **Audit Policies** link to display the Audit Policies page. *"Audit policies page information" on page 300* describes the information on the Audit Policies page.

**Table 16-5: Audit policies page information**

Field	Description
<b>Name</b>	The name of the audit policy.
<b>Accessor Name</b>	The name of the user, group, or role that are assigned this audit policy.
<b>Is Group</b>	Indicates whether the user specified in the Accessor Name column is belongs to a group.

## 16.11.1 Creating, modifying, or deleting an audit policy

You must be the Install Owner to create, modify, or delete an audit policy.

**Table 16-6: Audit policy information**

Field	Description
<b>Name</b>	The name of the audit policy.
<b>Accessor Name</b>	The user, group, or role to which this audit policy is assigned.
<b>Audit Policy Rules</b>	<p>Specifies the policy rules, as follows:</p> <ul style="list-style-type: none"> <li>• Click <b>Add</b> to add a rule. The Create/Edit Rule page displays. Select an attribute and enter a value for the attribute.</li> <li>• Select an attribute name, then click <b>Edit</b> to modify the rule. The Create/Edit Rule page displays. Modify the attribute.</li> <li>• Select an attribute name, then click <b>Remove</b> to delete the rule. There must be at least one rule or condition to save the audit policy.</li> </ul>

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, modifying, or deleting an audit policy.

## 16.11.2 Audit policy example

The following audit policy example specifies the Test purge policy that enables user1 to purge the audit record for the object\_type attribute type1 and the is\_archived attribute T:

**Table 16-7: Audit policy example values**

Field	Description
<b>Name</b>	Test
<b>Accessor Name</b>	user1
<b>Audit Policy Rules</b>	
<b>Attribute Name</b>	Attribute Value
<b>object_type</b>	type1
<b>is_archived</b>	T

The policy described in this example only protects audit records that satisfy the policy. For example, the policy does not protect audit records that have the

is\_archived attribute set to F. Any user with purge audit extended privilege can delete those records.

## 16.12 Registering audits

The Register Audit page specifies the properties that are audited for an object or object instance.

Select the properties as described in “[Object and object instance auditing properties](#)” [on page 302](#) to define the audited properties and register the object or object instance for auditing.

The following fields are disabled:

- Application Code
- Lifecycle
- State
- Has signature manifested
- Include all subtypes
- Authentication Required

These fields are enabled only for auditing by object type.

**Table 16-8: Object and object instance auditing properties**

Field	Description
<b>Attributes</b>	Records the values of particular properties of the object in the audit trail. Click <b>Select Attributes</b> to access the <b>Choose an attribute</b> page.  Select the properties whose values you want to record, click >, then click <b>Add</b> . To remove any properties, select them on the right-hand side of the page and click <. Click <b>OK</b> when you are finished.
<b>Add</b>	Click to access the <b>Choose an event</b> page and select the events you want to register.  Select one or more events to audit and click > to move the events to the Selected Items column. To remove any events, select them in the Selected Items column and click <. Click <b>OK</b> when you are finished.  To unregister any events, select them in the Event Name list and click <b>Remove</b> .

## 16.13 Adding, modifying, or removing audits

Register Audit page lists object instances or an object type that you selected for auditing, as well as the audited criteria and events. On this page, you can add, edit, or remove audits.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding, modifying, or removing audits by object type and object instance.

## 16.14 Verifying or purging audit trails

Audit trails are displayed on the Audit Trails page after a search query has been issued, as described in “[Search audit](#)” on page 299.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing, verifying, or purging audit trails.

## 16.15 Interpreting audit trails of Foundation Java API method, workflow, and lifecycle events

Audit trail entries for Foundation Java API method, workflow, and lifecycle events are stored in the repository as audit trail objects. Each audit trail object records one occurrence of a particular event. The audit trail object properties describe the event.

The properties that have a common purpose for entries generated by Documentum CM Server include all the properties other than the string\_<x> and id\_<x> properties. An audit trail object also has five ID-datatype properties and five string properties. These properties are named generically, id\_1 to id\_5 and string\_1 to string\_5. In audit trail entries for workflows and lifecycle events, Documentum CM Server uses these properties to store information specific to the particular kinds of events. Some of the events generated by methods other than workflow or lifecycle-related methods use these generic properties and some do not. A user-defined event can use these properties to store any information wanted.

### 16.15.1 Audit trails for events generated by non-workflow or lifecycle methods

The following table describes how Documentum CM Server uses the generic string and id properties in audit trails generated by methods other than workflow or lifecycle methods. Only those events that use the generic properties are listed. If an event is not listed in this table, Documentum CM Server does not use the generic properties in audit trails generated by that event.

**Table 16-9: Usage of generic properties by API events**

Event	Generic property use
Adddigsignture	<p><i>string_1</i>, User name provided as an argument to the method or the name of the connected user if the user argument was not specified</p> <p><i>string_2</i>, Reason for the signing</p>
Addesignature (success)	<p><i>string_1</i>, User who signed the object</p> <p><i>string_2</i>, Justification text</p> <p><i>string_3</i>, The number of the signature, the name of the method used to generate the signature, and the pre-signature hash argument. For example: 2/PDFSign/<i>pre-signature hash_argument</i></p> <p><i>string_4</i>, Hash of the primary content (page number 0)</p> <p><i>string_5</i>, Hash of the signed content. Note that if the signed content is the primary content (rather than a rendition), this value is the same as the hash in <i>string_4</i>.</p>
Addesignature (failure)	<p><i>string_1</i>, User who signed the object</p> <p><i>string_2</i>, Error message indicating why the failure occurred</p> <p><i>string_3</i>, The number of the signature, text indicating the reason for the audit entry, and the pre-signature hash argument. For example: 2/ENTRY_F0R_FAILED_ESIGN_OPERATION/<i>pre-signature hash_argument</i></p>
Addnote	<p><i>id_1</i>, Object ID of document to which the note is attached</p> <p><i>id_2</i>, Object ID of the note</p>

Event	Generic property use
Addrendition	<i>id_1</i> , Object ID of the content object <i>string_1</i> , Format of the rendition <i>string_2</i> , Either “Replace Old Rendition” or “Save New Rendition”, depending on whether the added rendition replaces an existing rendition or is a new rendition.
Addretention	<i>id_1</i> , Object ID of the retainer object
Appendcontent	See Setfile
Appendfile	See Setfile
Appendpart	<i>id_1</i> , Object ID of the virtual document to which you are appending the component <i>id_2</i> , Object ID of the component <i>id_3</i> , Object ID of the containment object that links the virtual document and the component <i>string_1</i> , The version label of the component <i>string_2</i> , The use_node_ver_label setting <i>string_3</i> , The follow_assembly setting <i>string_4</i> , The copy_child setting
Assume	<i>string_1</i> , The success or failure of the user authentication
Audit	<i>string_1</i> , The audited operation
Authenticate	<i>string_1</i> , The success or failure of the user authentication
Bindfile	See Setfile
Checkin	<i>id_1</i> , Object ID of the version from which the new version created by the checkin was derived

Event	Generic property use
Connect	<p><i>string_1</i>, Format is Client ID;Client name where          Client ID is the unique ID generated for each Foundation Java API client          Client name (optional) is the name of the application set using Foundation Java API EndUserInfo API</p> <p><i>string_2</i>, (Optional) IP address of the client machine</p> <p><i>string_3</i>, (Optional) Geographical location of the client machine</p> <p><i>string_4</i>, Format is Foundation Java API Host;Foundation Java API IP where</p> <ul style="list-style-type: none"> <li>• Host is the host name of the client machine from which the user is connected</li> <li>• IP is the IP address of the client machine from which the user is connected</li> </ul> <p><i>string_5</i>, Identifies the authentication mechanism used to authenticate the user. Values are:</p> <ul style="list-style-type: none"> <li>• ticket, for ticketed login</li> <li>• trusted, for trusted login</li> <li>• unified, for Windows unified login</li> <li>• operating system password, for operating system password authentication</li> <li>• plug-in password, for plug-in authentication</li> <li>• operating system external, for authentication with operating system password by an external password checking program</li> </ul>
Destroy	Destroy uses the generic properties only when the object to be destroyed is a dm_audittrail object or a subtype of dm_audittrail. For details, see the Purge Audit entry in this table.
Getcontent	See Getfile
Getfile	<i>id_1</i> , Object ID of the content object for the content file

Event	Generic property use
Getlogin	<p><i>id_1</i>, Object ID of the user object representing the user identified in <i>string_1</i></p> <p><i>string_1</i>, Name of the user for whom the ticket was requested</p> <p> <b>Note:</b> This API contains the <code>server_name</code> argument that identifies a server for the scope of a single-use ticket. If <code>single_use</code> is T and <code>server_name</code> is ANY_SERVER, the scope of the ticket is any server in a load balancing setup.</p>
Getpath	See Getfile
Insertcontent	See Setfile
Insertfile	See Setfile
Insertpart	<p><i>id_1</i>, Object ID of the virtual document to which you are inserting the component</p> <p><i>id_2</i>, Object ID of the component</p> <p><i>id_3</i>, Object ID of the containment object that links the virtual document and the component</p> <p><i>string_1</i>, The version label of the component</p> <p><i>string_2</i>, The <code>use_node_ver_label</code> setting</p> <p><i>string_3</i>, The <code>follow_assembly</code> setting</p> <p><i>string_4</i>, The <code>copy_child</code> setting</p>
Kill	<i>id_1</i> , Session ID of the terminated session
Link	<p><i>id_1</i>, Object ID of the folder to which the object is linked.</p> <p><i>id_2</i>, Object ID of the linked object</p> <p><i>string_1</i>, Name of the folder to which the object is linked</p> <p><i>string_2</i>, Name of the linked object</p>

Event	Generic property use
Logon Failure	<p><i>string_1</i>, Format is Client ID;Client name where      Client ID is the unique ID generated for each Foundation Java API client      Client name (optional) is the name of the application set using Foundation Java API EndUserInfo API</p> <p><i>string_2</i>, (Optional) IP address of the client machine</p> <p><i>string_3</i>, (Optional) Geographical location of the client machine</p> <p><i>string_4</i>, Format is Foundation Java API Host;Foundation Java API IP where</p> <ul style="list-style-type: none"> <li>• Host is the hostname of the client machine from which the user is connected</li> <li>• IP is the IP address of the client machine from which the user is connected</li> </ul> <p><i>string_5</i>, UserLogonName as entered by the user</p> <p> <b>Note:</b> If the user enters a valid user name, it is same as user_name of the dm_user object.</p>
Mark	<p><i>string_1</i>, Name of the version label</p> <p> <b>Note:</b> One audit trail entry is created for each label assigned in the Mark method.</p>
Move Content	<p><i>string_1</i>, Name of the storage area from which the content was moved</p> <p><i>string_2</i>, Name of the storage area to which the content was moved.</p> <p><i>id_1</i>, Object ID of the SysObject containing the moved content file.</p>

Event	Generic property use
Purge Audit	<p><i>string_1</i>, the time_stamp value of the first deleted audit trail entry in the transaction</p> <p><i>string_2</i>, the time_stamp value of the last deleted audit trail entry in the transaction</p> <p><i>string_3</i>, the actual number of audit trail entries deleted in the transaction</p> <p><i>string_5</i>, the list of arguments defined in the method command line</p> <p><i>id_1</i>, the object ID of the first audit trail entry deleted by the transaction</p> <p><i>id_2</i>, the object ID of the last audit trail entry deleted by the transaction</p>
Removecontent	<p><i>id_1</i>, Object ID of the content object representing the content file removed from the SysObject.</p> <p><i>string_1</i>, The page that was removed.</p>
Removenote	<p><i>id_1</i>, Object ID of the object to which the note was attached</p> <p><i>id_2</i>, Object ID of the note</p>
Removepart	<p><i>id_1</i>, Object ID of the virtual document from which you are removing the component</p> <p><i>id_2</i>, Object ID of the component</p> <p><i>id_3</i>, Object ID of the containment object that links the virtual document and the component</p> <p><i>string_1</i>, If specified, the order_no that identifies the component to be removed</p>
Removerendition	<p><i>id_1</i>, Object ID of the content object representing the content file of rendition</p> <p><i>string_1</i>, Rendition format</p>
Removeretention	<i>id_1</i> , Object ID of the retainer object
Setcontent	See Setfile

<b>Event</b>	<b>Generic property use</b>
Setfile	<p><i>id_1</i>, Object ID of the content object for the content file</p> <p><i>string_1</i>, Name of the API</p> <p><i>string_2</i>, Name of the file (unused for Appendcontent, Bindfile, Inserttcontent, Setcontent)</p> <p><i>string_3</i>, Page number of the content file</p> <p><i>string_4</i>, Format of the content file</p>
Setpath	See Setfile
Setoutput	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_5</i>, Output port name</p>
Setretentionstatus	<p><i>string_1</i>, Original status of the retainer</p> <p><i>string_2</i>, New status of the retainer</p>
Unaudit	<i>string_1</i> , Name of the operation from which auditing was removed
Unlink	<p><i>id_1</i>, Object ID of the folder to which the object is linked.</p> <p><i>id_2</i>, Object ID of the linked object</p> <p><i>string_1</i>, Name of the folder to which the object is linked</p> <p><i>string_2</i>, Name of the linked object</p>
Unmark	<i>string_1</i> , Name of the version label.

Event	Generic property use
Updatepart	<p><i>id_1</i>, Object ID of the virtual document into which you are inserting the component</p> <p><i>id_2</i>, Object ID of the component</p> <p><i>id_3</i>, Object ID of the containment object that links the virtual document and the component</p> <p><i>string_1</i>, The version label of the component</p> <p><i>string_2</i>, The use_node_ver_label setting</p> <p><i>string_3</i>, The follow_assembly setting</p> <p><i>string_4</i>, The copy_child setting, if specified</p> <p><i>string_5</i>, The order_no if specified</p>

## 16.15.2 Lifecycle audit trails

The following table describes how Documentum CM Server uses the generic string and id properties in audit trails generated by lifecycle events:

**Table 16-10: Usage of generic properties by lifecycle events**

Event	Generic property use
Attach	<p><i>id_1</i>, Object ID of the business policy</p> <p><i>string_1</i>, State to which object is being attached</p>
Demote	<p><i>id_1</i>, Object ID of the business policy</p> <p><i>string_1</i>, State from which object was demoted</p> <p><i>string_2</i>, State to which the object was demoted</p>
Install	Does not use the generic properties.
Promote	<p><i>id_1</i>, Object ID of the business policy</p> <p><i>string_1</i>, State from which object was promoted</p> <p><i>string_2</i>, State to which object was promoted</p>
Resume	<p><i>id_1</i>, Object ID of the business policy</p> <p><i>string_1</i>, State to which the object is returned</p>

Event	Generic property use
Suspend	<i>id_1</i> , Object ID of the business policy <i>string_1</i> , The business policy state of object at the time of suspension
Uninstall	Does not use the generic properties.
Validate	<i>string_1</i> , Number of states in the business policy.

### 16.15.3 Workflow audit trails

The following table describes how Documentum CM Server uses the generic string and id properties in audit trails generated by workflow events:

**Table 16-11: Usage of generic properties by workflow events**

Event	Generic property use
Abort workflow (dm_abortworkflow)	<i>id_1</i> , Object ID of the workflow
Add attachment (dm_addattachment)	<i>id_1</i> , Object ID of the workflow <i>id_5</i> , Object ID of the attached object <i>string_5</i> , Name of the attached object
Add note (dm_addnote)	<i>id_1</i> , Object ID of the workflow <i>id_5</i> , Object ID of the note object <i>string_1</i> , Activity sequence number <i>string_2</i> , Activity name <i>string_5</i> , Value of the keep_permanent flag note

Event	Generic property use
Add package (dm_addpackage)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item (used only if addPackage is called with the work item referenced in the arguments)</p> <p><i>id_5</i>, Object ID of the document in the package. If there are multiple documents, there are a corresponding number of audit trail entries, each with a different value in <i>id_5</i>.</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_3</i>, Names of the components identified in the componentIds argument. This is only set if package control is not enabled.</p> <p><i>string_5</i>, Package name</p>
Auto Delegation of Activity Failed (dm_wf_autodelegate_failure)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p>
Auto Transition of Activity (autotransactivity)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_5</i>, Index position of the TRUE condition in the dm_cond_expr object examined for the transition.</p> <p>This event is supported for backwards compatibility. The Portselect event provides additional or more current information about an automatic transition.</p>
Change activity instance state (dm_changedactivity_instancestate)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>id_5</i>, Value in the r_exec_results property of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_5</i>, Value of the return_value property of the work item</p>

<b>Event</b>	<b>Generic property use</b>
Change process state (dm_changestateprocess)	<p><i>string_3</i>, Previous state</p> <p><i>string_4</i>, New state</p>
Change supervisor (dm_changeworkflowsupervisor)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>string_4</i>, New supervisor name</p> <p><i>string_5</i>, Old supervisor name</p>
Change workflow state (dm_changestateworkflow)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>string_3</i>, Previous state</p> <p><i>string_4</i>, New state</p>
Change work item priority (dm_changepriorityworkitem)	<p><i>id_1</i>, Object ID of the workflow that contains the work item</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>string_1</i>, Sequence number of the activity that generated the work item</p> <p><i>string_2</i>, Name of the activity</p> <p><i>string_3</i>, Old priority value</p> <p><i>string_5</i>, New priority value</p>
Completed work item (dm_completedworkitem)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>id_5</i>, For automatic work items: Object ID of the document containing the results of the execution. (This is the value in the r_exec_results property.)</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_3</i>, Comma-separated list of work item properties and their values. The properties are: user_time, user_cost, a_wq_name, a_wq_flag, and a_wq_doc_profile. (a_wq_name and a_wq_doc_profile are enclosed in double quotes)</p> <p><i>string_5</i>, Value in the return_value property of work item</p>

Event	Generic property use
Create workflow (dm_createworkflow)	<i>id_1</i> , Object ID of the workflow <i>string_4</i> , Supervisor name <i>string_5</i> , Name of the workflow
Delegated work item (dm_delegatedworkitem)	<i>id_1</i> , Object ID of the workflow <i>id_2</i> , Object ID of the work item <i>string_1</i> , Activity sequence number <i>string_2</i> , Activity name <i>string_3</i> , Activity type (Manual or Automatic) <i>string_4</i> , Name of the workqueue, if any, to which the task is assigned <i>string_5</i> , Name of the user to which the task is delegated
Finish workflow (dm_finishworkflow)	<i>id_1</i> , Object ID of the workflow
Install workflow or activity definition (dm_install)	Does not use the generic properties.
Invalidate workflow or activity definition (dm_invalidate)	Does not use the generic properties.
Pause work item (dm_pauseworkitem)	<i>id_1</i> , Object ID of the workflow <i>id_2</i> , Object ID of the work item <i>string_1</i> , Activity sequence number <i>string_2</i> , Activity name
Port select (dm_portselect)	<i>id_1</i> , Object ID of the workflow <i>string_1</i> , Activity sequence number <i>string_2</i> , Activity name <i>string_5</i> , Selected output port. If multiple ports are selected, a corresponding number of audit trail entries are created, each with a different value in <i>string_5</i> .

Event	Generic property use
Pseudo-completed work item (dm_pseudocompletedworkitem)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>string_1</i>, Sequence number of the activity</p> <p><i>string_2</i>, Name of the activity</p> <p><i>string_3</i>, State of the work item prior to pseudo-completion</p> <p><i>string_5</i>, Name of the task owner</p>
Remove attachment (dm_removeattachment)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_5</i>, Object ID of the attached object that was removed</p> <p><i>string_5</i>, Name of the attached object that was removed</p>
Remove note (dm_removenote)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_5</i>, Object ID of the note object. If the remove note event is triggered by a remove package event that removes a package with multiple notes attached to its components, there are multiple remove note audit trail entries, each with a different <i>id_5</i> value.</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p>
Remove package (dm_removepackage)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_5</i>, Object ID of the document in the package. If there are multiple documents, there are a corresponding number of audit trail entries, each with a different value in <i>id_5</i>.</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_5</i>, Package name</p>
Repeat work item (dm_repeatworkitem)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p>

Event	Generic property use
Resume work item (dm_resumeworkitem)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p>
Save a workqueue (dm_save_workqueue)	<p><i>id_1</i>, Object ID of the workqueue</p> <p><i>id_2</i>, Value of the wq_policy_id property of the workqueue object</p> <p><i>string_1</i>, Name of the workqueue</p> <p><i>string_2</i>, Number of users in the workqueue</p>
Save a workqueue policy (dm_save_workqueuepolicy)	<p><i>id_1</i>, Object ID of the workqueue policy object</p> <p><i>string_1</i>, Name of the workqueue policy</p> <p><i>string_2</i>, Maximum threshold of the policy</p>
Selected work item (dm_selectedworkitem, a work item has been acquired)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_4</i>, Name of the workqueue, if any, to which the task is assigned</p>
Sign off work item (dm_signoff)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>id_5</i>, Object ID of the document in the package. If there are multiple documents, there are a corresponding number of audit trail entries, each with a different value in <i>id_5</i>.</p> <p><i>string_1</i>, For Windows, the domain and user name (used to validate signature) of user</p> <p><i>string_5</i>, Text provided by <i>reason</i> argument in Signoff method</p>

Event	Generic property use
Started work item (dm_startedworkitem)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i>, Object ID of the work item</p> <p><i>id_5</i>, For automatic activities, the object ID of the dm_method object for the method executed by the activity. For manual activities, this is null.</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_3</i>, Comma-separated list of work item properties and their values. The properties are: r_priority, a_wq_name, and a_wq_doc_profile. a_wq_name and a_wq_doc_profile are enclosed in double quotes.</p> <p><i>string_4</i>, Name of the performer of the work item.</p> <p><i>string_5</i>, Value in the dependency_type property of the corresponding queue item object.</p>
Start workflow (dm_startworkflow)	<i>id_1</i> , Object ID of the workflow
Suspend workqueue task (dm_suspendedworkqueuetask)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i> Object ID of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_4</i>, Workqueue name</p>
Uninstall workflow or activity definition (dm_uninstall)	Does not use the generic properties.
Unsuspend workqueue task (dm_unsuspendedworkqueue)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i> Object ID of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_4</i>, Workqueue name</p>
Validate workflow or activity definition (dm_validate)	Does not use the generic properties.

Event	Generic property use
Generate report on an activity if at least one package has been defined accordingly (dm_wf_business_data)	<p><i>id_1</i>, Object ID of the workflow</p> <p><i>id_2</i> Object ID of the work item</p> <p><i>string_1</i>, Activity sequence number</p> <p><i>string_2</i>, Activity name</p> <p><i>string_3</i>, Process name</p> <p><i>string_4</i>, User name</p> <p>There is always a dmi_audittrail_attrs object associated with the audit trail of the dm_wf_business_data event. The dmi_audittrail_attrs object has the following entries:</p> <p><i>audit_obj_id</i>: Object ID of corresponding audit trail object.</p> <p><i>attribute_list</i>: An XML string containing data from all packages.</p>

## 16.16 Interpreting ACL and group audit trails

Audit trail entries generated when ACLs are created, changed, or destroyed are recorded in dm\_audittrail\_acl objects. Entries generated when groups are created, changed, or destroyed are recorded in dm\_audittrail\_group objects. The dm\_audittrail\_acl and dm\_audittrail\_group object types are subtypes of the dm\_audittrail type.

The properties defined for the dm\_audittrail\_acl object type store information about an audited ACL. The properties identify the event (dm\_save, dm\_saveasnew, or dm\_destroy), the target ACL, the ACL entries or changes to the entries. For example, suppose you create an ACL with the following property values:

```
r_object_id:451e9a8b0001900
r_accessor_name [0]:dm_world
                [1]:dm_owner
                [2]:John Doe
r_accessor_permit [0]:6
                  [1]:7
                  [2]:3
r_accessor_xpermit [0]:0
                   [1]:0
                   [2]:196608
r_is_group [0]:F
            [1]:F
            [2]:F
```

The audit trail acl object created in response has the following property values:

```
r_object_id:<audit trail acl obj ID>
audited_obj_id      :451e9a8b0001900
event_name          :dm_save
```

```

string_1          :Create
accessor_operation[0] :I
[1] :I
[2] :I
accessor_name      [0] :dm_world
[1] :dm_owner
[2] :John Doe
accessor_permit     [0] :6
[1] :7
[2] :3
accessor_xpermit   [0] :0
[1] :0
[2] :196608
application_permit [0]:
[1]:
[2]:
permit_type        [0]:0
[1]:0
[2]:0
is_group           [0] :F
[1] :F
[2] :F

```

The event\_name records the repository event, a save method, that caused the creation of the audit trail entry. The string\_1 property records the event description, in this case, Create, indicating the creation of an ACL. The accessor\_operation property describes what operation was performed on each accessor identified at the corresponding index position in accessor\_name. The accessor\_permit and accessor\_xpermit properties record the permissions assigned to the user (or group) identified in the corresponding positions in accessor\_name. Finally, the is\_group property identifies whether the value in accessor\_name at the corresponding position represents an individual user or a group.

Now suppose you change the ACL. The changes you make are:

- Add the Sales group
- Remove John Doe
- Change the access of world to None

The resulting audit trail acl object has the following properties:

```

r_object_id          :<audit trail acl obj ID>
audited_obj_id       :451e9a8b0001900
event_name           :dm_save
string_1             :Save
accessor_operation   [0] :U
[1] :I
[2] :D
accessor_name        [0] :dm_world
[1] :Sales
[2] :JohnDoe
accessor_permit       [0] :0
[1] :2
[2] :3
accessor_xpermit     [0] :0
[1] :0
[2] :196608
application_permit   [0]:
[1]:
[2]:
permit_type          [0]:0
[1]:0

```

is_group	[2]:0 [0] :F [1] :T [2] :F
----------	-------------------------------------

dm\_world is found in accessor\_name[0]. Consequently, the values in the corresponding position in the accessor\_operation, accessor\_permit, and accessor\_xpermit properties identify the changes made to dm\_world. In this case, the operation is U, meaning update. The values in accessor\_permit and accessor\_xpermit show the updated permissions for dm\_world.

Sales is found in accessor\_name[1]. The value in accessor\_operation[1], I, shows that an entry for Sales was added (inserted) into the ACL. The values in accessor\_permit and accessor\_xpermit show the permissions assigned to Sales.

JohnDoe is found in accessor\_name[2]. The value in accessor\_operation[2], D, indicates that the entry for JohnDoe was removed from the ACL. The values in the corresponding positions in accessor\_permit and accessor\_xpermit identify the permissions previously assigned to JohnDoe.

Audit trail group objects are interpreted similarly. The values in the corresponding index positions in users\_names and users\_names\_operations represent one individual user who is a member of the audited group. The values in the corresponding positions in groups\_names and groups\_names\_operations represent one group that is a member of the audited group. The operations property defines what operation was performed on the member at the corresponding names property.



# Chapter 17

## Methods and jobs

### 17.1 Methods

Methods are executable programs that are represented by method objects in the repository. The program can be a Docbasic script, a Java method, or a program written in another programming language such as C++. The associated method object has properties that identify the executable and define command line arguments, and the execution parameters.

Methods are executed by issuing a DO\_METHOD administration method from the command line or using a job. Using a DO\_METHOD allows you to execute the method on demand. Using a job allows you to schedule the method for regular, automatic execution. “[Jobs](#)” on page 352 contains more information on creating jobs.

The executable invoked by the method can be stored in the file system or as content of the method object. If the method is executed by the Java method server, the entire custom or xml app JAR must be stored in the \$DM\_JMS\_HOME/webapps/DmMethods/WEB-INF/lib directory. For workflow methods, the .jar files must be placed under the Process Engine deployment in the \$DM\_JMS\_HOME/webapps/bpm/WEB-INF/lib directory.

By default, all repositories contain methods used by Documentum CM Server. All methods with object names that begin with dm\_ are default methods.

#### 17.1.1 Creating or modifying methods

The executable invoked by the method can be stored in an external file or as content of the method object. All other programs, except Java programs, are stored on the Documentum CM Server file system or in the repository as the content of the method object.

If the program is a Java method and you want to execute it using the Java method server, install the method on host file system of the application server. Only the application server instance installed during Documentum CM Server installation can execute Java methods. Do not store the program in the repository as the content of the method object.

Creating methods requires superuser privileges.

**Table 17-1: Method Info tab properties**

Field	Description
<b>Name</b>	<p>The method name.</p> <p>Do not use the format dm_&lt;methodname&gt; to name the method. This naming convention is reserved for default OpenText Documentum CM objects.</p>
<b>Verb</b>	<p>The method verb, including arguments.</p> <p>The method verb is the command-line name of the procedure or the name of the interpretive language that executes the program file.</p> <p>You can specify a full path, a relative path, or no path for the method verb. If you do not specify a path, the server searches the directories in the search path of the user.</p> <p>To store the program as the content of the method object, you must import the content after you created the method.</p>
<b>Method Type</b>	<p>Specifies the programming language of the method. Valid values are:</p> <ul style="list-style-type: none"> <li>• <i>dmbasic</i>: The method is written in Docbasic.</li> <li>• <i>dmawk</i>: The method is written in dmawk.</li> <li>• <i>java</i>: The method is written in Java and executed on the Java Method Server.</li> <li>• <i>program</i>: The method is writing in a programming language, such as C or C++.</li> </ul> <p>If the method is executed using Documentum CM Server or the dmbasic method server, and the executable is stored as content for the method, setting the method type to dmawk or dmbasic, directs the server to add -f in front of the filename. The server pass all arguments specified on the DO_METHOD command line to the program.</p>
<b>Arguments</b>	Specifies method arguments. Click <b>Edit</b> to add arguments.
<b>Method Success Codes</b>	Specifies method success codes. Click <b>Edit</b> to add success codes.

Field	Description
<b>Method Success Status</b>	Specifies the valid value for current status in the completed job. If this option is selected, the current status property value of the job must match the success status value after the job completes. The property is ignored if the option is not selected.
<b>Timeout Minimum</b>	The minimum timeout that can be specified on the command line for this procedure. The minimum timeout value cannot be greater than the default value specified in the timeout default field.
<b>Timeout Default</b>	<p>The default timeout value for the procedure. The system uses the default timeout value if no other time-out is specified on the command line.</p> <p>The default timeout value is 60 seconds and cannot be greater than the value specified in the timeout maximum field.</p>
<b>Timeout Maximum</b>	The maximum timeout that can be specified on the command line for this procedure. The default is 300 seconds.
<b>Launch Direct</b>	Specifies whether the program is executed by the system call or exec API call. When the launch direct option is selected, the server uses the exec call to execute the procedure. In this case, the method verb must be a fully qualified path name.
<b>Launch Asynchronously</b>	<p>Specifies whether the server runs the method asynchronously or not.</p> <p>If this option is selected and the method is launched on the application server, setting SAVE_RESPONSE on to TRUE on the command line is ignored.</p> <p>If this option is selected and the method is launched on the method server or Documentum CM Server and SAVE_RESULTS is set to TRUE on the command line, the method is always launched synchronously.</p>

Field	Description
<b>Run As Owner</b>	Specifies whether to run method to run as the installation owner account, with the privileges of the installation owner. If this option is not selected, the method runs with the privileges of the method user.  This option must be selected to execute a method on the method server or application server.
<b>Trace Launch</b>	Specifies whether to save internal trace messages generated by the method to the session log.
<b>Use Method Server</b>	Specifies whether to use the dmbasic method server or Java method server to execute a dmbasic or Java method.
<b>Restartable</b>	Specifies whether the method can be restarted, if the Java Method Server crashes or fails to respond.  This option is only available for non-system Java methods.
<b>Failover Awareness</b>	Specifies whether the method is enabled for failover, if the server is associated with more than one Java Method Server.  This option can only be configured for non-system Java methods.

**Table 17-2: SysObject Info tab properties**

Field	Description
<b>Title</b>	A descriptive title for the method.
<b>Subject</b>	A subject associated with the method.
<b>Keywords</b>	One or more keywords that describe the method. Click <b>Edit</b> to add keywords.
<b>Authors</b>	One or more method authors. Click <b>Edit</b> to add authors.
<b>Owner Name</b>	The name of the method owner. Click <b>Edit</b> to select a different owner.
<b>Version Label</b>	The current version label of the method. Click <b>Edit</b> to change the version label.
<b>Checkout Date</b>	The date when the method was checked out last.
<b>Checked Out by</b>	The name of the user who checked out the method.

Field	Description
<b>Created</b>	The date and time when the method was created.
<b>Creator Name</b>	The name of the user who created the method.
<b>Modified</b>	The date and time when the method was last modified.
<b>Modified By</b>	The name of the user who last modified the method.
<b>Accessed</b>	The time and date when the method was last accessed.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on creating or modifying methods.

### 17.1.2 Importing method content

If the program that a method is running is a script that requires an interpretive language to run it, store the program as the content of the associated method object.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on importing method content.

### 17.1.3 Running methods

You can manually run a method. To run the method periodically, create a job to execute the method on a schedule.

If you run a default OpenText Documentum CM method from the Run Method page, select **Run as server** unless you are logged in as the installation owner.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running methods.

### 17.1.4 Viewing the results of a method

The results of a method are displayed only after you run a method from Documentum Administrator.

After you run the method, the following method results appear:

- The result returned, if any
- Any document IDs that result
- The process ID
- Whether the method launched successfully

- The return value, if any
- Whether there were errors on the operating system from running the method
- Whether the method timed out
- The method timeout length

Click **OK** to exit the results page and return to the Methods list page.

### 17.1.5 Exporting method content

You can view a script imported into a method object.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on exporting method content.

### 17.1.6 Editing method content

You can edit the content of a method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on editing method content.

### 17.1.7 Checking in method content

You see this page only when you check in a checked-out script that is method content.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on checking in method content.

### 17.1.8 Deleting methods

You can delete a method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on deleting methods.

## 17.2 Method execution agents

The execution agents are the server processes that execute methods. There are three execution agents:

- The dmbasic method server

The dmbasic method server is a separate process that is installed with Documentum CM Server and resides on the same host. It is enabled by default. After it is started, it runs continuously. The method server uses connection pooling, regardless of whether connection pooling is enabled for the Documentum CM Server.

The dmbasic method server uses a method execution queue to manage methods submitted for execution. When you direct a method to the method server, Documentum CM Server places a method execution request on the bottom of the method execution queue. The method server reads the queue and executes the request at the top of the queue. The method server has a configurable number of worker threads to execute requests. The maximum number of requests the queue can contain is the number of threads times 100. For example, if the method server is configured to use 5 threads, then the method execution queue can contain 250 requests.

- Java method server

The Java method server is a third-party application server, installed as a component of Documentum CM Server installation. “[Java Method Servers](#)” on page 125 contains more information about the Java method server.

- Documentum CM Server

The Documentum CM Server is the default execution agent for a method if the method is not configured to execute on the method server or Java method server.

## 17.3 Administration methods

Administration methods are methods that perform a variety of administrative and monitoring tasks, in categories such as process management, content storage management, full-text indexing, and database methods. Use Documentum Administrator to execute the administration methods interactively.

### 17.3.1 Viewing administration methods

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing a list of administration methods.

### 17.3.2 Running administration methods

This section contains information on the method, including the permissions you must have to run it, the method arguments, and the results it returns.

The following sections provide more information about content methods:

- “[CAN\\_FETCH](#)” on page 331
- “[CLEAN\\_LINKS](#)” on page 331
- “[DELETE\\_REPLICA](#)” on page 331
- “[DESTROY\\_CONTENT](#)” on page 331
- “[EXPORT\\_TICKET\\_KEY](#)” on page 332
- “[GET\\_PATH](#)” on page 332
- “[IMPORT\\_REPLICA](#)” on page 332

- “[IMPORT\\_TICKET\\_KEY](#)” on page 332
- “[MIGRATE\\_CONTENT](#)” on page 333
- “[PURGE\\_CONTENT](#)” on page 338
- “[REPLICATE](#)” on page 339
- “[RESTORE\\_CONTENT](#)” on page 339
- “[SET\\_STORAGE\\_STATE](#)” on page 340

The following sections provide more information about database methods:

- “[DB\\_STATS](#)” on page 340
- “[DROP\\_INDEX](#)” on page 341
- “[EXEC\\_SQL](#)” on page 341
- “[FINISH\\_INDEX\\_MOVES](#)” on page 341
- “[GENERATE\\_PARTITION\\_SCHEME\\_SQL](#)” on page 342
- “[MAKE\\_INDEX](#)” on page 345
- “[MOVE\\_INDEX](#)” on page 345

The following sections provide more information about full-text indexing methods:

- “[ESTIMATE\\_SEARCH](#)” on page 345
- “[MARK\\_FOR\\_RETRY](#)” on page 346
- “[MODIFY\\_TRACE](#)” on page 346

The following sections provide more information about trace methods:

- “[GET\\_LAST\\_SQL](#)” on page 347
- “[MODIFY\\_TRACE](#)” on page 346
- “[LIST\\_RESOURCES](#)” on page 347
- “[LIST\\_TARGETS](#)” on page 347
- “[SET\\_OPTIONS](#)” on page 347

The following section provides more information about the workflow method:

- “[RECOVER\\_AUTO\\_TASKS](#)” on page 349
- “[WORKFLOW\\_AGENT\\_MANAGEMENT](#)” on page 349

### 17.3.2.1 CAN\_FETCH

Any user can run the CAN\_FETCH administration method to determine whether the server can fetch a specified content file.

CAN\_FETCH returns TRUE if the fetch is possible or FALSE if it is not.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the CAN\_FETCH administration method.

### 17.3.2.2 CLEAN\_LINKS

The CLEAN\_LINKS administration method removes linked\_store links not associated with sessions, unnecessary dmi\_linkrecord objects, and auxiliary directories.

CLEAN\_LINKS returns TRUE if the operation succeeds or FALSE if it fails.

You must have superuser privileges to run CLEAN\_LINKS.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the CLEAN\_LINKS administration method.

### 17.3.2.3 DELETE\_REPLICA

The DELETE\_REPLICA administration method removes a content file from a component area of a distributed storage area.

DELETE\_REPLICA returns TRUE if the operation succeeds or FALSE if it fails.

You must have superuser privileges to run DELETE\_REPLICA.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the DELETE\_REPLICA administration method.

### 17.3.2.4 DESTROY\_CONTENT

The DESTROY\_CONTENT method removes content objects from the repository and their associated content files from storage areas.

DESTROY\_CONTENT returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator or superuser privileges to run DESTROY\_CONTENT.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the DESTROY\_CONTENT administration method.

### **17.3.2.5 EXPORT\_TICKET\_KEY**

The EXPORT\_TICKET\_KEY administration method encrypts and exports a login ticket from the repository to a client machine.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the EXPORT\_TICKET\_KEY administration method.

### **17.3.2.6 GET\_PATH**

The GET\_PATH administration method returns the directory location of a content file stored in a distributed storage area.

Any user can run GET\_PATH.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the GET\_PATH administration method.

### **17.3.2.7 IMPORT\_REPLICA**

The IMPORT\_REPLICA administration method imports files from one distributed storage area into another distributed storage area.

The IMPORT\_REPLICA method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator or superuser privileges to use the IMPORT\_REPLICA method.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the IMPORT\_REPLICA administration method.

### **17.3.2.8 IMPORT\_TICKET\_KEY**

The IMPORT\_TICKET\_KEY administration method decrypts a login ticket from a client machine and imports the ticket into the repository.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the IMPORT\_TICKET\_KEY administration method.

### 17.3.2.9 MIGRATE\_CONTENT

The MIGRATE\_CONTENT administration method migrates content files from one storage area to another.

The MIGRATE\_CONTENT method requires superuser privileges to migrate:

- Single content objects.
- Single SysObject.
- Sets of content objects qualified by a DQL predicate against dmr\_content.
- Set of content objects qualified by a DQL predicate against dm\_sysobject or its subtypes.
- All content in a file store.

Use the MIGRATE\_CONTENT administration method to move content from file stores, retention type stores, blob stores, and distributed stores to file stores, retention type stores, and distributed stores. Documentum Administrator 6.5 SP2 and later supports migration from external stores. You cannot move files to a blob store. The storage areas can be online, offline, or read-only.

Before running MIGRATE\_CONTENT:

- Make sure that all objects to be migrated are checked in to the repository. If you migrate any checked-out objects, check-in fails because of mismatched versions.
- Make sure that the file store to which you migrate objects has sufficient disk space for the migration.
- Before you migrate a file store, use the SET\_STORAGE\_STATE administration method to mark it READ-ONLY. If the source file store has associated full-text indexes, the target file store must also have full-text indexes. Documentum Administrator does not allow you to select a target file store without full-text indexes.

The MIGRATE\_CONTENT method returns an integer indicating the number of objects migrated successfully.

Regardless of the mode in which MIGRATE\_CONTENT is run, the original content file can be removed or left in the source file store. If you do not have the file removed, you must specify the path to a log file that logs the path of the source content file. Those files can be removed at another time using Dmfilescan.



#### Notes

- For a read-only filestore, when you use MIGRATE\_CONTENT with the remove\_original parameter set to <TRUE>, the migration fails because the method is unable to remove the content from the SOURCE filestore. You must make the storage area online for a successful migration.
- The ALL VERSIONS option is supported for the migrate content (MIGRATE\_CONTENT) job. When ALL VERSIONS=true, all versions of the

object are migrated from the source store to the target file store. When **ALL VERSIONS=false**, only the current version of the object is migrated. If you do not specify, it defaults to false.

**Table 17-3: Parameters for moving a single object**

Field	Description
<b>Migrate</b>	Select <b>A single object</b> from the drop-down list.
<b>Content</b>	<p>Click <b>Select Object</b>, then select an object type from the <b>Select From</b> drop-down list.</p> <p>Specify a limiting <b>Where</b> clause, or leave the <b>Where</b> field blank to select from all objects in the repository. To display all object versions, select the <b>Use all versions</b> checkbox and then click <b>Go</b>.</p> <p>Select the objects to migrate and click <b>Add</b>.</p> <p>Select <b>Remove the original source</b> to remove the original content file. The <b>Remove the original source</b> option cannot be edited, if the selected object belongs to an external store.</p>
<b>Path</b>	Click <b>Select Path</b> and select a location on the server file system for the log file path.
<b>Target</b>	Select a target file store from the drop-down list.
<b>Source Direct Access</b>	<p>Specifies whether the content files in the source store can be directly accessed through a full file path.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Migrate With</b>	<p>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>

Field	Description
<b>Update Only</b>	This option is used only in conjunction with the Direct Copy or Direct Move option. When selected, move or copy commands are written to the log file specified in the <b>Command File Name</b> field.  This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.
<b>Command File Name</b>	A string that specifies a file path to a log file.  This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store and if the <b>Update Only</b> option is selected.

**Table 17-4: Parameters for moving all content in a store**

Field	Description
<b>Migrate</b>	Select <b>All content in a filestore</b> from the drop-down list.
<b>Source</b>	Select a source file store from the <b>Source</b> drop-down list.  Select <b>Remove the original source</b> to remove the original content file. The <b>Remove the original source</b> option cannot be edited, if the selected object belongs to an external store.
<b>Path</b>	Click <b>Select Path</b> and select a location on the server file system for the log file path
<b>Target</b>	Select a target file store from the drop-down list.
<b>Maximum</b>	Specifies the maximum number of objects to migrate.  The default is to migrate all objects.
<b>Batch Size</b>	Specifies the number of objects migrated in a single transaction.  The default value is 500. Multiple transactions are run until the maximum number of objects to migrate is reached.

Field	Description
<b>Content Migration Threads</b>	<p>Specifies the number of internal sessions used to execute the method.</p> <p>The default value is 0, indicating that the migration executes sequentially. The value cannot exceed the Maximum Content Migration Threads value in the server configuration object.</p> <p>This option is available with Content Storage Services on Documentum CM Server.</p>
<b>Source Direct Access</b>	<p>Specifies whether the content files in the source store can be directly accessed through a full file path.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Migrate With</b>	<p>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Update Only</b>	<p>This option is used only in conjunction with the Direct Copy or Direct Move option. When selected, move or copy commands are written to the log file specified in the <b>Command File Name</b> field.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Command File Name</b>	<p>A string that specifies a file path to a log file.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store and if the <b>Update Only</b> option is selected.</p>

**Table 17-5: Parameters for moving content selected by a query**

Field	Description
<b>Migrate</b>	Select All content satisfying a query from the drop-down list.

Field	Description
<b>Select Object Type to Migrate</b>	<p>Specify the object type to migrate.</p> <p>If you select <b>dm_sysobject or it's subtype</b>, click <b>Select</b> to access the Choose a type page to select a subtype of dm_sysobject.</p>
<b>Select r_object_id from dmr_content where</b>	<p>Specify the DQL query.</p> <p>Select <b>Remove the original source</b> to remove the original content file. The <b>Remove the original source</b> option cannot be edited, if the selected object belongs to an external store.</p>
<b>Path</b>	<p>Click <b>Select Path</b> and select a location on the server file system for the log file path</p>
<b>Target</b>	<p>Select a target file store from the drop-down list.</p>
<b>Maximum</b>	<p>Specifies the maximum number of objects to migrate.</p> <p>The default is to migrate all objects.</p>
<b>Batch Size</b>	<p>Specifies the number of objects migrated in a single transaction.</p> <p>The default value is 500. Multiple transactions are run until the maximum number of objects to migrate is reached.</p>
<b>Content Migration Threads</b>	<p>Specifies the number of internal sessions used to execute the method.</p> <p>The default value is 0, indicating that the migration executes sequentially. The value cannot exceed the Maximum Content Migration Threads value in the server configuration object.</p> <p>This option is available with Content Storage Services on Documentum CM Server.</p>
<b>Source Direct Access</b>	<p>Specifies whether the content files in the source store can be directly accessed through a full file path.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>

Field	Description
<b>Migrate With</b>	<p>Specifies whether the source content is copied or moved to the target store during migration. Direct Move is applicable to file stores only.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Update Only</b>	<p>This option is used only in conjunction with the Direct Copy or Direct Move option. When selected, move or copy commands are written to the log file specified in the <b>Command File Name</b> field.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store.</p>
<b>Command File Name</b>	<p>A string that specifies a file path to a log file.</p> <p>This option is only available if the <b>Source</b> is an external store and the <b>Target</b> is either a file store or a ca store and if the <b>Update Only</b> option is selected.</p>

If the MIGRATE\_CONTENT method fails with an error, the entire batch transaction is rolled back. If the destination has content files that were created from the successful migrations within the batch, you can clean up those files running the Dmfilescan job, as described in “[Dmfilescan](#)” on page 375.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on the following operations:

- Migrating a single object
- Migrating all content files in a file store
- Migrating objects selected by a query

#### 17.3.2.10 PURGE\_CONTENT

The PURGE\_CONTENT administration method marks a content file as offline and deletes the file from its storage area. The method does not back up the file before deleting it; make sure that you have archived the file before running PURGE\_CONTENT on it.

The PURGE\_CONTENT method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator or superuser privileges to use the PURGE\_CONTENT method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running the PURGE\_CONTENT administration method.

### 17.3.2.11 REPLICATE

The REPLICATE administration method copies content files from one component of a distributed storage area to another. This task is normally performed by the Content Replication tool or by the Surrogate Get feature. Use the REPLICATE administration method as a manual backup to Content Replication and Surrogate Get.

The REPLICATE method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator or superuser privileges to use the REPLICATE method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running the REPLICATE administration method.

### 17.3.2.12 RESTORE\_CONTENT

The RESTORE\_CONTENT administration method restores an offline content file to its original storage area. It operates on one file at a time. If you need to restore more than one file at a time, use the API Restore method.

You can use RESTORE\_CONTENT only when one server handles both data and content requests. If your configuration uses separate servers for data requests and content file requests, you must issue a Connect method that bypasses the Documentum CM Server to use RESTORE\_CONTENT in the session.

The RESTORE\_CONTENT method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator or superuser privileges to use the RESTORE\_CONTENT method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running the RESTORE\_CONTENT administration method.

### 17.3.2.13 SET\_STORAGE\_STATE

The SET\_STORAGE\_STATE administration method changes the state of a storage area. A storage area is in one of three states:

- On line  
An on-line storage area can be read and written to.
- Off line  
An off-line storage area cannot be read or written to.
- Read only  
A read-only storage area can be read, but not written to.

You can use SET\_STORAGE\_STATE only when one server handles both data and content requests. If your configuration uses separate servers for data requests and content file requests, you must issue a Connect method that bypasses the content file server to use SET\_STORAGE\_STATE in the session.

The SET\_STORAGE\_STATE method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator or superuser privileges to use the SET\_STORAGE\_STATE method.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the SET\_STORAGE\_CONTENT administration method.

### 17.3.2.14 DB\_STATS

The DB\_STATS administration method displays statistics about database operations for the current session. The statistics are counts of the numbers of:

- Inserts, updates, deletes, and selects executed
- Data definition statements executed
- RPC calls to the database
- Maximum number of cursors opened concurrently during the session

Any user can run the DB\_STATS method.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the DB\_STATS administration method.

### 17.3.2.15 **DROP\_INDEX**

The DROP\_INDEX administration method destroys a user-defined index on an object type. The DROP\_INDEX method returns TRUE if the operation succeeds or FALSE if it fails. You must have superuser privileges to run the DROP\_INDEX administration method.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the DROP\_INDEX administration method.

### 17.3.2.16 **EXEC\_SQL**

The EXEC\_SQL administration method executes SQL statements, with the exception of SQL Select statements.

The EXEC\_SQL method returns TRUE if the operation succeeds or FALSE if it fails.

You must have superuser privileges to run the EXEC\_SQL method.

Note the following restrictions on how the method works:

- If you use the Apply method to execute the method and the query contains commas, you must enclose the entire query in single quotes.
- In an EXECUTE statement, character-string literals must always be single-quoted.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the EXEC\_SQL administration method.

### 17.3.2.17 **FINISH\_INDEX\_MOVES**

The FINISH\_INDEX\_MOVES administration method completes unfinished object type index moves. The FINISH\_INDEX\_MOVES method returns TRUE if the operation succeeds or FALSE if it fails. You must have superuser privileges to run the FINISH\_INDEX\_MOVES administration method.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the FINISH\_INDEX\_MOVES administration method.

### 17.3.2.18 GENERATE\_PARTITION\_SCHEME\_SQL

The GENERATE\_PARTITION\_SCHEME\_SQL administration method is available to administrators and superusers. These additional restrictions apply:

- The method is available only on version 6.5 repositories.

Running the method generates a script, which can then be run to partition the repository. The GENERATE\_PARTITION\_SCHEME\_SQL administration method has three options:

- DB\_PARTITION (Database Partition)  
Generate a script to upgrade or convert a non-partitioned repository to a OpenText Documentum CM 6.5 partitioned repository.
- ADD\_PARTITION (Add Partition)  
Add a partition to a partitioned type.
- EXCHANGE\_PARTITION (Exchange Partition)  
Generate a script for bulk ingestion by loading data from an intermediate table into a new partition of a partitioned table.

**Table 17-6: GENERATE\_PARTITION\_SCHEME\_SQL parameters**

Parameter	Description
Operation	<p>Select an operation from the dropdown list box to define the subcommand. The options are:</p> <ul style="list-style-type: none"> <li>• <i>DB_PARTITION</i>: Generates a script to upgrade or convert a repository to a 6.5 partitioned repository. If selected: <ul style="list-style-type: none"> <li>– Select Partition Type or Table Name.</li> <li>– If Table Name is defined, optionally define the Owner Name.</li> <li>– Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</li> <li>– Last Partition and Last Tablespace are optional.</li> <li>– In the Partitions section, Partition Name, Range, and Tablespace are required.</li> </ul> </li> <li>• <i>ADD_PARTITION</i>: Generates a script to add a partition to a partitioned type. If selected: <ul style="list-style-type: none"> <li>– Select Partition Type or Table Name.</li> <li>– If Table Name is defined, optionally define the Owner Name.</li> <li>– Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</li> <li>– In the Partitions section, Partition Name, Range, and Tablespace are required.</li> </ul> </li> <li>• <i>EXCHANGE_PARTITION</i>: Generates a script for bulk ingestion by loading data from an intermediate table into a new partition of a partitioned table. If selected: <ul style="list-style-type: none"> <li>– Partition Type and Table Name are mutually exclusive.</li> <li>– If Table Name is defined, optionally define the Owner Name.</li> <li>– Include object type is optional. Select to apply the partition operation to the dmi_object_type table.</li> <li>– Partition Name, Range, and Tablespace are required.</li> <li>– Temp Table Suffix is optional.</li> </ul> </li> </ul>

Parameter	Description
Partition Type	Select a partition type from the dropdown list box, which displays a list of the partition types available for the repository. <i>All</i> is the default for DB_PARTITION and ADD_PARTITION, but is not available for EXCHANGE_PARTITION. If you select Partition Type, then you cannot select Table Name.
Table Name	Type a table name. If you select Table Name, then you cannot select Partition Type.
Include object type	Optionally, select to apply the partition operation to the dmi_object_type table.
Owner Name	Type an owner name. This field is enabled only if Table Name is selected.
Last Partition	Optionally, type a name for the last partition. This field appears only when DB_PARTITION is selected as the operation.
Last Tablespace	Optionally, type a tablespace name for the last partition. This field appears only when DB_PARTITION is selected as the operation.
Partition Name	Type a name for the partition. For DB_PARTITION and ADD_PARTITION operations, you must first click <b>Add</b> in the <b>Partitions</b> section to add information for each partition.
Range	Type the upper limit for the partition key range. For DB_PARTITION and ADD_PARTITION operations, you must first click <b>Add</b> in the <b>Partitions</b> section to add information for each partition.
Tablespace	Type the partition tablespace name. If not specified, the default tablespace is used. For DB_PARTITION and ADD_PARTITION operations, you must first click <b>Add</b> in the <b>Partitions</b> section to add information for each partition.
Temp Table Suffix	Type a temporary table suffix. This field is enabled and optional only if EXCHANGE_PARTITION is selected as the operation.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the GENERATE\_PARTITION\_SCHEME\_SQL administration method.

### 17.3.2.19 MAKE\_INDEX

The MAKE\_INDEX administration method creates an index for any persistent object type. You can specify one or more properties on which to build the index. If you specify multiple properties, you must specify all single-valued properties or all repeating properties. Also, if you specify multiple properties, the sort order within the index corresponds to the order in which the properties are specified in the statement. You can also set an option to create a global index.

If the MAKE\_INDEX method succeeds, it returns the object ID of the dmi\_index object for the new index. If the method fails, MAKE\_INDEX returns F. If the specified index already exists, the method returns 0000000000000000.

You must have superuser privileges to run the MAKE\_INDEX administration method. To run an index space query, you must have sufficient privileges in the database.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the MAKE\_INDEX administration method.

### 17.3.2.20 MOVE\_INDEX

The MOVE\_INDEX administration method moves an existing object type index from one tablespace or segment to another. The MOVE\_INDEX method returns TRUE if the operation succeeds or FALSE if it fails. You must have system administrator or superuser privileges to run the MOVE\_INDEX administration method.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the MOVE\_INDEX administration method.

### 17.3.2.21 ESTIMATE\_SEARCH

The ESTIMATE\_SEARCH administration method returns the number of results matching a particular full-text search condition.

ESTIMATE\_SEARCH returns one of the following:

- The exact number of matches that satisfy the SEARCH condition, if the user running the method is a superuser or there are more than 25 matches.
- The number 25 if there are 0-25 matches and the user running the method is not a superuser.
- The number -1 if there is an error during execution of the method.

Errors are logged in the session log file.

Any user can execute this method. However, the permission level of user affects the return value. The ESTIMATE\_SEARCH administration method is not available, if the connected repository is configured with the xPlore search engine.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running the ESTIMATE\_SEARCH administration method.

### **17.3.2.22 MARK\_FOR\_RETRY**

The MARK\_FOR\_RETRY administration method finds content that has a particular negative update\_count property value and marks such content as awaiting indexing. Use MARK\_FOR\_RETRY at any time to mark content that failed indexing for retry. Note that MARK\_FOR\_RETRY does not take the update\_count argument.

When the UPDATE\_FTINDEX method fails, it changes the update\_count property for the content object associated with the bad content to the negative complement of the update\_count value in the fulltext index object. For example, if the update\_count of the full-text index object is 5, the update\_count property of the bad content object is set to -5 (negative 5). *OpenText Documentum Content Management - Server DQL Reference Guide* (EDCCS250400-DRD) contains more information.

The MARK\_FOR\_RETRY method returns TRUE if the operation succeeds or FALSE if it fails.

You must have system administrator or superuser privileges to run the MARK\_FOR\_RETRY administration method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running the MARK\_FOR\_RETRY administration method.

### **17.3.2.23 MODIFY\_TRACE**

The MODIFY\_TRACE administration method turns tracing on and off for full-text indexing operations. The MODIFY\_TRACE method returns TRUE if the operation succeeds or FALSE if it fails. You must have system administrator or superuser privileges to run the MODIFY\_TRACE administration method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running the MODIFY\_TRACE administration method.

#### 17.3.2.24 GET\_LAST\_SQL

The GET\_LAST\_SQL administration method retrieves the SQL translation of the last DQL statement issued. Any user can run GET\_LAST\_SQL.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the GET\_LAST\_SQL administration method.

#### 17.3.2.25 LIST\_RESOURCES

The LIST\_RESOURCES administration method lists information about the server and the operating system environment of server. You must have system administrator or superuser privileges to run the LIST\_RESOURCES administration method.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the LIST\_RESOURCES administration method.

#### 17.3.2.26 LIST\_TARGETS

The LIST\_TARGETS administration method lists the connection brokers to which the server is currently projecting. Additionally, it displays the projection port, proximity value, and connection broker status for each connection broker, as well as whether the connection broker is set (in server.ini or the server configuration object). Any user can run LIST\_TARGETS.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the LIST\_TARGETS administration method.

#### 17.3.2.27 SET\_OPTIONS

The SET\_OPTIONS administration method turns tracing options on or off. You can set the following options:

Option	Action
clean	Removes the files from the server common area.
crypto_trace	Cryptography information.
debug	Traces session shutdown, change check, launch and fork information.
docbroker_trace	Traces connection broker information.

Option	Action
i18n_trace	<p>Traces client session locale and codepage. An entry is logged identifying the session locale and client code page whenever a session is started.</p> <p>An entry is also logged if the locale or code page is changed during the session.</p>
last_sql_trace	<p>Traces the SQL translation of the last DQL statement issued before access violation and exception errors.</p> <p>If an error occurs, the last_sql_trace option causes the server to log the last SQL statement that was issued prior to the error. This tracing option is enabled by default.</p> <p>It is strongly recommended that you do not turn off this option. It provides valuable information to OpenText Global Technical Services if it ever necessary to contact them.</p>
lock_trace	Traces Windows locking information.
net_ip_addr	Traces the IP addresses of client and server for authentication.
nettrace	Turns on RPC tracing. Traces Netwise calls, SSL, connection ID, client host address, and client hostname.
sql_trace	SQL commands sent to the underlying RDBMS for subsequent sessions, including the repository session ID and the database connection ID for each SQL statement.
trace_authentication	Traces detailed authentication information.
trace_complete_launch	Traces Linux process launch information.
trace_method_server	Traces the operations of the method server.

The SET\_OPTIONS method returns TRUE if the operation succeeds or FALSE if it fails. You must have system administrator or superuser privileges to run the SET\_OPTIONS administration method.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running the SET\_OPTIONS administration method.

### 17.3.2.28 RECOVER\_AUTO\_TASKS

Run the RECOVER\_AUTO\_TASKS administration method to recover workflow tasks that have been claimed, but not yet processed by a workflow agent associated with a failed Documentum CM Server.

If a Documentum CM Server fails, its workflow agent is also stopped. When the server is restarted, the workflow agent recognizes and processes any work items it had claimed but not processed before the failure. However, if you cannot restart the Documentum CM Server that failed, you must recover those work items already claimed by its associated workflow agent so that another workflow agent can process them. The RECOVER\_AUTO\_TASKS administration method performs that recovery.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the RECOVER\_AUTO\_TASKS administration method.

### 17.3.2.29 WORKFLOW\_AGENT\_MANAGEMENT

Run the WORKFLOW\_AGENT\_MANAGEMENT method to start and shut down a workflow agent.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running the WORKFLOW\_AGENT\_MANAGEMENT administration method.

If the workflow agent startup or shutdown process fails, the Administration Method Results page displays an error message indicating the process failure and provides additional information. There several reasons why a workflow agent startup or shutdown process can fail:

- The network is down.
- The Documentum CM Server containing the workflow agent is down.
- The Documentum CM Server projects to a connection broker that is not listed in the dfc.properties of the client running Documentum Administrator.

If the repository is not reachable, the Parameters page displays the Workflow Agent Current Status as *Unknown*.

### 17.3.2.30 REGEN\_EXPRESSIONS

By default, dmbasic expression generates the INTEGER data type. Use the following procedure to convert INTEGER to LONG:

1. Create an environmental variable at the Documentum CM Server host: DM\_DOCBASIC\_COND\_EXPR\_DATA\_TYPE
2. Set the value for the variable to LONG (all uppercase).
3. Restart the repository to fetch the new variable.
4. Run the following dmbasic command:

For Windows:

```
dmbasic -f %DM_HOME%\install\admin\dm_recreate_expr.ebs  
-e Recreate -- <repository> <username> <password> all
```

For Linux:

```
dmbasic -f $DM_HOME/install/admin/dm_recreate_expr.ebs  
-e Recreate -- <repository> <username> <password> all
```

To generate LONG data type for dmscript of a particular activity, use the following IAPI command:

```
apply,c,<activity_id>,REGEN_EXPRESSIONS
```

### 17.3.2.31 Administration Methods Results Page

This page displays the results of running an administration method. For information on the results, click the method name.

The following are content methods:

- “CAN\_FETCH” on page 331
- “CLEAN\_LINKS” on page 331
- “DELETE\_REPLICA” on page 331
- “DESTROY\_CONTENT” on page 331
- “EXPORT\_TICKET\_KEY” on page 332
- “GET\_PATH” on page 332
- “IMPORT\_REPLICA” on page 332
- “IMPORT\_TICKET\_KEY” on page 332
- “MIGRATE\_CONTENT” on page 333
- “PURGE\_CONTENT” on page 338
- “REPLICATE” on page 339
- “RESTORE\_CONTENT” on page 339

- “[SET\\_STORAGE\\_STATE](#)” on page 340

The following are database methods:

- “[DB\\_STATS](#)” on page 340
- “[EXEC\\_SQL](#)” on page 341
- “[MAKE\\_INDEX](#)” on page 345
- “[DROP\\_INDEX](#)” on page 341
- “[MOVE\\_INDEX](#)” on page 345
- “[FINISH\\_INDEX\\_MOVES](#)” on page 341

The following are full-text indexing methods:

- “[ESTIMATE\\_SEARCH](#)” on page 345
- “[MARK\\_FOR\\_RETRY](#)” on page 346
- “[MODIFY\\_TRACE](#)” on page 346

The following are trace methods:

- “[GET\\_LAST\\_SQL](#)” on page 347
- “[LIST\\_RESOURCES](#)” on page 347
- “[LIST\\_TARGETS](#)” on page 347
- “[MODIFY\\_TRACE](#)” on page 346
- “[SET\\_OPTIONS](#)” on page 347

The following are workflow methods:

- “[RECOVER\\_AUTO\\_TASKS](#)” on page 349
- “[WORKFLOW\\_AGENT\\_MANAGEMENT](#)” on page 349
- “[REGEN\\_EXPRESSIONS](#)” on page 350

### 17.3.2.32 Choosing a file on the server file system

This section describes how to choose a file on the server file system.

#### To choose a file on the server file system:

1. Navigate to the correct location on the file system.
2. Select the file.
3. Click **OK** to return to the Parameters page.

## 17.4 Jobs

Jobs are repository objects that automate method object execution. Methods associated with jobs are executed automatically on a user-defined schedule. The properties of a job define the execution schedule and turn execution on or off. Jobs are invoked by the agent exec process, a process installed with Documentum CM Server. At regular intervals, the agent exec process examines the job objects in the repository and runs those jobs that are ready for execution. Any user can create jobs.

When a repository is created, it contains jobs for:

- CA Store (Centera and NetApp SnapLock stores)
- Content
- Data Dictionary
- Distributed Content
- Repository
- Federation
- Fulltext
- Other
- Replication
- Workflow

You can create additional jobs to automate the execution of any method and you can modify the schedule for executing existing jobs.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains more information on federation and replication jobs.

### 17.4.1 Job descriptions

The following sections describes jobs that are automatically created with each repository. The descriptions of the jobs discusses the arguments that can be modified for each job.

#### 17.4.1.1 ACL replication (dm\_ACLReplication)

The ACL Replication job first sets external ACLs for replication within a repository federation and then launches ACL (permission set) replication. It is installed in an inactive state. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the information on replication and replication jobs.

#### 17.4.1.2 ACL replication (dm\_ACLRepl\_repository)

The dm\_ACLRepl\_job replicates ACLs to repositories in a federation. There is one job for each member repository, and *repository* is the first 19 bytes of the name of repository. It is an internal template job that is installed in an inactive state. Do not edit or remove this job. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the information on replication and replication jobs.

#### 17.4.1.3 Asynchronous write (dm\_AsyncronousWrite)

When users import documents in asynchronous mode, there may be instances where some or all content may not be immediately replicated from Branch Office Caching Services to Accelerated Content Services. This might happen if the Messaging Service server was not available or there were network issues between Branch Office Caching Services, Messaging Service, and/or Accelerated Content Services.

The Asynchronous Write job polls for content still in a parked state and generates new messages for the Messaging Service server to pass to Branch Office Caching Services to request the upload of the parked content. After execution, the job lists all content objects that had yet to be moved from the parked state and for which messages were sent to the Messaging Service server. If a Branch Office Caching Services server receives a request to migrate content that is has already processed, it will ignore the request.

This job is inactive by default, but should be enabled whenever asynchronous mode is allowed. The job is scheduled to run daily at 2:00 a.m. by default.

#### 17.4.1.4 Audit management

The Audit Management tool deletes audit trail entries. When an audited event occurs, an audit trail entry is created for that event. If the audit trail entries are not removed periodically, the tables for the dm\_audittrail object type can grow quite large, and performance degrades when audited events occur. The Audit Management tool automates the task of removing unneeded audit trail objects.

The tool runs under the OpenText Documentum CM installation owner account to execute the dm\_AuditMgt job. The job uses the PURGE\_AUDIT administration method to remove the audit trail entries from the repository. Consequently, to use this tool, the OpenText Documentum CM installation owner must have Purge Audit privileges. All executions of the tool are audited. The generated audit trail entry has the event name dm\_purgeaudit.

The cutoff\_days and custom\_predicate arguments determine which audit trail objects to remove. The cutoff\_days argument specifies the age of the objects to delete. The custom\_predicate argument is then applied to those items meeting the age requirement.

By default, the cutoff\_days argument is set to 90 and the custom\_predicate argument is set to remove only audit trail objects generated by system-defined events. (The tool does not delete audit trail objects generated by user-defined events by default.)

To change the age cutoff, reset the cutoff\_days argument.

To choose the objects to remove from the subset selected by cutoff\_days, change the custom\_predicate argument. By default, the custom predicate includes three conditions:

- delete\_flag=TRUE
- dequeued\_date=*value* (*value* is computed using the cutoff\_days argument)
- r\_gen\_source=1

You cannot change the first two conditions. The third condition, r\_gen\_source=1, directs the server to delete only audit trail objects generated by system-defined events. If you want to remove only audit trail objects generated by user-defined events, reset this to r\_gen\_source=0. If you want to remove audit trail objects generated by both system- and user-defined events, remove the r\_gen\_source expression from the custom predicate.

You may also add other conditions to the default custom predicate. If you add a condition that specifies a string constant as a value, you must enclose the value in two single quotes on each side. For example, suppose you want to remove only audit trail entries that record dm\_checkin events. To do so, add the following to the custom\_predicate:

```
event_name='dm_checkin'
```

dm\_checkin is enclosed by two single quotes on each side. Do not use double quotes. These must be two single quotes.

The Audit Management tool generates a status report that lists the deleted dm\_audittrail entries. The report is saved in the repository in /System/Sysadmin/Reports.

If an error occurs while the tool is executing, the server sends email and inbox notification to the user specified by the -auditperson argument.

The Audit Management tool is installed in the inactive state. The first time you execute the tool, it may take a long time to complete.

#### 17.4.1.4.1 Arguments

[“Audit management arguments” on page 355](#), lists the arguments to the Audit Management tool.

**Table 17-7: Audit management arguments**

Argument	Datatype	Default	Description
-window_interval	integer	120	Defines the execution window for the tool. Value is interpreted in minutes.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-custom_predicate <i>qualification</i>	string	-	A WHERE clause <i>qualification</i> for the query that selects audit trail entries for deletion.  The qualification must be a valid qualification and can reference only audit trail object type properties. For example, a valid qualification is event='approved' or name='dmadmin'. Refer to the general discussion of the tool for details of setting this argument.  The <i>OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)</i> for complete information about WHERE clause qualifications.

Argument	Datatype	Default	Description
-cutoff_days	<i>integer</i>	90	A minimum age, in days, for objects to delete. All audit trail objects older than the specified number of days and that meet the specified qualification are deleted.  To delete all audit trail objects, set this value to zero (0).

#### 17.4.1.4.2 Guidelines

Audit trail entries are the result of audited events. The more events you audit, the more audit trail entries are generated in a fixed period of time.

You must decide if there are any reasons to keep or maintain audit trail entries. For example, you may want to keep certain items for traceability purposes. If so, leave this tool inactive or set the cutoff\_days argument to a value that will save the audit trail items for a specified length of time.

After you have made your decisions, formulate a scheduling plan.

If you do not supply a value for custom\_predicate or cutoff\_days, all system-generated dm\_audittrail entries older than 90 days are deleted.

#### 17.4.1.4.3 Report sample

Here is a sample of the report generated by the Audit Management Tool.

```
AuditMgt Report For repository BLD9A As Of 10/19/98 12:26:31 PM
```

```
Parameters for removing audit trail items:
```

```
-----  
- No items audited before 90 days will be removed...  
- There is no custom predicate...
```

```
Looking for audit trail items to delete...  
Destroying audit trail item with ID 5f00010080000124  
Destroying audit trail item with ID 5f00010080000125  
Destroying audit trail item with ID 5f00010080000126  
Destroying audit trail item with ID 5f00010080000127  
Destroying audit trail item with ID 5f00010080000128  
Destroying audit trail item with ID 5f00010080000129  
Destroying audit trail item with ID 5f0001008000012a  
Destroying audit trail item with ID 5f0001008000012d  
Destroying audit trail item with ID 5f0001008000012e  
Destroying audit trail item with ID 5f0001008000012f  
Destroying audit trail item with ID 5f00010080000130  
Destroying audit trail item with ID 5f00010080000131  
Destroying audit trail item with ID 5f00010080000132  
Destroying audit trail item with ID 5f00010080000133  
Destroying audit trail item with ID 5f00010080000134  
Destroying audit trail item with ID 5f00010080000135
```

```

Destroying audit trail item with ID 5f00010080000136
Destroying audit trail item with ID 5f00010080000137
18 audit trail items deleted...

End of Audit Trail Management Report
Report End 10/19/98 12:26:33 PM

```

### 17.4.1.5 Consistency checker

The Consistency Checker tool scans the repository and reports any inconsistencies such as type or object corruption, objects that reference a user, group, or other object that is nonexistent in the repository and so forth. The tool does not attempt to fix any of the inconsistencies. Contact OpenText Global Technical Services for assistance in correcting errors in your repository found by the consistency checker.

[“Consistency checks” on page 647](#), lists the consistency checks conducted by the tool and the error number assigned to each.

The job generates a report that lists the categories checked and any inconsistencies found. The report is saved to the repository in /System/Sysadmin/Reports/ConsistencyChecker. If no errors are found, the current report overwrites the previous report. If an error is found, the current report is saved as a new version of the previous report.

It is recommended that you run this tool on a repository before upgrading the repository to a new version of the Documentum CM Server.

The Consistency Checker job is active by default, running once a day.

#### 17.4.1.5.1 Running the job from a command line

The Consistency Checker job is implemented as a script called consistency\_checker.ebs. You can run the script manually, from the operating system prompt. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point --repository_name superuser password
```

*repository\_name* is the name of the repository against which you are running the consistency checker, *superuser* is the user name of a repository superuser, and *password* is the password for the account of superuser.

When you run the consistency checker from the command line, the results of the checks are directed to standard output.

#### 17.4.1.5.2 Arguments

The Consistency Checker job has no arguments.

#### 17.4.1.5.3 Report sample

Here is a sample of a Consistency Checker report. This run of the tool found X inconsistencies.

```
Beginning Consistency Checks.....  
  
Repository Name: buzzard  
Server Version: 5.1.0.63 Win32.SQLServer  
Database: SQLServer  
  
#####  
##  
## CONSISTENCY_CHECK: Users & Groups  
##  
##      Start Time: 09-10-2002 10:15:55  
##  
##  
#####  
  
Checking for users with non-existent group  
  WARNING CC-0001: User 'docu' belongs to  
non-existent group ''  
  WARNING CC-0001: User 'engr' belongs to  
non-existent group ''  
  WARNING CC-0001: User 'marketing' belongs to  
non-existent group ''  
  WARNING CC-0001: User 'nagboat' belongs to  
non-existent group ''  
  WARNING CC-0001: User 'admingroup' belongs to  
non-existent group ''  
Rows Returned: 5  
  
Checking for users belonging to groups not in dm_user  
Checking for users not listed in dmi_object_type  
Checking for groups not listed in dmi_object_type  
Checking for groups belonging to non-existent groups  
Checking for groups with non-existent super groups  
  
#####  
##  
##  
## CONSISTENCY_CHECK: ACLs ##  
##  
##      Start Time: 09-10-2002 10:15:55  
##  
##  
#####  
  
Checking for ACLs with non-existent users  
Checking for ACLs with missing dm_acl_r table entries  
Checking for sysobjects with acl_domain set to  
  non-existent user  
Checking for sysobjects that belong to  
non-existent users  
Checking for sysobjects with non-existent ACLs  
Checking for ACL objects with missing dm_acl_s entry  
Checking for ACL objects with r_accessor_permit  
value but missing r_accessor_name value  
Checking for ACL objects with r_accessor_name value  
  but missing r_accessor_permit value  
Checking for ACL objects with r_is_group value but  
  missing r_accessor_permit value  
Checking for ACL objects with r_is_group value but  
  missing r_accessor_name value
```

```

Checking for ACL object with r_accessor_name value
  but missing r_is_group value
Checking for ACL object with r_accessor_permit value
  but missing r_is_group value

#####
## 
##  ## CONSISTENCY_CHECK: Sysobjects
## 
##      Start Time: 09-10-2002 10:15:58
## 
## #####
Checking for sysobjects which are not referenced in
dmi_object_type
Checking for sysobjects that point to non-existent
content
Checking for sysobjects that are linked to non-existent
folders
Checking for sysobjects that are linked to non-existent
primary cabinets
Checking for sysobjects with non-existent i_chronicle_id
Checking for sysobjects with non-existent i_antecedent_id
Checking for sysobjects with missing
dm_sysobject_r entries
Checking for sysobjects with missing
dm_sysobject_s entry

#####
## 
##  ## CONSISTENCY_CHECK: Folders and Cabinets
## 
##      Start Time: 09-10-2002 10:16:02
## 
## #####
Checking for folders with missing dm_folder_r table
entries
Checking for folders that are referenced in dm_folder_r
but not in dm_folder_s
Checking for dm_folder objects that are missing an
entry in dmi_object_type
Checking for dm_folder objects that are missing
corresponding dm_sysobject entries
Checking for folders with non-existent ancestor_id
Checking for cabinet that have missing dm_folder_r
table entries
Checking for cabinets that are missing an entry in
dmi_object_type
Checking for folder objects with missing
dm_sysobject_r entries
Checking for folder objects with null r_folder_path

#####
## 
##  ## CONSISTENCY_CHECK: Documents
## 
##      Start Time: 09-10-2002 10:16:03
## 
## #####
Checking for documents with a dm_sysobject_s entry
  but no dm_document_s entry

```

```
Checking for documents with missing dm_sysobject_s
entries
Checking for documents with missing dmi_object_type
entry
#####
##
## CONSISTENCY_CHECK: Content
##
##      Start Time: 09-10-2002 10:16:03
##
##
#####
Checking for content objects that reference
non-existent parents
Checking for content with invalid storage_id
Checking for content objects with non-existent format
#####
##
## CONSISTENCY_CHECK: Workflow
##
##
##      Start Time: 09-10-2002 10:16:03
##
##
#####
Checking for dmi_queue_item objects with non-existent
queued objects
Checking for dmi_workitem objects that reference
non-existent dm_workflow objects
Checking for dmi_package objects with missing
dmi_package_s entries
Checking for dmi_package objects that reference
non-existent dm_workflow objects
Checking for workflow objects with non-existent
r_component_id
Checking for workflow objects with missing
dm_workflow_s entry
Checking for work item objects with missing
dm_workitem_s entry
#####
##
## CONSISTENCY_CHECK: Types
##
##      Start Time: 09-10-2002 10:16:04
##
##
#####
Checking for dm_type objects with a non-existent
dm_type_info object
Checking for dm_type_info objects with a non-existent
dm_type object
Checking for type objects with corrupted property
positions
Checking for types with invalid property counts
#####
##
## CONSISTENCY_CHECK: Data Dictionary
##
##      Start Time: 09-10-2002 10:16:04
```

```

##  

##  

#####  

Checking for duplicate dmi_dd_attr_info objects  

Checking for duplicate dmi_dd_type_info objects  

Checking for any dmi_dd_attr_info objects that are  

missing an entry in dmi_dd_common_info_s  

Checking for any dmi_dd_type_info objects that are  

missing an entry in dmi_dd_common_info_s  

Checking for any dmi_dd_attr_info objects that are  

missing an entry in dmi_dd_attr_info_s  

Checking for any dmi_dd_type_info objects that are  

missing an entry in dmi_dd_type_info_s  

#####  

##  

##  

## CONSISTENCY_CHECK: Lifecycles  

##  

##      Start Time: 09-10-2002 10:16:11  

##  

#####  

Checking for sysobjects that reference non_existent  

policy objects  

Checking for any policy objects that reference  

non-existent types in included_type  

Checking for any policy objects with missing  

dm_sysobject_s entry  

Checking for any policy objects with missing  

dm_sysobject_r entries  

Checking for policy objects with missing dm_policy_r  

entries  

Checking for policy objects with missing dm_policy_s  

entry  

#####  

##  

##  

## CONSISTENCY_CHECK: FullText  

##  

##      Start Time: 09-10-2002 10:16:11  

##  

#####  

Checking for tdk index objects that point to  

non-existent fulltext index objects  

Checking for any tdk collect objects that point to  

non-existent tdk index objects  

Checking for any fulltext index objects that point  

to non-existent tdk index objects  

Checking for any tdk index objects that point to  

non-existent tdk collect objects  

Checking for any non-orphaned dmr_content objects  

that point to types that do not exist  

Checking for any non-orphaned dmr_content objects  

that point to non-existent formats  

Checking for any dmr_content objects that point to  

a non-existent fulltext index  

Checking for any fulltext index propertys that are  

no longer in dm_type  

#####  

##  

##  

## CONSISTENCY_CHECK: Indices  

##  

##      Start Time: 09-10-2002 10:16:11

```

```

#######
## Checking for dmi_index objects that reference
## non-existent types
## Checking for types with non-existent dmi_index
## object for <type>_s table
## Checking for types with non-existent dmi_index
## object for <type>_r table
## Checking for index objects with invalid property
## positions
#####
## CONSISTENCY_CHECK: Methods
## Start Time: 09-10-2002 10:16:11
## #####
## Checking for java dm_method objects that reference
## jview
## Consistency Checker completed successfully
## Total number of inconsistencies found: 5
## Disconnected from the server.
#####

```

#### 17.4.1.6 Content replication

The Content Replication tool automates content replication between the component storage areas of a distributed storage area. The tool uses dump and load operations, but unlike manual dump and load operations, only requires enough temporary disk space to transfer the largest individual content file to be replicated.

By default, the tool processes the content files in batches. It retrieves up to 500 content files (the default batch size) and releases resources in the source database before replicating the files. You can adjust the size of the batches by setting the `-batch_size` argument. Each execution of the job may process multiple batches, depending on the number of content files to be replicated and the batch size.

If the `-batch_size` argument is set to 0, the DQL hint `FETCH_ALL_RESULTS 0` is used in the query. All files to be replicated are cached in the memory of Documentum CM Server and transferred individually. Set `-batch_size` to 0 only if you have a very large amount of memory available.

If the `-batch_size` argument is set to 1, the `FETCH_ALL_RESULTS` hint is not used and query results are not cached.

If the `-batch_size` argument is set to any value greater than 1 and content transfer operations fail for the whole batch, the job exits and displays an error message.

The job uses a login ticket to connect to each source server. If you include the `-source_servers` argument, the job connects only to the servers in the list. If you do not include that argument, the job attempts to connect to each server in the repository.



**Note:** The clocks on the host machines of the source servers must be using UTC time and must be synchronized with the host machine on which the job runs. The login ticket for the job is valid for 5 minutes. If the clocks are not synchronized or the machines are using times set to different time zones, the source server to which the job is connecting may determine that the ticket has timed out and the job will fail.

A content replication job looks for all content not locally present, gets the files while connected to other sites, and performs an IMPORT\_REPLICA for each content file in need of replication. The job generates a report that lists each object replicated. The report is saved to the repository in /System/Sysadmin/Reports/ContentReplication.



**Note:** If the report was run against the content at a remote distributed site, the report name has the server configuration name appended with name of site. For example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/ContentReplicationLondon.

Installing the tool suite at a site creates a content replication job for the installation site. In a distributed environment, the argument values of job for the remote sites are based on those of the Content Replication job for the primary site, but the job name and target server will be unique for each site. The job name has the format:

```
dm_ContentReplicationserverconfig.object_name
```

The target\_server property of job identifies the local server performing the replication using the format *repository.serverconfig@hostname*.

The ContentReplication job is inactive by default.

#### 17.4.1.6.1 Arguments

“Content replication arguments” on page 363, describes the arguments for the tool.

**Table 17-8: Content replication arguments**

Argument	Datatype	Default	Description
-window_interval	integer	120	Defines window in which the tool can run. Value is interpreted in minutes.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.

Argument	Datatype	Default	Description
-batch_size	integer	500	Number of content files to process in each batch.
-custom_predicate	string	-	Qualification applied to the content to be replicated. Enter what would normally appear after WHERE in a DQL qualification (For example,  FOLDER ('/xyz', descend)
-source_servers	string	-	Comma-separated list of Documentum CM Servers to which to connect. Use the names of the servers' server configuration objects.  The argument accepts a maximum of 255 characters. The specified names are recorded in the method_arguments property of job.  If this argument is not included, the job attempts to connect to all other servers in the repository.

#### 17.4.1.6.2 Report sample

Here is a sample of a ContentReplication report.

```
ContentReplication Report For repository wagnerdb
As Of 3/16/97 4:58:34 PM
Making lists of distributed components that are
local and far
Far Store: StoreC
Near Store: StoreE
Getting the source user for connecting to
other sites...
Getting the source password for connecting
to other sites...
Now connected to WagnerA
  Replicated 1 KB, format text for document
DBWarning
  Replicated 7 KB, format text for document
StateOfDocbase
  Replicated 14 KB, format text for document
```

```

LogPurge
Replicated 2 KB, format text for document
ContentReplication
Replicated 3 KB, format text for document
ContentWarning
Replicated 5 KB, format text for document
DMClean
Replicated 4 KB, format text for document
DMFilescan
Replicated KB, format text for document
Disconnected from WagnerA
Report End 3/16/97 4:58:53 PM

```

### 17.4.1.7 Content warning

The Content Warning tool notifies you when disks that you use for content storage approach a user-defined capacity. The notification is sent to the repository Inbox of the queueperson and as an email message. The tool also generates a report that is stored in the Reports folder under the Sysadmin folder in the System cabinet.

The tool determines where the repository is storing its content and then uses operating system commands to determine whether these disks are reaching the specified threshold. When the disk space used meets or exceeds the value in the percent\_full argument of tool, a notification is sent to the specified queueperson and a report is generated and saved to the repository in /System/Sysadmin/Reports/ContentWarning.



#### Notes

- If the tool was run against the content at a remote distributed site, the report name has the server configuration name appended with name of site. For example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/ContentWarningLondon.
- The dm\_ContentWarning job may not work properly when the disk space is in terabytes scale.

The Content Warning tool is installed in the active state by default.

#### 17.4.1.7.1 Arguments

“Content warning arguments” on page 366, describes the arguments for the tool.

**Table 17-9: Content warning arguments**

Argument	Datatype	Default	Description
-percent_full	integer	85	Percent-full threshold at which a message is sent.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	720	Execution window for the tool, expressed in minutes.

#### 17.4.1.7.2 Report sample

Here is a sample of a ContentWarning report.

```

Object: test1_file_store
Type : dm_filestore
Path : /export/nfs2-4/dmadmin/data/test1/
test1_storage_location
Total Disk Total Used Total Free Percent Used
1,952,573 1,620,019 137,304 93

DocBasic Total Free: 1,124,794
Content File (Document) Space Utilization
In test1_file_store

-Active 2,485,090
-Deleted 81,397
-Total 2,566,487

Object: test1_file_store2
Type : dm_filestore
Path : /export/nfs2-1/dmadmin/data/test1/storage_02

Total Disk Total Used Total Free Percent Used
1,952,573 1,113,666 643,657 67

DocBasic Total Free: 977,871
Content File (Document) Space Utilization
In test1_file_store2
-Active 733,532
-Deleted 3,821
-Total 737,352

Object: support_file_store
Type : dm_filestore
Path : /export/nfs2-1/dmadmin/data/test1/docs_from_test2

```

Total Disk	Total Used	Total Free	Percent Used
1,952,573	1,113,666	643,657	67
DocBasic Total Free:			977,871
Content File (Document) Space Utilization In test2_file_store			
-Active	863		
-Deleted			
-Total	863		

### 17.4.1.8 Data dictionary publisher

The Data Dictionary Publisher tool publishes the data dictionary information. The data dictionary is information about object types and properties stored in internal objects by Documentum CM Server and made available to client applications through the publishing operation. Publishing the information creates dd type info and dd attr info objects. These are persistent objects whose properties store the data dictionary information. Client applications that use the data dictionary information can reference or query these objects and their properties. For more information about the data dictionary, see *OpenText Documentum Content Management - Server Fundamentals Guide (EDCCS250400-GGD)*.

Data Dictionary Publisher generates a status report that is saved in the repository in /System/Sysadmin/Reports/DataDictionaryPublisher.

#### 17.4.1.8.1 Arguments

“Data dictionary publisher argument” on page 367, describes the argument of tool.

**Table 17-10: Data dictionary publisher argument**

Argument	Datatype	Default	Description
-window_interval	integer	720	Execution window for the tool, expressed in minutes.

#### 17.4.1.8.2 Report sample

```
Connected To sqlntX.sqlntX
Job Log for System Administration Tool
DataDictionaryPublisher
-----
This job log consists of three distinct parts:
1) All print statements from the execution of the job
2) The report for the tool which is saved as a
   separate document in the repository in
   /System/Sysadmin/Reports.
3) The trace file results from the trace API,
   if the job's trace level is > 0.

Note: The report and trace file are also maintained
under the Documentum log location in:
$DOCUMENTUM/dba/log/<docbase hex id>/sysadmin
They are overwritten each time the job executes.
```

```

Start of log:
-----
DataDictionaryPublisher Tool Completed at
11/8/2000 12:15:25. Total duration was 0 minutes.
Calling SetJobStatus function...

--- Start
c:\Documentum\dba\log\000145df\sysadmin\
DataDictionaryPublisherDoc.txt report output ---
DataDictionaryPublisher Report For repository sqlntX
As Of 11/8/2000 12:15:24
DataDictionaryPublisher utility syntax:
apply,c,NULL,EXECUTE_DATA_DICTIONARY_LOG
Executing DataDictionaryPublisher...
Report End 11/8/2000 12:15:25

--- End
c:\Documentum\dba\log\000145df\sysadmin\
DataDictionaryPublisherDoc.txt report output ---

```

### 17.4.1.9 Database space warning

The Database Space Warning tool scans the RDBMS to determine:

- How full the tablespace (Oracle) or device (Sybase) is.
- Whether any tables are fragmented beyond a user-specified limit.
- Whether the expected number of indexes are present.

The tool also recreates any indexes that are identified by dmi\_index objects but not found in the database.



**Note:** The Database Space Warning Tool is not needed, and therefore not installed, for installations running against SQL Server.

If the tool finds that the space has reached the limit specified in the percent\_full argument of tool, it sends a notification to the user specified in queueperson. When it sends a notification, it also includes a message about any RDBMS tables that are fragmented beyond the limits specified in the max\_extents argument and a message regarding indexes, if it does not find the expected number in the RDBMS. The notifications are sent to the Inbox of user repository and through email.

In addition to these notifications, the tool generates a status report that is saved in the repository in /System/Sysadmin/Reports/DBWarning.

The Database Space Warning tool is installed in the active state.

For Sybase, you must set the ddl in tran database option to TRUE to run this job. The isql syntax is:

```
sp_dboption dbname, "ddl in tran", true
```

where *dbname* is the name of the database for your repository.

#### 17.4.1.9.1 Arguments

“Database space warning arguments” on page 369, lists the arguments of tool.

**Table 17-11: Database space warning arguments**

Argument	Datatype	Default	Description
-percent_full	integer	85	Percent-full threshold at which a message is sent.
-max_extents	integer	50	The number of extents that an RDMBS table may have before being reported as fragmented.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	720	Execution window for the tool, expressed in minutes.

#### 17.4.1.9.2 Report sample

Here is a sample of a Database Space Warning report. It shows the total number of blocks allocated for the database, how many are currently used for tables and indexes, the percentage used of the total allocated, and the number of free blocks. It also lists the number of fragments for all tables and indexes with more than max\_extents fragments and lists the number of indexes in the repository.

```

Database Block Allocation
Table   Index   TotalUsed    Free     Total  %Used/Total
620     647      1,267     81,929   83,196      2

DBMS Tables With Multiple Extents
# of Segs      Type        Name
  6            TABLE       DM_TYPE_R
  5            INDEX       DMINDEX_1F00096380000009
  4            TABLE       DM_SYSOBJECT_S
  3            TABLE       DMI_OBJECT_TYPE
  3            INDEX       DMI_OBJ_TYPE_INDEX
  3            INDEX       DMI_OBJ_ID_INDEX
  3            TABLE       DM_FORMAT_S
  3            TABLE       DM_SYSOBJECT_R

```

#### 17.4.1.9.3 Inbox and email message samples

Here is a sample Inbox message sent by the Database Space Warning tool:

```
Take a look at your DBMS tablespace--it's 90% full!
You have 8 fragmented tables in your DBMS instance
--you may want to correct this!
You are missing some Documentum indexes-contact Support!
```

Here is the corresponding email message:

```
Return-Path: <dmadmin@bigcat>
X-UIDL: 827349620.001
Date: Wed, 20 Mar 1996 11:18:54 -0800
From: dmadmin@bigcat (Documentum 2.0)
To: stevex@tiger
Subject: Event FraggedTables has occurred
on DBWarning.Doc
(090000018006ee33) by dm20

DOCBASE: test1
EVENT: FraggedTables
NAME: DBWarning.Doc
SENT BY: dmadmin
TASK NAME: event

MESSAGE:
You have 18 fragmented tables in your DBMS instance
--you may want to correct this!
```

#### 17.4.1.10 Distributed operations (dm\_DistOperations)

The dm\_DistOperations job performs inter-repository distributed operations. These tasks include:

- Propagating distributed events (dmi\_queue\_items) across repositories
- Creating checkout references for remote checkout operations
- Refreshing reference links

The dm\_DistOperations job is configured to run every five minutes by default. Do not change the schedule.

It is installed in the repository in an inactive state.

#### 17.4.1.11 Archive

The Archive tool automates archive and restore between content areas. Archive older or infrequently accessed documents to free up disk space for newer or more frequently used documents. Restore archived documents to make the archived documents available when users request them. For complete information on configuring archiving, refer to “[Archiving and restoring documents](#)” on page 533.

The Archive tool is active by default, and runs once daily.

#### 17.4.1.11.1 Arguments

“Archive arguments” on page 371 describes the arguments for the tool

**Table 17-12: Archive arguments**

Argument	Datatype	Default	Description
<code>-docbase_name <i>repository</i></code>	string(64)	-	Identifies the repository that contains the document or documents to archive. Use the name of repository.
<code>-Username</code>	string(64)	-	Identifies the user executing dmarchive. If unspecified, the current user is assumed.
<code>-Ppassword</code>	string(64)	-	Password for the user executing dmarchive. If unspecified, the user is prompted.
<code>-archive_dir <i>directory</i></code>	string	-	The location of the archive directory. Use a full path specification.
<code>-queue_name <i>name</i></code>	string	-	Identifies the repository operator. Specify the repository user name of operator. If unspecified, the tool assumes the user named in the operator_name property of the server configuration object.
<code>-queue_event <i>event_id</i></code>	ID	-	Object ID of the queue item object representing an archive or restore event.  If set, the tool processes only the specified event.

Argument	Datatype	Default	Description
-do_archive_events	Boolean	-	TRUE directs the tool to process only archive events.
-do_restore_events	Boolean	-	TRUE directs the tool to process only restore events.
-verbose	Boolean	T	TRUE directs the tool to print trace messages.
-window_interval	integer	720	Defines window in which the tool can run. Value is interpreted in minutes.
-queueperson	string	-	Identifies the user who receives Inbox and email notifications from the tool.

#### 17.4.1.11.2 Guidelines

The Archive tool puts all the documents it is archiving in one dump file. This means you must move the entire dump file back to the archive directory to restore a single document in the file. If the files are extremely large, this can be a significant performance hit for restore operations.

#### 17.4.1.12 Dmclean

The Dmclean tool automates the dmclean utility. The utility scans the repository for orphaned content objects and content objects. The utility generates a script to remove these orphans. The Dmclean tool performs the operations of dmclean and (optionally) runs the generated script.

When the agent exec program invokes the script, the tool generates a report showing what content objects and content files are removed upon execution of the generated script. The status report is saved in /System/Sysadmin/Reports/DMClean.



**Note:** If the tool was run against the content at a remote distributed site, the report name has the server configuration name appended with the name of the site. For example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/DMCleanLondon.

The Dmclean tool is installed in the inactive state.

#### 17.4.1.12.1 Arguments

“Dmclean arguments” on page 373, describes the arguments for the tool.

**Table 17-13: Dmclean arguments**

Argument	Datatype	Default	Description
-clean_content	Boolean	TRUE	Controls whether the tool searches for orphaned content objects. Set to FALSE if you do not want to include content objects in the dmclean operation.
-clean_castore	Boolean	FALSE	Controls whether the tool includes orphaned content with expired retention dates in Centera storage areas in the operation. T means that expired, orphaned content in Centera storage areas is included in the operation.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	120	Execution window for the tool.

#### 17.4.1.12.2 Guidelines

If you are using Distributed Content, Dmclean requires the default storage area for dm\_sysobjects to be the distributed store.

How often you run Dmclean will depend on

- Your business rules
- The size of the repository
- The amount of storage capacity

#### 17.4.1.12.3 Report sample

Here is a sample of a Dmclean report:

```
DMClean Report For DocBase testdoc
As Of 5/14/2002 11:58:46

Arguments for the dmclean method:
objects will be cleaned up...
Orphaned content objects will be cleaned up...
Generated DMClean script will be executed...

The trace level is set to 0...
DMClean utility syntax: apply,c,NULL,DO_METHOD,
METHOD,S,dmclean

Executing DMClean...
All Clean contents were successfully removed.
Generated script from the DMClean method:
----- Start
C:\Documentum\dba\log\000003e8\sysadmin\
080003e8800005d6.bat
output -----
# Opening document base testdoc...
#   Total shared memory size used: 1554112 bytes
#   Making /System cabinet.
#   /System cabinet exists.
#   Making /Temp cabinet.
#   /Temp cabinet exists.
#   Making /System/Methods folder.
#   /System/Methods folder exists.
#   Making /System/FileSystem folder.
#   /FileSystem folder exists.
#   Making /System/DataDictionary folder.
#   /System/DataDictionary folder exists.
#   Making /System/Procedures folder.
#   /System/Procedures folder exists.
#   Making /System/Procedures/Actions folder.
#   /System/Procedures/Actions folder exists.
#   Making /System/Distributed References folder.
#   /System/Distributed References folder exists.
#   Making /System/Distributed References/Links
   folder.
#   /System/Distributed References/Links folder
   exists.
#   Making /System/Distributed References/Checkout
   folder.
#   /System/Distributed References/Checkout folder
   exists.
#   Making /System/Distributed References/Assemblies
   folder.
#   /System/Distributed References/Assemblies folder
   exists.
#   Making /System/Distributed References/Workflow
   folder.
#   /System/Distributed References/Workflow folder
   exists.
#   Making /System/Distributed References/VDM folder.
#   /System/Distributed References/VDM folder exists.
#   Making docbase config object.
#   Making server configuration object.
#
# dmclean cleans up orphan content objects and content files.
# Instead of immediately destroying the orphan content objects,
# dmclean generates an API script, which can
# be used for verification before cleanup actually
# happens.
# This is done in this manner because deleted content
# objects by mistake are difficult to recover.
#
```

```

# To remove orphan content objects after verification,
# do the following in iapi:
#
# % iapi <DOCBASE> -U<USER> -P<PWD>
# API> @<SCRIPT_NAME>
# API> quit
#
# Starting to clean up unused content objects...
# Content object 060003e880002100 has parent
# count of zero.
apply,c,060003e880002100,DESTROY_CONTENT
getmessage,c
close,c,q0
# Content object 060003e880002101 has parent
# count of zero.
apply,c,060003e880002101,DESTROY_CONTENT
getmessage,c
close,c,q0
# Content object 060003e880002105 has parent
# count of zero.
apply,c,060003e880002105,DESTROY_CONTENT
getmessage,c
close,c,q0
# Content object 060003e88000210c has parent
# count of zero.
apply,c,060003e88000210c,DESTROY_CONTENT
getmessage,c
close,c,q0
# Content object 060003e880002114 has parent
# count of zero.
apply,c,060003e880002114,DESTROY_CONTENT
getmessage,c
close,c,q0
# Content object 060003e880002119 has parent
# count of zero.
apply,c,060003e880002119,DESTROY_CONTENT
getmessage,c
close,c,q0
# Count of objects with zero parent count was: 6
# Content cleanup complete.
# Starting to clean up unused subcontent objects...
# SubContent cleanup complete.
----- End
C:\Documentum\dba\log\000003e8\sysadmin\
080003e8800005d6.bat output -----
Destroying DMclean script with ID 090003e880002907...
Report End 5/14/2002 11:59:16

```

### 17.4.1.13 Dmfilescan

The Dmfilescan tool automates the dmfilescan utility. This utility scans a specific storage area or all storage areas for any content files that do not have associated content objects and generates a script to remove any that it finds. The tool executes the generated script by default, but you can override the default with an argument. “[dmfilescan utility](#)” on page 529 provides detailed information about the dmfilescan utility.

Dmfilescan also generates a status report that lists the files it has removed. The report is saved in the repository in /System/Sysadmin/Reports/DMFilescan.



#### Notes

- If the tool was run against the content at a remote distributed site, the report name has the server configuration name appended with name of site. For

example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/DMFilescanLondon.

- The tool is not supported for Centera filestores.

Centera is an object-based storage system that uses Clip IDs instead of traditional file paths. Since Dmfilescan depends on the file system paths to locate and validate content, it is inherently incompatible with Centera.

Dmfilescan is installed in the inactive state.

#### 17.4.1.13.1 Arguments

[“Dmfilescan arguments” on page 376](#), lists the arguments for the tool. Refer to the description of the dmfilescan utility in [“dmfilescan utility” on page 529](#), for instructions on specifying values for the -from and -to arguments.

**Table 17-14: Dmfilescan arguments**

Argument	Datatype	Default	Description
-s <i>storage_name</i>	string	-	Specifies a target storage area. If this argument is not included, all storage areas are scanned.
-from <i>directory_path</i>	string	-	Starting subdirectory for the scan operation.
-to <i>directory_path</i>	string	-	Ending subdirectory for the scan operation.
-scan_now	Boolean	TRUE	Controls whether the generated script is executed. TRUE (the default) executes the generated script. Set this to FALSE if you want to execute the script manually.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	120	Execution window for the tool.

Argument	Datatype	Default	Description
-force_delete	Boolean	FALSE	Controls whether orphan files created within 24 hours of the execution job are deleted. Refer to the Guidelines for details.
-no_index_creation	Boolean	FALSE	Controls whether dmfilescan creates and destroys the indexes on dmr_content.data_ticket and dmr_content.other ticket or assumes they exist.  T (TRUE) means that the utility assumes that the indexes exist prior to the start of the utility. F (FALSE) means the utility will create these indexes on startup and destroy them at the finish.
-grace_period	integer	168	Defines the grace period for allowing orphaned content files to remain in the repository. The default is 168 hours (1 week), expressed as hours. The job removes orphaned files whose age exceeds 1 week or the value defined in the -grace_period argument.  The integer value for this argument is interpreted as hours.

#### 17.4.1.13.2 Guidelines

Typically, if you run the Dmclean tool regularly, it is not necessary to run the Dmfilescan tool more than once a year. By default, the tool removes all orphaned files from the specified directory or directories that are older than 24 hours. If you wish to remove orphaned files younger than 24 hours, you can set the -force\_delete flag to T (TRUE). However, this flag is intended for use only when you must remove younger files to clear disk space or to remove temporary dump files created on the target that were not removed automatically. If you execute Dmfilescan with -force\_delete set to T, make sure that there are no other processes or sessions creating objects in the repository at the time the job executes.

If you are using Distributed Content, dmfilescan requires the default storage area for dm\_sysobjects to be the distributed store.

#### 17.4.1.13.3 Report sample

The following is a sample of a Dmfilescan report:

```
DMFilescan Report For DocBase boston2
As Of 9/17/96 11:08:54 AM
Generated DMFilescan script will be executed...
The trace level is set to 5...
DMFilescan utility syntax: apply,c,NULL,DO_METHOD,
METHOD,S,dmfilescan
Executing DMFilescan...
Executing DMFilescan script...
sh /u106/dm/dmadmin/dba/log/00000962/sysadmin/
0900096280012800.bat
>/u106/dm/dmadmin/dba/log/00000962/sysadmin/
0900096280012800.txt
Generated script from the DMFilescan method:
----- Start
/u106/dm/dmadmin/dba/log/00000962/sysadmin/
0900096280012800.bat output
-----
#!/bin/sh -x
#
# Documentum, Inc.
#
# This script is generated by dmfilescan for later
# verification and/or clean-up. This script is in
# trace mode by default. To turn off the trace mode,
# remove the '-x' in the first line.
#
# To see if there are any content objects referencing
# a file reported below, use the following query
# (executed in idql):
#
# % idql <docbase> -U<user> -P<pwd>
# 1> select r_object_id from dmr_content
# 2> where storage_id = '<storage_id>' and data_ticket =
# <data_ticket>
# 3> go
#
# If there are no rows returned, then this is an
# orphan file.
#
# Opening document base boston2...
#   Making distributed object_id map.
#   Making /System cabinet.
#   /System cabinet exists.
#   Making /Temp cabinet.
#   /Temp cabinet exists.
```

```

#      Making /System/Methods folder.
#      /System/Methods folder exists.
#      Making /System/FileSystem folder.
#      /System/FileSystem folder exists.
#      Making docbase config object.
#      Making server configuration object.
# Document base boston2 opened. Starting filescan...
# Building indexes for content lookups ...
# Checking store filestore_01...
# Checking store replica_filestore_01...
# Checking store replicate_temp_store...
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/01'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/02'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/03'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/04'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/05'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/06'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/07'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/08'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/09'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/0a'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/0b'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/0c'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/0d'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/0e'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/0f'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/10'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/11'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/12'
# Reading directory '/u127/dm/data/boston2/
content_storage_01/00000962/80/00/13'
# Reading directory '/u127/dm/data/boston2/
replica_content_storage_01/00000962'
# Reading directory '/u127/dm/data/boston2/
replica_content_storage_01/00000962/80'
# Reading directory '/u127/dm/data/boston2/
replica_content_storage_01/00000962/80/00'
# Reading directory
'/u127/dm/data/boston2(replica_content_storage_01/
00000962/80/00/01'
# Reading directory
'/u127/dm/data/boston2(replica_content_storage_01/
00000962/80/00/02'
# Reading directory
'/u127/dm/data/boston2(replica_content_storage_01/
00000962/80/00/03'
# Reading directory

```

```
'/u127/dm/data/boston2/replica_content_storage_01/
00000962/80/00/09'
# Reading directory
'/u127/dm/data/boston2/replica_content_storage_01/
00000962/80/00/0a'
# Reading directory
'/u127/dm/data/boston2/replica_content_storage_01/
00000962/80/00/0c'
# Reading directory
'/u127/dm/data/boston2/replica_content_storage_01/
00000962/80/00/07'
# Reading directory '/u127/dm/data/boston2/
temp_replicate_store/00000962'
# Directory /u127/dm/data/boston2/temp_replicate_store/
00000962 is empty
# 0 orphan files were found
#
# Cleaning up content indexes ...
----- End /u116/dm/dmadmin/dba/log/00000962/sysadmin/
0900096280012800.bat output
-----
Destroying DMFilescan result file with ID 0900096280012800...
Report End 9/17/96 11:09:54 AM
```

### 17.4.1.14 Fix folder (dm\_fixfolder)

This tool checks each folder in the repository for corruption in r\_folder\_path or i\_ancestor\_id. This tool:

- Runs the dm\_fixfolder\_Java method.
- Checks that r\_folder\_path values reflect r\_folder\_path of the parents.
- Checks that i\_ancestor\_id values correctly reflect the IDs of the parents.
- Looks for (and removes) self-linked folders and attaches the orphaned folders to the /Temp cabinet.
- Issues warnings about folder paths which exceeds the field width.

#### 17.4.1.14.1 Arguments

The dm\_fixfolder tool has the following arguments:

- docbase\_name
- user\_name
- password
- method\_trace\_level
- (optional) folderQual: ID of the folder or query.
- (optional) report\_only\_mode: Valid values are True or False. Default is True, which means only a report is generated and the corrupted folders are not fixed.

#### 17.4.1.15 Federation copy (dm\_FederationCopy)

The Federation Copy tool transfers LDIF files, which contain user and group information, to member repositories from the governing repository. The job is installed in an inactive state. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the information on repository federations and the federation jobs.

#### 17.4.1.16 Federation export (dm\_FederationExport)

The Federation Export tool exports user and group information from the governing repository to an LDIF file. The job is installed in an inactive state. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the information on repository federations and the federation jobs.

#### 17.4.1.17 Federation import (dm\_FederationImport)

The Federation Import tool imports an LDIF file that contains user and group information into a member repository. The job is installed in an inactive state. When you create a federation, the job is activated in the member repositories. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the information on repository federations and the federation jobs.

#### 17.4.1.18 Federation status (dm\_FederationStatus)

The Federation Status tool polls the members of a federation to determine the current status of any Federation Import jobs running on the member repository. The job is installed in an inactive state. When you create a federation, the job is activated in the governing repository. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the information on repository federations and the federation jobs.

#### 17.4.1.19 Federation update (dm\_FederationUpdate)

The Federation Update tool executes on the governing repository of a federation to run all other methods in sequence, pushing user, group, and ACL changes to the member repositories. The job is installed in an inactive state. When you create a federation, the job is activated in the governing repository. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the information on repository federations and the federation jobs.

### 17.4.1.20 File report

The File Report tool assists you in restoring deleted repository documents. It generates a report that lists all documents in the repository and their corresponding content files. Using that report in conjunction with a file system backup, you can restore the content file of a deleted document. “[Using a report to restore a document](#)” on page 383 provides instructions on restoring a document.

If a document must be recreated, these reports identify which files must be restored to rebuild the document. The system administrator matches lost documents to the file names so that the content files can be recovered. This feature is especially useful for restoring a single document (or a small set of documents) to a previous state, which cannot be done from database backups.

The File Report tool as installed, runs a full report once a week against all file storage areas in the repository. It is possible to run incremental reports and reports that only examine a subset of the storage areas for the repository. “[Creating incremental or partial-repository reports](#)” on page 383 provides instructions to set up reports.



**Note:** File Report only provides a mechanism for restoring the document content. The document metadata must be restored manually.

File Report saves the generated report to /System/Sysadmin/Reports/FileReport.

The File Report tool is installed as inactive.

#### 17.4.1.20.1 Guidelines

Set up the File Report schedule on the same interval as the file system backups. For example, if nightly backups are done, also run File Report nightly and store the resulting report with the backups.

We recommend scheduling nightly incremental reports and generating full repository reports on a less frequent basis (weekly or biweekly).

If your repository is so large that creating full reports is not practical or generates cumbersome files, set up multiple jobs, each corresponding to a different storage area.

#### 17.4.1.20.2 Usage notes

This section describes two procedures for using file reports:

- Creating new file report jobs to create incremental reports or reports for a subset of storage areas.
- Using file reports to recover a document

#### 17.4.1.20.3 Creating incremental or partial-repository reports

A File Report job creates an incremental report if its `-incremental_report` argument is set to TRUE. Incremental reports only include documents that have changed since the last File Report was run.

If you include the `-storage_area` argument, the job generates a report on the documents in the specified storage area.

If you include the `-folder_name` argument, the job generates a report on documents in the specified folder.

Including both the `-storage_area` and `-folder_name` arguments generates a report on those documents in the specified folder that are also stored in the given storage area.

To create a job that generates incremental reports or only reports on some storage areas, copy an existing File Report job object and set its properties and arguments as needed. Provide a new name for the copy that identifies it meaningfully.

[“Creating a job” on page 420](#), provides instructions for creating new jobs, and *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* contains a description of the properties of `dm_job` object. You can create or copy a job using Documentum Administrator.

#### 17.4.1.20.4 Using a report to restore a document

The following procedure describes how to use a report to restore a document:

##### To restore a document to the repository:

1. Find the last backup file report with the document listed in it.
2. Find the name(s) of the content file(s) which comprise the document.
3. Restore the named files from your file system backups to the original storage area.

This restores the content files to the storage area directory. This *does not* restore the documents to the repository. Until the files are imported back into the repository, they are treated as orphaned content files and will be removed by the next invocation of the `dm_clean` utility.

If you wish, you can move these files out of the storage area directories to a more appropriate work area in order to import them into the repository.

4. Use the restored content files to recreate the repository documents.

The best way to do this is to use a OpenText Documentum CM client to recreate the object metadata and then use a Foundation Java API session on the server machine to restore the content.

If you need to restore renditions of the document pages manually, use an `addRendition` method.

You can restore documents that have only one content file using the Import function of client if the content files are directly accessible by the client. Because

the content files restored from file system backups are written to the server storage areas, you must either directly access those directories from the client or copy the restored files to a network disk and import them from there.

If the document has multiple pages, use Foundation Java API methods to restore it.

#### 17.4.1.20.5 Arguments

"File report arguments" on page 384, lists the arguments for the tool.

**Table 17-15: File report arguments**

Argument	Datatype	Default	Description
<code>-folder_name <i>folder_path</i></code>	string	-	Identifies a folder path on which to run the report. May be used in conjunction with the <code>-storage-area</code> argument.
<code>-incremental_report</code>	Boolean	FALSE	When set to TRUE, the report is run incrementally. An incremental report only reports documents modified since the last time the job ran. (A full report is generated on the first execution of the job).
<code>-storage_area <i>storage_name</i></code>	string	-	Identifies a storage area on which to run the report. Use the name of storage area. If this argument is not set, the report runs against all storage areas in the repository.

Argument	Datatype	Default	Description
-output_device	string	-	<p>Identifies a file to which to write the report data. The specification must be in the format:</p> <p>directory_path/file_name</p> <p>If the file already exists, data is appended to it.</p> <p>Use this option when you want to write directly to a tape drive or other device.</p> <p>If not set, the report file is saved to: System/Sysadmin/Reports/FileReport</p>
-report renditions	Boolean	TRUE	When set to TRUE, rendition files are reported as well as the primary format files. Set to False if you do not wish to report renditions.
-sort_results	Boolean	TRUE	<p>When set to TRUE, the file report is sorted by folder_path/object_name.</p> <p>Because this option requires a database sort of the entire data set returned, you may need to tune your sort/temp space parameters of database if you use this option.</p>
-window_interval	integer	120	Execution window for the tool.
-queueperson	string	-	Identifies the user who receives Inbox and email notifications from the tool.

#### 17.4.1.20.6 Report sample

Each line of a File Report contains the following information:

- Document object\_id
- Document folder\_path and object\_name
- Document owner
- Document modification date
- Document version
- Content format
- Content page number
- Content file name

The following sample report describes a two-page Word document:

```
100015b4800001b5 /roger/research/newproject_1 roger  
4/26/95 19:07:22 1.3 msw6 0  
  
/u120/install/dmadmin/data/rogbase2/content_storage_01  
/000015b4/80/00/01/49.doc  
100015b4800001b5 /roger/research/newproject_1 roger  
4/26/95 19:07:22 1.3 msw6 1  
  
/u120/install/dmadmin/data/rogbase2/content_storage_01  
/000015b4/80/00/01/4a.doc
```

The following sample report describes a single-page Word document with a PDF rendition:

```
090015b4800004f1 /roger/research/newproject_2  
roger 6/16/95 20:00:47 1.7 msw6 0  
  
/u120/install/dmadmin/data/rogbase2/content_storage_01  
/000015b4/80/00/02/52.txt  
090015b4800004f1 /roger/research/newproject_2 roger  
6/16/95 20:00:47 1.7 pdf 0  
  
/u120/install/dmadmin/data/rogbase2/  
content_storage_01/000015b4/80/00/02/6e.pdf
```

#### 17.4.1.21 Group rename

The Group Rename tool renames repository groups. This tool works in conjunction with Documentum Administrator. To rename a group, you must use the Groups pages in Documentum Administrator to identify the group and its new name. Documentum Administrator offers you two options for actually executing the rename operation:

- Running the Group Rename tool immediately after you identify the new name
- Queuing the operation until the next scheduled execution of the Group Rename tool

You cannot use a set method to change a group name. You must go through Documentum Administrator and either a manual or automatic Group Rename

execution to change a group name. The Group Rename tool generates a report that lists the changes made to the repository objects for the group rename. The report is saved in the repository in /System/Sysadmin/Reports/GroupRename. The tool is installed in the inactive state.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on changing the method name.

#### 17.4.1.21.1 Arguments

The Group Rename tool has no arguments.

#### 17.4.1.22 Dm\_LDAPSynchronization

The dm\_LDAPSynchronization tool finds the changes in the user and group information in an LDAP directory server that have occurred since the last execution of the tool and propagates those changes to the repository. If necessary, the tool creates default folders and groups for new users. If there are mapped user or group properties, those are also set.

The tool can:

- Import new users and groups in the directory server into the repository
- Rename users in the repository if their names changed in the directory server
- Rename groups in the repository if their names changed in the directory server
- Inactivate users in the repository that if they were deleted from the directory server.

When using iPlanet, you must enable the changelog feature to use the inactivation operation. Instructions for enabling the changelog feature are found in the *iPlanet documentation*.

The behavior of the tool is determined by the property settings of the dm\_ldap\_config object. The tool has four arguments that you can use to override the property settings controlling which operations the tool performs. These are listed in “[dm\\_LDAPSynchronization arguments](#)” on page 388.

The dm\_LDAPSynchronization tool requires the Java method server. Make sure that the Java method server in your Documentum CM Server installation is running.

The dm\_LDAPSynchronization tool generates a report that is saved in the repository in /System/Sysadmin/Reports/LDAPSynchronization. The tool is installed in the inactive state. After it is activated, it is executed once a day at 4 a.m. by default. Before you set it to the active state, you must define the ldap config object for the repository.

From Documentum CM Server 7.x versions, return codes of the dm\_LDAPSynchronization job have been modified as follows:

- SYNC RETURN SUCCESS = 0
- SYNC RETURN FAILURE = -1
- SYNC RETURN WARNING = 1

#### 17.4.1.22.1 Arguments

[“dm\\_LDAPSynchronization arguments” on page 388](#), describes the arguments for the tool.

**Table 17-16: dm\_LDAPSynchronization arguments**

Argument	Datatype	Default	Description
-deactivate_user_option	Boolean	FALSE	<p>Set to TRUE, directs the job to inactivate users in the repository that have been deleted from the directory server.</p> <p>Setting this overrides the deactivate_user_option property in the ldap config object.</p>
-full_sync	Boolean	FALSE	<p>Set to TRUE, this directs the job to retrieve all entries from the LDAP directory that satisfy the search criteria.</p> <p>FALSE causes the job to import into the repository only new or updated LDAP entries.</p>
-import_mode	string(7)	both	<p>Controls whether the job imports users, groups, or both into the repository. Valid values are: users, groups, and both.</p> <p>Setting this overrides the import_mode property in the ldap config object.</p>

Argument	Datatype	Default	Description
-import_user_ldap_dn	Boolean	TRUE	<p>By default, the dm_LDAPSynchronization job imports the dm_user attribute user_ldap_dn to the repository.</p> <p>If you do want to import this attribute, set the dm_ldap_config.bind_type to bind_search_dn and set the argument import_user_ldap_dn to FALSE.</p> <p><i>OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)</i> contains more information.</p>
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-rename_group_option	Boolean	FALSE	<p>Set to TRUE, directs the job to rename groups in the repository if their names have changed in the directory server.</p> <p>Setting this overrides the rename_group_option property in the ldap config object.</p>

Argument	Datatype	Default	Description
-rename_user_option	Boolean	FALSE	<p>Set to TRUE, directs the job to rename users in the repository if their names have changed in the directory server.</p> <p>Setting this overrides the rename_user_option property in the ldap config object.</p>
-source_directory		dm_all_directories	<p>Controls which LDAP servers are synchronized when the job runs.</p> <p>If not set, all LDAP servers associated with the server configuration object are synchronized. If set to particular LDAP servers, only those servers are synchronized.</p> <p><i>"Explicitly specifying LDAP servers in -source_directory" on page 391</i>, describes how specify multiple servers individually.</p>
-window_interval	integer	1440	Execution window for the tool.

#### 17.4.1.22.2 Executing dm\_LDAPSynchronization manually

You can execute the dm\_LDAPSynchronization tool manually from the command line. The syntax is

```
java com.documentum.ldap.LDAPSync -docbase_name <repositoryname> -user_name
<superuser_login> -method_trace_level <integer> -full_sync true
```

where <repositoryname> is the name of the repository, <superuser\_login> is the login for a Superuser, and <integer> is the required trace level for the method.

#### 17.4.1.22.3 Explicitly specifying LDAP servers in -source\_directory

Use the object name of LDAP server to identify the server in the -source\_directory argument. If you want to identify multiple servers, use the following syntax:

```
ldap_config_obj_name+ldap_config_obj_name{+ldap_config_obj_name}
```

where ldap\_config\_object\_name is the object name value of the ldap config object for the LDAP directory server. For example:

```
ldap_engr1+ldap_engr2+ldapQA
```

#### 17.4.1.23 Log purge

The Log Purge tool deletes old log files. “[Files deleted by the log purge](#)” on page 391, lists the log files deleted by Log Purge.

**Table 17-17: Files deleted by the log purge**

Log file or report	Location
Server log files	Documentum CM Server installation log location
dmbasic method server	Documentum CM Server installation log location
Connection broker log files	Documentum CM Server installation log location
Agent Exec log files	Documentum CM Server installation log location
Session log files	Documentum CM Server installation log location
Result log files	Temp cabinet
Job log files	Temp cabinet
Job reports	/System/Sysadmind/Reports folder
Lifecycle log files	Documentum CM Server installation log location
Method server log files	Documentum CM Server installation log location, MethodServer subdirectory

Result log files are generated by the execution of methods when the SAVE\_RESULTS argument of method is set. Result log files are stored in Temp/Result.method\_name.

Job log files are generated when a job is run. The job log file for tools contains the trace file of job and the text of its report. Job log files are stored in Temp/Jobs/job\_name/log\_file.

The lifecycle log files are generated when a lifecycle operation such as promote or demote occurs. The files are named bp\_transition\_\*.log or bp\_schedule\_\*.log,

depending on the operation. They are stored in %\DOCUMENTUM%\dba\log\repository\_id\bp (\$DOCUMENTUM/dba/log/repository\_id/bp).

Files are considered old and are deleted if they were modified prior to a user-defined cutoff date. By default, the cutoff date is 30 days prior to the current date. For instance, if you run Log Purge on July 27, all log files that were modified before June 28 are deleted. You can change the cutoff interval by setting the -cutoff\_days argument for the tool. “[Arguments](#)” on page 392 provides instructions.

Log Purge generates a report that lists all directories searched and the files that were deleted. The report is saved in the repository in /System/Sysadmin/Reports/LogPurge.



**Note:** If the tool is run at a remote distributed site, the report name has the server configuration name appended with name of site. For example, if London is a remote site, its report is found in /System/Sysadmin/Reports/LogPurgeLondon.

The Log Purge tool is installed in the inactive state.

#### 17.4.1.23.1 Arguments

“[Log purge arguments](#)” on page 392, lists the arguments for the tool.

**Table 17-18: Log purge arguments**

Argument	Datatype	Default	Description
-cutoff_days	integer	30	Controls what logs are deleted. All logs older than the specified number of days are deleted.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	120	Execution window for the tool.

#### 17.4.1.23.2 Guidelines

Your business rules will determine how long you keep old log files and result log files. However, we recommend that you keep them at least 1 month as you may need them to debug a problem or to monitor the result of a method or job.

We recommend that you run this tool daily. This ensures that your repository never has log files older than the number of days specified in the cutoff\_days argument.

#### 17.4.1.23.3 Report sample

The following is a sample of a Log Purge report. Its start\_date property is set to June 3, 1996. The cutoff\_days argument is set to 30 so that all logs older than 30 days will be deleted. The report looks for server and connection broker logs, session logs, and result logs from method objects and job objects (older than 30 days) and destroys them.

```

LogPurge Report For DocBase boston2
As Of 7/25/96 7:18:09 PM
Parameters for removing Logs:
-----
- Inbox messages will be queued to boston2
- Logs older than 30 days will be removed...

Looking for server and connection broker logs in the log
location...
Log Location: log
Log Location File Path: /u106/dm/dmadmin/dba/log
Changing directory to server log location:
/u106/dm/dmadmin/dba/log
Looking for session logs...
The top-level session log directory is:
/u106/dm/dmadmin/dba/log/00000962
Changing directory to:
/u106/dm/dmadmin/dba/log/00000962/boston2
Removing /u106/dm/dmadmin/dba/log/00000962/
boston2/01000962800008be
Removing /u106/dm/dmadmin/dba/log/00000962/
boston2/01000962800008e0
Removing /u106/dm/dmadmin/dba/log/00000962/
boston2/0100096280000904
Removing /u106/dm/dmadmin/dba/log/00000962/
boston2/0100096280000e28
Removing /u106/dm/dmadmin/dba/log/00000962/
boston2/0100096280000e72
Removing /u106/dm/dmadmin/dba/log/00000962/
boston2/0100096280000ed7
Changing directory to:
/u106/dm/dmadmin/dba/log/00000962/dmadmin
Removing /u106/dm/dmadmin/dba/log/00000962/
dmadmin/01000962800008b9
Removing /u106/dm/dmadmin/dba/log/00000962/
dmadmin/01000962800008ba
Removing /u106/dm/dmadmin/dba/log/00000962/
dmadmin/01000962800008b7
Removing /u106/dm/dmadmin/dba/log/00000962/
dmadmin/01000962800008b8
Changing directory to:
/u106/dm/dmadmin/dba/log/00000962/tuser3
Removing /u106/dm/dmadmin/dba/log/00000962/tuser3/
01000962800008fd
Changing directory to:
/u106/dm/dmadmin/dba/log/00000962/tuser1
Changing directory to:
/u106/dm/dmadmin/dba/log/00000962/agentexec

```



```
Destroying 06/05/96 11:40:02 boston1 object
Destroying 05/29/96 11:40:06 boston1 object
Destroying 05/30/96 11:40:49 boston1 object

End of Log Purge Report
Report End 7/25/96 7:19:13 PM
```

### 17.4.1.24 Queue management

The Queue Management Tool deletes dequeued Inbox items. Whenever an item is queued to the Inbox of a user, an object of type dmi\_queue\_item is created for that queued item. When users forward or otherwise remove an item from their Inboxes, the corresponding dmi\_queue\_item object is marked dequeued, but it is not removed from the repository. If these dequeued items are not removed, the tables for the dmi\_queue\_item type grow quite large, and performance degrades when users access their Inboxes. The Queue Management tool automates the task of removing these unneeded dmi\_queue\_item objects.

The cutoff\_days and custom\_predicate arguments determine which dmi\_queue\_items are removed. The cutoff\_days argument specifies the age of the objects you want to delete. The custom\_predicate argument is applied to those items meeting the age requirement, allowing you to delete all or only some of them. For example, the tool could delete all dequeued dmi\_queue\_items that are older than 30 days and were queued to a specific user.

The tool generates a status report that provides you with a list of the deleted dmi\_queue\_items. The report is saved in the repository in /System/Sysadmin/Reports/QueueMgt.

If there is an error in the execution of tool, an email and Inbox notification is sent to the user specified by the -queueperson argument.

The Queue Management tool is installed in the inactive state.

#### 17.4.1.24.1 Arguments

[“Queue management arguments” on page 396](#), lists the arguments for the tool.

**Table 17-19: Queue management arguments**

<b>Argument</b>	<b>Datatype</b>	<b>Default</b>	<b>Description</b>
-custom_predicate <i>qualification</i>	string	-	<p>Defines a WHERE clause qualification for the query that selects dequeued items for deletion.</p> <p>The qualification must be a valid qualification and must work against the dmi_queue_item object. For example, a valid qualification is "event='APPROVED'" or "name='dmadmin'".</p> <p>Refer to the <i>OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)</i> for complete information about WHERE clause qualifications.</p>
-cutoff_days	integer	90	<p>Defines a minimum age, in days, for dequeued items. All dequeued dmi_queue_items older than the specified number of days and that meet the specified qualification are deleted.</p> <p>To include all dequeued items in the search, set this value to zero (0).</p>
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.

Argument	Datatype	Default	Description
-window_interval	integer	120	Execution window for the tool.



**Note:** The tool creates a base qualification that contains two conditions:

- delete\_flag = TRUE
- dequeued\_date = *value* (computed using cutoff\_days argument)

Any qualification you add is appended to the base qualification.

#### 17.4.1.24.2 Guidelines

Dequeued items are the result of moving objects out of an inbox. Objects are placed in inboxes by workflows, event notifications, archive and restore requests, or explicit queue methods. Objects are moved out of an inbox when they are completed or delegated.

You must decide if there are any reasons to keep or maintain dequeued items. For example, you may want to keep dequeued items for auditing purposes. If so, leave this tool inactive or set the cutoff\_days argument to a value that will save the dequeued items for a specified length of time.

After you have made your decisions, formulate a scheduling plan.



**Note:** The first time you execute the Queue Management tool, it may take a long time to complete if dequeued items have never been deleted before.

#### 17.4.1.24.3 Report sample

Here is a sample of the report generated by the Queue Management tool.

```

QueueMgt Report For DocBase boston2
As Of 7/26/96 5:09:00 PM
Parameters for removing dequeued items:
-----
- Inbox messages will be queued to dmadmin
- No items dequeued before 7 days will be removed...
- The custom predicate is:
  name='tuser5'

Looking for dequeued items to delete...
Destroying queue item with ID 1b00096280000603
Destroying queue item with ID 1b000962800002e4
Destroying queue item with ID 1b00096280000304
Destroying queue item with ID 1b00096280000324
Destroying queue item with ID 1b00096280000344
5 dequeued items deleted...

End of Queue Management Report
Report End 7/26/96 5:09:00 PM

```

### 17.4.1.25 Remove expired retention objects

The Remove Expired Retention Objects (RemoveExpiredRetnObjects) tool removes objects from the repository whose content, stored in an Centera storage area, has an expired retention date. The tool does not remove the actual content files or the associated content objects.

The tool invokes the CHECK\_RETENTION\_EXPIRED administration method to determine which SysObjects to remove from the repository. By default, the tool operates only on objects stored in Centera storage areas that require a retention date. You can also direct the tool to operate on Centera storage areas that allow but do not require a retention date by setting the INCLUDE\_ZERO\_RETENTION\_OBJECTS argument. The tool never includes objects stored in Centera storage areas that do not allow retention periods. Refer to the Guidelines for more information.

After the tool runs the method to find the objects, it uses a destroy method to remove them from the repository.

The tool generates a status report that provides you with a list of the deleted objects. The report is saved in the repository in /System/Sysadmin/Reports/RemoveExpiredRetnObjects. For each deleted object, the report lists the following properties:

- r\_object\_id
- object\_name
- a\_storage\_type
- r\_creation\_date
- retention\_date

The retention\_date property is a computed property.

The tool is installed in the inactive state.

#### 17.4.1.25.1 Arguments

“Remove expired retention objects arguments” on page 398, describes the arguments for the tool.

**Table 17-20: Remove expired retention objects arguments**

Argument	Datatype	Default	Description
-query <i>qualification</i>	string	-	Identifies which objects are selected for possible removal.  This is a DQL where clause qualification.

Argument	Datatype	Default	Description
-include_zero_retention_objects	Boolean	F (FALSE)	Setting this to T (TRUE) directs the job to consider objects stored in a Centera storage area that allows but does not require a retention period.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	1440	Execution window for the tool.

#### 17.4.1.25.2 Guidelines

A Centera or NetApp SnapLock storage area can have three possible retention period configurations:

- The storage area may require a retention period.

In this case, the a\_retention\_attr name property is set and the a\_retention\_attr\_req is set to T.

- The storage area may not allow a retention period.

In this case, the a\_retention\_attr name property is not set and the a\_retention\_attr\_req is set to F.

- The storage area may allow but not require a retention period.

In this case, the a\_retention\_attr name property is set , but the a\_retention\_attr\_req is set to F.

By default, the method does not include objects whose content has a 0 retention period because the assumption is that such content is meant to be kept forever. However, in a storage area that allows but does not require a retention period, a 0 retention period can be result from two possible causes:

- The user deliberately set no retention period, and consequently, the server set the retention period to 0
- The user specified a retention date that had already elapsed. When this occurs, the server sets the retention period to 0.

Because the meaning of 0 is ambiguous in such storage areas, the tool supports the INCLUDE\_ZERO\_RETENTION\_OBJECTS argument to allow you to include

content with a zero retention in storage areas that allow but do not require a retention period.

If you set INCLUDE\_ZERO\_RETENTION\_OBJECTS to T, when the tool examines objects in storage areas that allow but do not require a retention period and it will remove from the repository any object with an expired or zero retention period. the tool does not remove the actual content files or associated content objects. (You must run dmclean to remove those.)

The *OpenText Documentum Content Management - Server DQL Reference Guide* (EDCCS250400-DRD) contains information on the underlying method.

#### 17.4.1.25.3 Report sample

```
--- Start C:\Documentum\dba\log\00002710\sysadmin\
RemoveExpiredRetnObjectsDoc.txt report output ---
RemoveExpiredRetnObjects Report For DocBase dctm52
As Of 2/26/2004 15:39:10

RemoveExpiredRetnObjects utility syntax:
apply,c,NULL,CHECK_RETENTION_EXPIRED,
QUERY,S,'a_storage_type = ''destroy_test3'''
,INCLUDE_ZERO_RETENTION_OBJECTS,B,T
Executing RemoveExpiredRetnObjects...
Object 090027108000c910 destroyed successfully.
Object 090027108000c911 destroyed successfully.
# of objects with expired retention that matched
the condition: 2
# of successfully destroyed: 2
# of objects not destroyed : 0
Report End 2/26/2004 15:39:14
--- End C:\Documentum\dba\log\00002710\sysadmin\
RemoveExpiredRetnObjectsDoc.txt report output ---
```

#### 17.4.1.26 Rendition manager

The Rendition Manager tool removes unwanted renditions of versioned documents. A rendition is a copy of content of a document in a different format than the original. Renditions, such as the original content files, are stored in storage areas. Over time, unneeded renditions from previous versions of documents can take up noticeable amounts of disk space. For information about renditions, refer to *OpenText Documentum Content Management - Server Fundamentals Guide* (EDCCS250400-GGD).

The arguments of the tool define which renditions are removed. The tool can delete renditions based on their age, format, or source (client- or server-generated). The tool removes the content objects associated with unwanted renditions. The next execution of the Dmclean tool automatically removes the orphaned content files (assuming that clean\_content argument of Dmclean is set to TRUE) of rendition.



**Note:** Renditions with the page modifier dm\_sig\_template are never removed by Rendition Manager. These renditions are electronic signature page templates; they support the electronic signature feature available with Trusted Content Services.

The report generated by the tool lists the renditions targeted for removal. The report is saved in the repository in /System/Sysadmin/Reports/RenditionMgt.

The Rendition Manager tool is installed in the inactive state.

#### 17.4.1.26.1 Arguments

[“Rendition manager arguments” on page 401](#), describes the arguments for the Rendition Manager tool.

**Table 17-21: Rendition manager arguments**

Argument	Datatype	Default	Description
-keep_slabs	Boolean	TRUE	Indicates whether you wish to keep renditions with symbolic labels. When this is TRUE, the -keep_current argument is ignored because CURRENT is a symbolic label.
-keep_current	Boolean	TRUE	Indicates whether you wish to keep renditions of documents with the symbolic label CURRENT. When this is TRUE, the CURRENT version is always kept even if -keep_slabel is set to FALSE.

Argument	Datatype	Default	Description
-keep_keep_flag	Boolean	TRUE	<p>Controls whether content objects with a rendition property value of 3 are deleted by the tool. T (TRUE) instructs the tool to not delete the objects.</p> <p>The default value is F (FALSE), meaning the content objects are not deleted.</p> <p> <b>Note:</b> The rendition property in a content object is set to 3 when a rendition is added to content with the keepRendition argument in the addRendition method set to T (TRUE).</p>
-keep_esignature	Boolean	TRUE	<p>Controls whether renditions with the page modifier dm_sig_source are removed.</p> <p>T (TRUE) means to keep those renditions. F (FALSE) means to remove those renditions.</p>
-cutoff_days	integer	180	The maximum age, in days, of renditions that you want to keep. All renditions older than the specified number of days are considered for deletion.

Argument	Datatype	Default	Description
-server renditions	string	all	<p>Specifies which server-based renditions to remove. Valid values are:</p> <ul style="list-style-type: none"> <li>all</li> <li>none</li> <li>or a list of formats</li> </ul> <p>If a list of formats is specified, the format names must be separated by single spaces.</p> <p>The default is all.</p>
-client renditions	string	none	<p>Specifies which client renditions to remove (includes the renditions added using an addRendition method). Valid values are:</p> <ul style="list-style-type: none"> <li>all</li> <li>none</li> <li>or a list of formats</li> </ul> <p>If a list of formats is specified, the format names must be separated by single spaces.</p> <p>The default is none.</p>
-report only	Boolean	TRUE	Indicates whether to generate only a report and not delete renditions. Set this to FALSE if you want to actually delete the renditions in addition to generating a report.

Argument	Datatype	Default	Description
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	120	Execution window for the tool.

#### 17.4.1.26.2 Guidelines

The Rendition Manager tool removes all renditions that meet the specified conditions and are older than the specified number of days. For example, if you execute this tool on July 30 and the -cutoff\_days argument is set to 30, then all renditions created or modified prior to June 30 are candidates for deletion. On July 31, all renditions created or modified before July 1 are removed.

OpenText recommends that you run this tool with the -report\_only argument set to TRUE first to determine how much disk space renditions are using and what type of renditions are in the repository. With -report\_only set to TRUE, you can run the tool several times, changing the other arguments each time to see how they affect the results.

OpenText recommends that you have a thorough knowledge of how and when renditions are generated before removing any. For example, client renditions, such as those added explicitly by an Addrendition method, may be difficult to reproduce if they are deleted and then needed later. Documentum CM Server renditions are generated on demand by the server and are generally easier to reproduce if needed.

To make sure that your repository never has rendition files older than the number of days specified in the -cutoff\_days argument, run this tool daily.



**Note:** The first time you execute the Rendition Manager tool, it may take a long time to complete if the old renditions have never been deleted before.

### 17.4.1.26.3 Report sample

Here is a sample of the Rendition Manager report.

```
RenditionMgt Report For DocBase boston2
As Of 7/27/96 3:57:01 PM
Parameters for removing renditions:
-----
- Inbox messages will be queued to dmadmin
- No renditions accessed in the last 0 days will
be removed...
- Renditions of documents having symbolic labels
will be removed...
- Renditions for the current version will NOT
be removed...
- This will generate a report only; no renditions
will be removed...
- The following client renditions are candidates
for removal:
  1) mactext
- The following server renditions are candidates
for removal:
  1) crtext

NOTE: This is a report only - no renditions will be
removed

Querying for renditions...
Object NameOwner Name FormatAccess DateRendition Type
RenditionMgtdmadmincrtext07/27/96 15:44:31server
RenditionMgtdmadmincrtext07/27/96 15:45:31server
RenditionMgtdmadmincrtext07/27/96 15:45:31server
teststatus2boston2crtext07/24/96 18:40:23server
SwapInfodmadmincrtext07/11/96 16:16:16server
DBWarningdmadmincrtext07/12/96 18:31:11server
foo717bbbdmadmincrtext07/24/96 20:48:46server
ContentWarningdmadmincrtext07/18/96 18:01:19server
...
...
SwapInfodmadmincrtext07/27/96 13:20:47server
RenditionMgtdmadmincrtext07/27/96 15:48:09server
rend722 dmadminmactext07/02/96 11:00:11client/external
rend722dmadminmactext07/02/96 11:02:13client/external
rendz2dmadminmactext07/02/96 11:05:04client/external
rendyy2dmadminmactext07/02/96 12:16:10client/external
rendww2dmadminmactext07/02/96 12:27:05client/external
foor717atuser4mactext07/17/96 17:48:25client/external
foor725atuser5mactext07/25/96 12:05:07client/external
Report Summary:
-----
The Docbase has a total of 39,216 kbytes of content.
54 renditions were reported.
The renditions reported represent 82 kbytes of content
or 0.21%
End of Rendition Management Report
Report End 7/27/96 3:57:10 PM
```

### 17.4.1.27 SCS log purge (dm\_SCSLogPurgeJob)

Only repositories where you have installed Site Caching Services 5.2 or later contain this job and its associated method. It is similar to the Log Purge job.

Files are considered old and are deleted if they were modified prior to a user-defined cutoff date. By default, the cutoff date is 30 days prior to the current date. For instance, if you run SCS Log Purge on July 27, all log files that were modified before June 28 are deleted. You can change the cutoff interval by setting the -cutoff\_days argument for the tool.

SCS Log Purge generates a report that lists all directories searched and the files that were deleted. The report is saved in the repository in /System/Sysadmin/Reports/SCSLogPurge.

The SCS Log Purge tool is installed in the inactive state.

### 17.4.1.28 State of repository report

The State of the Repository Report tool generates a report to help you troubleshoot repository problems. A partial list of the information included in the report is:

- The property values in the repository configuration object
- Server initialization information from the server.ini file
- The directory paths defined by the location objects in the server configuration object
- Version numbers of your server, RDBMS, and operating system

The report is saved in the repository in /System/Sysadmin/Reports/StateOfDocbase.

The State of the Repository tool is installed in the active state.

#### 17.4.1.28.1 Arguments

"State of the repository arguments" on page 406, describes the argument of tool.

**Table 17-22: State of the repository arguments**

Argument	Datatype	Default	Description
-window_interval	integer	720	Execution window for the tool.

### 17.4.1.28.2 Report sample

Here is a sample report from the State of the Repository tool. The example shows all of the sections in the report of tool, but truncates entries in some sections in the interests of space.

```
StateOfDocbase Report For Docbase dm_master As Of 4/12/1999 09:26:32

Docbase Configuration:
Description:The Test Repository
Federation Name:<dm_master is not in a Federation>
Docbase ID:22000
Security Modeacl
Folder Security:On
Authorization Protocol:<Not defined>
Database:SQLServer
RDBMS Index Store:<Not defined>
Mac Access Protocol:none

Server Configuration:
Server Name:dm_master
Server Version:4.0 Win32.SQLServer7
Default ACL:Default ACL of User
Host Name:bottae1
Install Owner:dmadmin
Install Domain:bottae1
Operator Name:dm_master
Agent Launcher:agent_exec_method
Checkpoint Interval:300 seconds
Compound Integrity:On - Server enforces integrity for virtual documents
Turbo Backing Store:filestore_01
Rendition Backing Store:<Not defined>
Web Server Location:BOTTAE1
Web Server Port:80
Rightsite Image:/rs-bin/RightSit

Server Locations:
events_locationD:\DOCUMENTUM\share\data\events
common_locationD:\DOCUMENTUM\share\data\common
temp_locationD:\DOCUMENTUM\share\temp
log_locationD:\DOCUMENTUM\dba\log
system_converter_location D:\DOCUMENTUM\product\4.0\convert
user_converter_location<Not defined>
verity_locationD:\DOCUMENTUM\product\4.0\verity
user_validation_location <Not defined>
assume_user_locationD:\DOCUMENTUM\dba\dm_assume_user.exe
change_password_locationD:\DOCUMENTUM\dba\dm_change_password.exe
signature_chk_locD:\DOCUMENTUM\dba\dm_check_password.exe
stage_destroyer_location<Not defined>

Set Information:
CLASSPATH=C:\PROGRA~1\DOCUME~1\DFCRE40\lib\dfc.jar;C:\PROGRA~1\DOCUME~1\Classes;
COLORS=white on blue
COMPUTERNAME=BOTTAE1
ComSpec=C:\WINNT\system32\cmd.exe
CVSROOT=godzilla.documentum.com:/docu/src/master
CVS_SERVER=cvs1-9
DM_HOME=D:\DOCUMENTUM\product\4.0
DOCUMENTUM=D:\DOCUMENTUM
HOMEDRIVE=C:
HOME DRIVE=C:
HOME PATH=\BOTTAE1
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Os2LibPath=C:\WINNT\system32\os2\dll;
Path=D:\DOCUMENTUM\product\4.0\bin;C:\PROGRA~1\DOCUME~1\DFCRE40\bin;
D:\DOCUMENTUM\product\3.1\bin;C:\WINNT\system32;C:\WINNT;
c:\program files\maestro.nt;C:\PROGRA~1\DOCUME~1\Shared;
```

```
c:\SDK-Java.201\Bin;c:\SDK-Java.201\Bin\PackSign;c:\Winnt\Piper\dll;
c:\Program Files\DevStudio\SharedIDE\bin;
c:\Program Files\DevStudio\SharedIDE\bin\ide;D:\MSSQL7\BINN;
c:\cvs1.9;c:\csh\bin;c:\csh\samples;C:\DOCUME~1\RIGHTS~1\product\bin
PATHEXT=.COM;.EXE;.BAT;.CMD
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 5 Model 2 Stepping 5, GenuineIntel
PROCESSOR_LEVEL=5
PROCESSOR_REVISION=0205
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINNT
TEMP=C:\TEMP
TMP=C:\TEMP
USERDOMAIN=BOTTAE1
USERNAME=dmadmin
USERPROFILE=C:\WINNT\Profiles\dmadadmin
windir=C:\WINNT
```

#### Registered tables in the Repository:

Table NameTable OwnerOwner:Group:World Permits

```
adm_turbo_sizedbo 1:1:1
dm_federation_logdbo 15:7:3
dm_portinfodbo 1:1:1
dm_queuedbo 1:1:1
```

#### Number of Documents by Type:

Document Type	Count
dmi_expr_code	74
dm_method	66
dm_document	44
dm_folder	31
dm_job	29
dm_location	14
dm_registered	14
dm_procedure	10
dm_cabinet	6
dm_script	3
dm_smart_list	2
dm_business_pro	1
dm_docbase_config	1
dm_mount_point	1
dm_outputdevice	1
dm_query	1
dm_server_config	1
Total:	-----
	299

#### Number of Documents by Format:

Document Format	Count
crtext	11
mdoc55	9
maker55	5
<NO CONTENT>	2
msw8template	2
vrf	2
wp6	2
excel5book	1
excel8book	1
excel8template	1
ms_access7	1
ms_access8_mde	1
msw6	1
msw8	1
powerpoint	1
ppt8	1

<table border="1"> <tbody> <tr><td> </td><td> </td></tr> <tr><td>ppt8_template</td><td>1</td></tr> <tr><td>ustn</td><td>1</td></tr> <tr><td>Total:</td><td>-----</td></tr> <tr><td></td><td>44</td></tr> </tbody> </table>			ppt8_template	1	ustn	1	Total:	-----		44	
ppt8_template	1										
ustn	1										
Total:	-----										
	44										
<b>Number of Documents by Storage Area:</b>											
Storage Area	Count										
filestore_01	40										
dm_turbo_store	4										
Total:	-----										
	44										
<b>Content Size(KB) by Format:</b>											
FormatLargestAverageTotal											
mdoc5515885772											
crtext 10115436											
text19621254											
vrf 192119238											
maker553722114											
<b>Content Size(KB) by Renditions:</b>											
FormatLargestAverageTotal											
<b>Content Size(KB) Summary:</b>											
filestore_01											
Largest Content:	196										
Average Content:	31										
Total Content:	2,092										
dm_turbo_store											
Largest Content:	8										
Average Content:	5										
Total Content:	34										
-----											
GTotal Content:	2,127										
GTotal Rendition:	(0.00% of total content)										
<b>Number of Users and Groups:</b>											
Named Users	4										
Groups	2										
<b>ACL Summary:</b>											
Number of ACLs:	33										
Number of Internal ACLs:	29										
Number of External System ACLs:	4										
Number of External Private ACLs:											
<b>Report End</b> 4/12/1999 09:26:54											

### 17.4.1.29 Swap info

The Swap Info tool uses operating system commands to retrieve information about swap space usage and availability. The tool generates a report but does not issue warnings because there is no realistic way to determine if the swap space is too low as this determination has too many variables. The status report is saved in the repository in /System/Sysadmin/Reports/SwapInfo.



**Note:** If the tool was run at a remote distributed site, the report name has the server configuration name appended with name of site. For example, if London is a remote site, its report would be found in /System/Sysadmin/Reports/SwapInfoLondon.

The Swap Info tool is installed in the active state.

#### 17.4.1.29.1 Arguments

"Swap info arguments" on page 410, describes the arguments for the tool.

**Table 17-23: Swap info arguments**

Argument	Datatype	Default	Description
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	120	Execution window for the tool.

#### 17.4.1.29.2 Report sample

The format of the report generated by Swap Space Info varies by operating system. Here is a sample:

```
SwapInfo Report For DocBase boston2
As Of 7/26/96 4:00:59 PM
Summary of Total Swap Space Usage and Availability:

total: 59396k bytes allocated + 49216k reserved =
 108612k used, 287696k available
Swap Status of All Swap Areas:
swapfile      dev swaplo blocks   free
/dev/dsk/c0t3d0s1  32,25      8 717688 626640
Report End 7/26/96 4:00:59 PM
```

### 17.4.1.30 Update statistics

The Update Statistics tool generates current statistics for the RDBMS tables owned by the repository owner. Generating statistics is always useful, particularly after you perform load operations or if table key values in the underlying RDMBS tables are not normally distributed.

When you run the tool against an Oracle or Sybase database, the tool uses a file that contains commands to tweak the database query optimizer. For Oracle, the file is named `custom_oracle_stat.sql`. For Sybase, it is named `custom_sybase_stat.sql`. The file is stored in `%DOCUMETNUM%\dba\config\repository_name($DOCUMETNUM /dba/config/repository_name)`. You can add commands to this file. However, do so with care. Adding to this file affects query performance. If you do add a command, you can use multiple lines, but each command must end with a semi-colon (`:`). You cannot insert comments into this file.

The `-dbreindex` argument controls whether the method also reorganizes database tables in addition to computing statistics. For SQL Server, you can set the argument to either READ or FIX. Setting it to READ generates a report on fragmented tables but does not fix them. Setting it to FIX generates the report and fixes the tables. (In either case, the report is included in the overall job report.)

For Sybase, the `-dbreindex` argument is only effective if set to FIX, to reorganize the tables. Setting it to READ does not generate a report on Sybase. If you include the `-dbreindex` argument set to FIX, the repository owner (the account under which the tool runs) must have sa role privileges in the database.

The `-dbreindex` argument has no effect on a Oracle database.

The tool generates a report that is saved in the repository in System/Sysadmin/Reports/UpdateStats. The exact format of the report varies for each database.

The Update Statistics tool is installed in the active state, running once a week. Because this tool can be CPU and disk-intensive, it is recommended that you run the tool during off hours for database use. Consult with your RDBMS DBA to determine an optimal schedule for this tool.

#### 17.4.1.30.1 Arguments

[“Update statistics arguments” on page 412](#), lists the arguments for the tool.

**Table 17-24: Update statistics arguments**

<b>Argument</b>	<b>Datatype</b>	<b>Default</b>	<b>Description</b>
-dbreindex	string	READ	<p>Controls whether the tool actually updates statistics or only reports on RDBMS tables that need updating.</p> <p>READ generates only the report. This setting is valid only for SQL Server database.</p> <p>FIX generates the report and updates the tables. This setting is valid on SQL Server and Sybase databases. However, on Sybase, it only fixes the tables. A report is not generated.</p> <p>This argument is not available for Oracle databases.</p>
-server_name	string(32)	-	<p>Name of the database server.</p> <p>This is a required argument on SQL Server and Sybase. It is set for the job when the administration tools are installed in repositories running against a SQL Server or Sybase database.</p>
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	120	Execution window for the tool.

#### 17.4.1.30.2 Guidelines

Run this tool after you perform large loading operations.

When the job is run with -dbreindex set to READ and the statistics need updating, the report will say:

```
-dbreindex READ. If rows appear below, the corresponding
tables are fragmented.
Change to -dbreindex FIX and rerun if you want to reindex
these tables.
```

When the job is run with -dbreindex set to FIX, the report will say:

```
-dbreindex FIX. If rows appear below, the corresponding
tables have been reindexed.
Change to -dbreindex READ if you do not want to reindex
in the future.
```

#### 17.4.1.30.3 Report sample

The Update Statistics report tells you when the tool was run and which tables were updated. The report lists the update statistics commands that it runs in the order in which they are run. Here is a sample of the report:

```
Update Statistics Report:

Date of Execution: 06-04-96

update statistics dmi_object_type
go
update statistics dm_type_s
go
update statistics dm_type_r
go
update statistics dm_type_r
go
update statistics dmi_index_s
go
.
.
.
End of Update Statistics Report
```

#### 17.4.1.31 Usage tracking (dm\_usageReport)

Documentum CM Server tracks software usage by recording login times. The Documentum CM Server global registry contains a registered table, dm\_usage\_log. This table contains a record of the first and the latest login time for each user of each application that connects to Documentum CM Server. A user, dm\_report\_user, was created when the global registry was configured. This user has read-only access to the dm\_usage\_log table. The initial password for dm\_report\_user is the global registry user password.

The dm\_usageReport job runs monthly to generate a usage report. “[Viewing job reports](#)” on page 441 contains the information to view the report. You can also generate a current report. “[Running jobs](#)” on page 440 contains the information to generate a current report.

The information stored in dm\_usage\_log can also be exported from the global registry by using a utility program. Execute the following Java utility:

```
java com.documentum.server.impl.method.license.ExportUsageLog repository  
dm_report_user password
```

Where `repository` is the global registry name and `password` is the `dm_report_user` password. Use your OS shell tools to redirect the output to a file.

### 17.4.1.32 User change home repository

The UserChgHomeDb tool changes the home repository of a user. This job works in conjunction with Documentum Administrator. To change the home repository of a user, you must connect to the repository using Documentum Administrator and make the change through the Users pages. Documentum Administrator gives you two options for performing the change:

- Execute the UserChgHomeDb tool immediately after you save the change
- Queue the change, to be performed at the next scheduled execution of UserChgHomeDb.

You cannot change the home repository of a user using a set method. When the home repository of a user changes, the change must be cascaded to several other objects that make use of it.

The UserChgHomeDb tool generates a report that lists the objects changed by the operation. The report is saved in the repository in `/System/Sysadmin/Reports/UserChgHomeDb`.

The User Chg Home Db tool is installed in the inactive state.

#### 17.4.1.32.1 Arguments

The UserChgHomeDb tool has no arguments.

### 17.4.1.33 User rename

The User Rename tool changes the repository name of a user. This job works in conjunction with Documentum Administrator. To change the name of a user, you must connect to the repository using Documentum Administrator and make the change through the Users screens. Documentum Administrator gives you two options for performing the change:

- Execute the User Rename tool immediately after you save the change
- Queue the change, to be performed at the next scheduled execution of User Rename.

You cannot change the name of a user name using the Set method. When the name of a user changes, the change must be cascaded to many other objects that make use of it.

The User Rename tool generates a report that lists the objects changed by the operation. The report is saved in the repository in /System/Sysadmin/Reports/UserRename.

The User Rename tool is installed in the inactive state.



**Note:** The unlock\_locked\_obj argument is introduced in dm\_LDAPSynchronization job to preserve lock or unlock on objects that are associated with the user who is affected by the UserRename job. Set the unlock\_locked\_obj argument value to <False> to preserve lock.

#### 17.4.1.33.1 Arguments

The User Rename tool has no arguments.

#### 17.4.1.33.2 Report sample

This sample report was generated when the tool was run in Report Only mode.

```
Job: dm_UserRename
Report For Repository example.db_1;
As Of 3/6/2000 12:00:27 PM

=====
3/6/2000 12:00:28 PM=====
Reporting potential changes in repository example.db_1
when renaming user 'dm_autorender_mac' to 'test'.

The following user rename options were specified:
Execution Mode: Report Only
Checked out Objects: Unlock
WARNING: There are 15 sessions currently open. It is
recommended that user rename is performed in single
user connection mode.

=====
DM_USER OBJECT =====
Object type : dm_user
Object id : 1100162180000103
Name : dm_autorender_mac
propertys referencing user dm_autorender_mac: user_name
-----
===== ACL Objects referencing user dm_autorender_mac ====
-----
Object type : dm_acl
Object id : 450016218000010c
Name : dm_450016218000010c
propertys referencing user dm_autorender_mac:
owner_name
-----
**** Number of ACL objects affected: 1

===== Alias Set Objects referencing user dm_autorender_mac ====
**** Number of Alias Set objects affected: 0

===== Dm_user object. Default ACL of user object is
referencing dm_autorender_mac
-----
Object type : dm_user
Object id : 1100162180000103
Name : dm_autorender_mac
propertys referencing user dm_autorender_mac: acl_domain
-----
===== Sysobjects referencing user 'dm_autorender_mac',
which are not locked
**** Number of sysobjects affected: 0
```

```
===== Sysobject referencing user 'dm_autorender_mac',
which are locked (all the objects in this list will be
unlocked and modified)
**** Number of sysobjects affected: 0

===== Sysobjects locked by user 'dm_autorender_mac' ==
(all the objects in this list will be unlocked)
**** Number of sysobjects affected: 0

===== Routers referencing user dm_autorender_mac. ===
**** Number of router objects affected: 0

===== Workflow objects referencing user
dm_autorender_mac.
**** Number of dm_workflow objects affected: 0

===== Activity objects referencing user
dm_autorender_mac.
**** Number of dm_activity objects affected: 0

===== Workitem objects referencing user
dm_autorender_mac.
**** Number of dmi_workitem objects affected: 0

===== Groups referencing user dm_autorender_mac. ===
-----
Object type : dm_group
Object id : 1200162180000100
Name : docu
propertys referencing user dm_autorender_mac:
users_names[2]
-----
**** Number of group objects affected: 1

===== dmi_queue_item objects referencing user
dm_autorender_mac.
**** Number of dmi_queue_item objects affected: 0

===== dmi_registry objects referencing user
dm_autorender_mac.
**** Number of dmi_registry objects affected: 0

===== The following dm_registered objects have table_owner
property referencing user dm_autorender_mac. The script
will not update the objects. You have to modify them manually.

===== The following dm_type objects have owner_name
property referencing user dm_autorender_mac. The script
will not update the objects. You have to modify them
manually.

===== The following dmi_type_info objects have acl_domain
property referencing user dm_autorender_mac. The script
will not update the objects. You have to modify them manually.

-----3/6/2000 12:00:28 PM-----
```

### 17.4.1.34 Version management

The Version Management tool removes unwanted versions of documents from the repository. This tool automates the destroy and prune methods. Refer to *OpenText Documentum Content Management - Server Fundamentals Guide (EDCCS250400-GGD)* for a discussion of how versioning works. The tool removes only the repository object. It does not remove content files associated with the object. To remove content files, use the Dmclean tool, described in “[Dmclean](#)” on page 372.

The arguments you define for the tool determine which versions are deleted. For example, one argument (keep\_slabs) lets you choose whether to delete versions that have a symbolic label. Another argument (custom\_predicate) lets you define a WHERE clause qualification to define which versions are deleted. Refer to the *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* for instructions on writing WHERE clauses.

The Version Management tool generates a status report that is saved in the repository in /System/Sysadmin/Reports/VersionMgt.

The Version Management tool is installed in the inactive state.

#### 17.4.1.34.1 Arguments

“[Version management arguments](#)” on page 417, lists the arguments for the tool.

**Table 17-25: Version management arguments**

Argument	Datatype	Default	Description
-keep_slabs	Boolean	TRUE	Indicates whether you wish to keep versions of documents with symbolic labels. The default is TRUE.
-custom_predicate <i>qualification</i>	string	-	Defines a WHERE clause qualification for the query that selects versions for deletion.  The qualification must be a valid qualification. Refer to the <i>OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)</i> for information about WHERE clause qualifications.

Argument	Datatype	Default	Description
-cutoff_days	integer	180	The maximum age, in days, of the versions that you want to keep. All versions older than the specified number of days are considered for deletion. If you set this flag, you cannot set the -keep_latest flag. The two flags are mutually exclusive.
-keep_latest	integer	-	Directs the tool to keep the specified number of versions directly derived from each end node of a version branch. If you set this flag, you cannot set the -cutoff_days flag. The two flags are mutually exclusive.
-report_only	Boolean	TRUE	Indicates whether to generate only the report. Set this to FALSE to actually remove versions.
-queueperson	string(32)	-	User who receives email and inbox notifications from the tool. The default is the user specified in the operator_name property of the server configuration object.
-window_interval	integer	120	Execution window for the tool.

#### 17.4.1.34.2 Guidelines

We recommend that you have a thorough knowledge of what prior versions mean for your business requirements. If you need to keep all versions to satisfy auditing requirements, do not run this tool at all. Individual users or departments may also have needs and requirements for older versions. Needs for disk space may also affect the decisions about how many older versions to keep.

Run this tool initially with the -report\_only argument set to TRUE to determine how much disk space versions are using and how many versions are in the repository. With -report\_only set to TRUE, you can run the report several times, changing the other arguments each time to see how they affect the results.

If you are using the -cutoff days argument to ensure that your repository never has only versions older than a specified number of days, run this tool daily. If you are using -keep\_latest argument to keep only a specified number of versions, you can run this tool less frequently. The frequency will depend on how often new versions are generated (thereby necessitating the removal of old versions to keep the number of versions constant).

You can use this tool for one-time events also. For example, after a project is completed, you might remove all older versions of the project documentation. You must set the arguments appropriately for such occasions and reset them after the job is finished.



**Note:** The first execution of the tool may take a long time to complete if the old versions have never been deleted before.

#### 17.4.1.34.3 Report sample

```
VersionMgt Report For DocBase boston2
As Of 9/12/96 11:33:33 AM
Parameters for deleting versions:-----
- Inbox messages will be queued to boston2
- Keep the 3 most recent versions of each version
tree...
- Documents having symbolic labels will NOT be
deleted...
- This will generate a report and delete the
versions...
- The custom predicate is:
  object_name='ver911c'
- The server is enforcing compound integrity
(the compound_integrity property in the Server
Config object is set to true).

Querying for versions...
Object Name    Owner Name    Modify Date      Version Labels
ver911c        tuser1       09/12/96 11:19:30  1.7.1.2
ver911c        tuser1       09/12/96 11:18:49  1.7.1.0
ver911c        tuser1       09/11/96 16:18:46  1.3.1.1
ver911c        tuser1       09/11/96 16:18:37  1.3.1.0
ver911c        tuser1       09/11/96 16:07:40  1.5
ver911c        tuser1       09/11/96 16:07:39  1.4
ver911c        tuser1       09/11/96 16:07:37  1.1
ver911c        tuser1       09/11/96 16:07:35  1.0
Report Summary:
-----
```

```
The Docbase has a total of 21,986 kbytes of content.  
8 versions were removed.  
The versions removed represented 12 kbytes of content  
or 0.05%  
The documents contents are now orphaned. Use the  
Dmclean system administration tool to actually remove  
the contents.
```

#### 17.4.1.35 WfmsTimer (dm\_WfmsTimer)

The WfmsTimer tool checks running workflows for expired activity timers such as Pre Timer Expires and Post Timer Expires. OpenText™ Documentum™ Content Management Workflow Designer can set timers that send a message to the workflows supervisor when an activity fails to start or complete within a given time frame. The tool also sends an email message to the performer of the activity. The WfmsTimer tool is installed in the inactive state. When activated, the tool runs every hour by default. “Workflow events” on page 622 and *OpenText Documentum Content Management - Workflow Designer User Guide (EDCPKL250400-AWF)* provides more information about Pre Timer Expires and Post Timer Expires events.

### 17.4.2 Creating a job

Before you create a job, determine which method the job runs or create a Docbasic script, Java method, or other program to perform the task. If you create your own script, method, or program, you must then create a method object referencing the program. “Methods” on page 323 contains the information on creating method objects.

The New Job and Job Properties pages are identical for standard jobs, replication jobs, records migration jobs, remove expired retention objects, Branch Office Caching Services caching jobs, and job sequences. The following topics contain the instructions on creating a specific type of job:

- “Creating replication jobs” on page 427
- “Creating records migration jobs” on page 433
- “Creating remove expired retention objects jobs” on page 435
- “Creating Branch Office Caching Services caching jobs” on page 435
- “Creating job sequences” on page 437

**Table 17-26: Job Info properties**

Field	Description
Name	The name of the job object.

Field	Description
<b>Job Type</b>	<p>A label identifying the job type.</p> <p>If you are creating a replication job, records migration job, remove expired retention object, Branch Office Caching Services caching job, or a job sequence, this field is automatically populated with the associated job type.</p>
<b>Trace Level</b>	<p>Controls how much information is recorded in trace logs. May be set from 0 to 10.</p> <p><a href="#">"Viewing job trace logs" on page 441</a> contains the instructions on viewing trace logs.</p>
<b>Designated Server</b>	<p>When more than one server runs against a repository, use to designate a server to run the job. The default is <i>Any Running Server</i>.</p>
<b>State</b>	<p>Determines how the job runs:</p> <ul style="list-style-type: none"> <li>• If set to Active, the job runs as scheduled.</li> <li>• If set to Inactive, the job does not run automatically, but can be executed manually.</li> </ul>
<b>Job Start Date</b>	<p>Specifies when the job was started. This option is a read-only field that only displays for existing jobs.</p>
<b>Options</b>	
<b>Deactivate on Failure</b>	<p>Specifies whether to make the job inactive if it does not run successfully.</p>
<b>Run After Update</b>	<p>Specifies whether to run the job immediately after any changes to the job are saved.</p>
<b>Save If Invalid</b>	<p>Specifies whether to save the job object if Documentum Administrator is unable to validate the job.</p>
<b>Job Run History</b>	
<b>Last Run</b>	<p>Displays the last date and time the job ran and was completed. This option is a read-only field that displays for existing jobs.</p>
<b>Last Status</b>	<p>Displays the last time the job completed and the length of time the job took to run. This option is a read-only field that displays for existing jobs.</p>
<b>Last Return Code</b>	<p>Displays the last value returned by the job. This option is a read-only field that displays for existing jobs.</p>

Field	Description
<b>Runs Completed</b>	Displays the number of times the job has run to completion. This option is a read-only field that displays for existing jobs.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on creating a basic job.

### 17.4.3 Changing the schedule of a job

You can modify a job schedule, whether the job is a standard job, replication job, remove expired retention objects job, Branch Office Caching Services caching job, records migration job, or job sequence. Schedule each job to run with a frequency that meets your business needs. If a job is installed in the inactive state, change its status on the Job Properties - Info page.



#### Caution

Set up the schedules for replication jobs so that jobs for the same target repository do not run at the same time. Running replication jobs simultaneously to the same target repositories causes repository corruption.

**Table 17-27: Job schedule properties**

Field	Description
<b>Next Run Date and Time</b>	Specifies the next start date and time for the job. The default is the current date and time.
<b>Repeat</b>	Specifies the time interval in which the job is repeated.
<b>Frequency</b>	Specifies how many times the job is repeated. For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.
<b>End Date and Time</b>	Specifies the end date and time for the job. The default end date is 10 years from the current date and time.
<b>After</b>	Specifies the number of invocations after which the job becomes inactive.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on changing a job schedule.

#### 17.4.4 Setting the qualifier rules for the remove retention-expired objects job

The *Qualifier rules* determine which objects to remove from a content-addressable store when the remove expired retention objects (dm\_RemoveExpiredRetn\_Objects) job runs.

Create standard rules or custom rules on the New Job - Qualifier Rules or Job Properties - Qualifier Rules page for content-addressable stores. There are no restrictions on the number of conditions in a custom rule, but the length is limited to 255 characters.

Standard rules are limited to five selection criteria defined by choosing properties from drop-down lists. The available properties are:

- Name
- Title
- Subject
- Authors
- Keywords
- Created
- Modified
- Accessed

After selecting a property, select an operand and type or select the correct value. For example, two rules might be Name contains Linux and Created before January 1, 2004. When the job runs, the criteria are connected with AND, so that all criteria must apply to a particular object for it to be deleted. If you require an OR for example, Name contains Linux OR Created before January 1, 2004 use a custom rule.

A custom rule is entered into a text box as a DQL WHERE clause. There are no restrictions on the number of conditions in a custom rule, but the length is limited to 255 characters. Custom rules can be based on the values of any standard SysObject properties, provided those values are present before an object is saved. For example, a custom rule might be `object_name="Test"` or `object_name="Delete"`. Custom rules are not validated by Documentum Administrator.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on setting qualifier rules for the remove expired retention objects job.

## 17.4.5 Assigning a method to a job

Each job executes a method to perform particular tasks. Methods are executable scripts or programs represented by method objects in the repository. The script or program can be a Docbasic script, a Java method, or a program written in another programming language such as C++.

The associated method object has properties that identify the executable and define command line arguments and the execution parameters. For example, the dm\_DMCLean job executes the dm\_DMCLean method. Some OpenText Documentum CM jobs execute a specific method that cannot be changed.

If you assign a user-defined method to a job, that method must contain the code to generate a job report. If you turn on tracing, only a DMCL trace is generated.

**Table 17-28: Job method properties**

Field	Description
<b>Method Name</b>	Specifies the name of the method that is associated with the job.  Click <b>Select Method</b> to display the <b>Choose a method</b> page. Select a method name and click <b>OK</b> .  <i>"Locating a method for a job" on page 426</i> contains the instructions to locate a method.

Field	Description
<b>Arguments</b>	<p>Specifies the method arguments.</p> <p>Click <b>Edit</b> to display the <b>Method Arguments</b> page. Enter new arguments, remove unnecessary arguments, or change the values to the method by the job.</p> <p>Many jobs take the queueperson and window_interval arguments.</p> <ul style="list-style-type: none"> <li>• The queueperson argument defines which repository user receives the inbox and email notifications generated by the jobs. If you do not designate a repository user for a specific job, the notifications are sent to the user identified by the operator_name property of the server configuration object of server. This property is set to the repository owner name by default.</li> <li>• The window_interval argument defines a window on either side of the scheduled run time of job in which the job can run. This ensures that if a server must be restarted, the startup is not delayed by jobs that must be run.</li> </ul>
<b>Pass Standard Arguments</b>	<p>Select this option to pass the standard arguments for the method.</p> <p>The standard arguments are:</p> <ul style="list-style-type: none"> <li>• Repository owner</li> <li>• Repository name</li> <li>• Job ID</li> <li>• Trace level</li> </ul>

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on assigning a method to a job.

### 17.4.6 Locating a method for a job

On the **Choose a method** page, select the method to be executed by a job.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on locating a method for a job.

### 17.4.7 Creating, viewing, or modifying SysObject properties

The SysObject Info page displays information (metadata) about an object. To see more or less information, click the **show more** or **hide more** links.

**Table 17-29: SysObject properties**

Field	Description
Title	A name or title for the object.
Subject	A subject that describes the object.
Keywords	One or more keywords that describe the object. Click <b>Edit</b> to add, modify, remove, or change the order of keywords.
Authors	One or more authors associated with the object. Click <b>Edit</b> to add, modify, remove, or change the order of authors.
Owner Name	The user who owns the object. Click <b>Edit</b> to add or modify the owner name.
Version Label	The version number of the object. Click <b>Edit</b> to add, modify, remove, or change the order of version numbers.
Checkout Date	The date on which the object was last checked out. This is a read-only property.
Checked Out By	The name of the user who checked out the object. This is a read-only property.
Created	The date on which the object was created. This is a read-only property.
Creator Name	The name of the user who created the object. This is a read-only property.
Modified	The date on which the object was last modified. This is a read-only property.
Modified By	The name of the user who modified the object. This is a read-only property.
Accessed	The date on which the object was last accessed. This is a read-only property.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying SysObject properties.

### 17.4.8 Creating replication jobs

A replication job automates replication between the component storage areas of a distributed storage area. You can use replication jobs to replicate objects (property data and content) between repositories. By using parameters that you define, the replication job dumps a set of objects from one repository, called the *sourcerepository*, and loads them into another repository, called the *target* repository. After the replication job is saved and the job runs successfully for the first time, you cannot change the source or target repository. If you need to change the source or target repository, set the job to inactive or delete the job, then create a new replication job with the correct source or target repository.

If you are replicating objects from multiple source repositories into the same target repository, or if you are replicating replica object, use a job sequence to designate the order in which the jobs run so that they do not conflict with each other. [“Creating job sequences” on page 437](#) contains the information on creating job sequences.

The information and instructions in this section apply only to object replication, not to content replication. You cannot configure content replication with Documentum Administrator.

When you create a replication job, you must choose a replication mode and a security mode. Each security mode behaves differently depending on which replication mode you choose. In addition, replica objects in the target repository are placed in different storage areas depending on which security mode you choose. [“Choosing replication and security modes” on page 431](#) contains information on choosing replication and security modes.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains more information on replication jobs.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating a replication job.

#### 17.4.8.1 Selecting the source repository for a replication job

The From Source tab displays when you are creating or modifying a replication job and is used to select the source repository for the replication job. The source repository is the repository from which objects are replicated.

[“Creating replication jobs” on page 427](#) contains the instructions on how to access the New Replication Job - Source page and create new replication jobs.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on selecting the source repository for a replication job.

### 17.4.8.2 Selecting the target repository for a replication job

The To Target tab displays when you are creating or modifying a replication job and is used to select the target repository for a replication job. The target repository is the repository to which objects are replicated.

[“Creating replication jobs” on page 427](#) contains the instructions on how to access the New Replication Job - To Target page and create new replication jobs.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on selecting the target repository.

### 17.4.8.3 Setting replication job options

The Replication Options tab displays when you are creating or modifying a replication job pages are used to set replication job options.

[“Creating replication jobs” on page 427](#) contains the instructions on how to create new replication jobs.

**Table 17-30: Replication options**

Field	Description
<b>Code Page</b>	<p>Specifies the correct code page for the replication job. Keep the value at the default, UTF-8, unless it must be changed.</p> <p>Select <b>Full Refresh</b> to replicate every object in the source cabinet or folder. By default, the replication job is incremental and only replicates objects that have changed since the last execution of the job.</p> <p>Select <b>Fast Replication</b>, to use fast replication.</p> <div style="background-color: #e0e0e0; padding: 5px; margin-top: 10px;">  <b>Caution</b>            Fast replication does not replicate all relationships. <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i> contains more information.         </div>

Field	Description
<b>Full Text Indexing</b>	<p>Specifies the full-text indexing mode. Valid options are:</p> <ul style="list-style-type: none"> <li>• <b>Use target repository settings for indexing:</b> The same documents are indexed in the source and target.</li> <li>• <b>Do not index replicas:</b> None of the replicas are marked for indexing.</li> <li>• <b>Index all replicas:</b> All replicas in a format that can be indexed are marked for indexing.</li> </ul>
<b>Replication Mode</b>	<p>Specifies the replication mode.</p> <p>You can select federated mode whether or not the source and target repositories are in a federation. <a href="#">“Choosing replication and security modes” on page 431</a> contains more information on selecting a replication mode.</p> <p>Nonfederated replication mode is called external replication mode in the <i>OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)</i>.</p>
<b>Security Option</b>	<p>Specifies how to handle security if there is no matching permission set in the target repository.</p> <ul style="list-style-type: none"> <li>• Select <b>Preserve</b> to replicate the source permission set in the target repository.</li> <li>• Select <b>Remap</b> to reset the acl_domain of replica to the permission set specified on the target if the source permission set is an external permission set.</li> </ul> <p><a href="#">“Choosing replication and security modes” on page 431</a> contains more information on choosing a security mode.</p>

Field	Description
<b>Maximum objects per transfer</b>	<p>Specifies the maximum number of objects dumped and transferred in each operation.</p> <p>When selected, the replication job dumps and transfers the total number of objects to be replicated in batches of the size specified. For example, if 100,000 objects must be replicated and the maximum is set to 10,000, the objects are replicated in 10 batches.</p> <p>Select <b>Manual Transfer</b> if you intend to manually move the dump file from the source to the target, then click <b>Select User</b> next to the <b>Transfer Operator</b> field.</p>
<b>Transfer operator</b>	<p>Specifies the user who manually transfers the replication job.</p> <p>Click <b>Select User</b> and select the user in the target repository to notify that a replication job is ready for manual transfer.</p> <p>The system sends an email notification to the selected user.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <b>Caution</b>            The replication job creates a dump file and a delete synchronization file. Both files must be transferred to the target. Always transfer the dump file first.         </div>

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on setting replication options.

#### 17.4.8.4 Choosing a replication folder

You can choose a replication source or target folder on the Choose a folder page.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on choosing a folder.

#### 17.4.8.5 Choosing a replication job user

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on choosing a user.

#### 17.4.8.6 Choosing a permission set for replica objects

You can choose a permission set.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on choosing a permission set.

#### 17.4.8.7 Choosing a storage area

On the Choose a storage page, select a storage area and then click OK.

#### 17.4.8.8 Choosing replication and security modes

On the Replication Options tab, you select a replication mode and a security mode.

The replication modes are:

- Federated mode, which can be used whether or not the source and target repositories are in a federation.
- Non-federated mode, which is named external replication mode in the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*. This mode can be used whether or not the source and target repositories are in a federation.

The security modes determine how a permission set is assigned to replica objects in the target repository. The security modes are:

- Preserve
- Remap

Depending on whether you selected federated or non-federated (external) mode, the two security modes behave differently and replica objects are stored differently, as described in “[Security mode behavior](#)” on page 432.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains information on the two replication modes.

**Table 17-31: Security mode behavior**

<b>Selection</b>	<b>Replication Mode</b>
Federated and Preserve	<ul style="list-style-type: none"> <li>If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.</li> <li>If the permission set of a replicated object does not exist in the target repository, the permission set in the source repository is replicated to the target repository and the replica is assigned that permission set.</li> <li>Replica objects in the target repository are stored in the same storage area as in the source repository. If the storage area does not exist in the target repository, replica objects are stored in the default storage area designated in the replication job.</li> </ul>
Non-Federated and Preserve	<ul style="list-style-type: none"> <li>If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.</li> <li>If the permission set of a replicated object does not exist in the target repository, the replica is assigned the default replica permission set designated in the replication job. This is the permission set selected on the Target tab. If no permission set is chosen, the server creates a default permission set that assigns RELATE permission to the every user and group levels and DELETE permission to the replica owner.</li> <li>Replica objects in the target repository are stored in the same storage area as in the source repository. If the storage area does not exist in the target repository, replica objects are stored in the default storage area designated in the replication job.</li> </ul>

Selection	Replication Mode
Federated and Remap	<ul style="list-style-type: none"> <li>• If the permission set of a replicated object exists in the target repository, the replica is assigned that permission set.</li> <li>• If the permission set of a replicated object does not exist in the target repository, the replica is assigned the default replica permission set designated in the replication job.</li> </ul> <p>This is the permission set selected on the Target tab. If no permission set is selected, the server creates a default permission set that assigns RELATE permission to the every user and group levels and DELETE permission to the replica owner.</p> <ul style="list-style-type: none"> <li>• Replica objects in the target repository are stored in the same storage area as in the source repository.</li> </ul> <p>If the storage area does not exist in the target repository, replica objects are stored in the default storage area designated in the replication job.</p>
Non-Federated and Remap	<ul style="list-style-type: none"> <li>• The replica is assigned the default replica permission set designated in the replication job.</li> </ul> <p>This is the permission set chosen on the Target tab. If no permission set is selected, the server creates a default permission set that assigns RELATE permission to the every user and group levels and DELETE permission to the replica owner.</p> <ul style="list-style-type: none"> <li>• Replica objects are stored in the replica storage area designated in the replication job.</li> </ul>

#### 17.4.9 Creating records migration jobs

Records migration jobs move content files from one storage area to another. The target storage area can be another file store storage area or a secondary storage medium, such as an optical jukebox or a tape. If the target storage area is secondary storage, the storage must be defined in the repository as a storage area. That is, it must be represented in the repository by some type of storage object. When you define the records migration job, you can define parameters for selecting the files that are moved. For example, you might want to move all documents that carry a particular version label or all documents created before a particular date. All the parameters you define are connected with an AND to build the query that selects the content files to move.

When a records migration job runs, it generates a report that lists the criteria selected for the job, the query built from the criteria, and the files selected for moving. You can execute the job in report-only mode, so that the report is created but the files are not actually moved.

You must have superuser privileges to create a records migration job.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on creating a records migration job.

#### **17.4.9.1 Setting the rules of a records migration job**

Use the Rules tab on the New Records Migration Job - Rules or Job Properties - Rules page to define which documents are migrated by a records migration job.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on setting the rules of a records migration job.

#### **17.4.9.2 Defining selection criteria for a records migration job**

Use the Selection Criteria page to define selection criteria for a records migration job. At least one criterion must be selected. The four primary choices are not mutually exclusive; you can select any combination of the following:

- **Select documents by location**
- **Select documents by age**
- **Select documents by attributes**
- **Select documents by version**
- **Search all versions**

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on defining selection criteria.

#### **17.4.9.3 Defining version criteria for records migration job**

Set the version criteria for a records migration job on the Define Version page. At least one version criterion must be selected.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on setting the version criteria for a records migration job.

## 17.4.10 Creating remove expired retention objects jobs

This section contains information on how to create remove expired retention objects job.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating a remove expired retention objects job.



**Note:** “Remove expired retention objects” on page 398 contains information on the remove expired retention objects tool.

## 17.4.11 Creating Branch Office Caching Services caching jobs

A Branch Office Caching Services content caching job does the following:

- Creates and schedules a job to collect a set of documents based on a query.
- Creates caching requests for the documents with the Branch Office Caching Services destination information where the documents need to be.
- Sends caching requests to Messaging Service on a predetermined schedule.

Any user type can create a Branch Office Caching Services caching job. DQL queries for Branch Office Caching Services caching jobs are not validated by Documentum Administrator.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating a Branch Office Caching Services caching job.

### 17.4.11.1 Setting Branch Office Caching Services caching rules

The caching rules specify the caching options and the content to be selected for caching to the Branch Office Caching Services servers.

“Creating Branch Office Caching Services caching jobs” on page 435 contains the instructions on how to create a Branch Office Caching Services caching job.

**Table 17-32: Caching rules properties**

Field	Description
Object Type	<p>The type of objects needed to create caching messages. By default, dm_sysobject is selected.</p> <p>Click <b>Select</b> to access the Choose a type page to select an object type.</p>

Field	Description
<b>Selection Criteria</b>	<p>Users can write their own DQL query or use the query builder to build the query for selecting the documents they want to create caching requests for.</p> <ul style="list-style-type: none"> <li>• Select <b>Build criteria (Maximum of 5 lines)</b> to create up to five lines using query builder. The first query section will have the property name; the second query section will have the condition (operator); the third query section will hold the value (operand).</li> <li>• Select <b>DQL</b> query to create more complex queries. There are no restrictions on the number of conditions in a DQL query. DQL queries for Branch Office Caching Services caching jobs are not validated by Documentum Administrator.</li> </ul>
<b>Network Location</b>	<p>The destination list of the cached content. Click <b>Select</b> to access the Choose Network Locations page to select from which network locations the content should be cached.</p>
<b>Cutoff Date</b>	<p>Select a cutoff date preference. The caching method compares the cutoff date to the last updated date of the document to determine if a caching request needs to be generated for the document.</p> <ul style="list-style-type: none"> <li>• Select <b>Cache all selected content</b> to cache all documents without considering the last modified date of the document.</li> <li>• Select <b>Cache only selected content added/modified after</b> and then select a date, hour, minute, and second to cache documents based on the selected date and time criteria.</li> </ul>
<b>Expiration</b>	Enter an expiration date at which the caching request will expire if it is not fulfilled by that date.
<b>Previous</b>	Click to move to the previous page.
<b>Next</b>	Click to move to the next page.
<b>OK or Finish</b>	Click to save the changes and return to the Jobs list page.
<b>Cancel</b>	Click to return to the Jobs list page without saving any changes.

## 17.4.12 Creating job sequences

A job sequence is a job that runs a series of other jobs. For each job in the sequence, one or more predecessor jobs may be designated. Each job is run in sequence after any predecessors run. Jobs that do not have predecessors run in parallel. Each job sequence must contain at least one job that does not have any predecessors.

Use a job sequence when jobs must run in a particular order or the periods of time in which jobs run must not overlap. For example, if replication jobs replicate objects from multiple source repositories to a single target repository or if replication jobs replicate replica objects, use a job sequence to control the order in which the jobs execute.

The following restrictions apply to job sequences:

- You must be a superuser to create a job sequence.
- All jobs in a job sequence must be inactive or the job sequence fails. This means you cannot use jobs that are active and scheduled to run independently of the job sequence. However, you are not prevented from selecting a job that is in the active state. If you select a job that is in the active state, change its state to inactive.
- All jobs in a job sequence must execute a method where there is a method success code or method success status in the method object, and only such jobs are displayed in the user interface when a job sequence is created. Before you create a job sequence, examine the jobs you plan to include and the methods executed by those jobs to make sure that a method success code or method success status is present.
- Each job sequence must include at least one job that has no predecessors. This job is the first job to run. There can be more than one job in the sequence with no predecessors.
- The jobs in the sequence run in parallel except when a job has a predecessor. Documentum Administrator ensures that there is no cyclic dependency.

Before you create a job sequence, obtain the username and password for a superuser in each repository where the sequence runs a job.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating a job sequence.

### 17.4.12.1 Providing repository and job information for a job sequence

Use the Connection Info tab on the New Job Sequence or Job Properties page to select repositories and to designate the jobs to run in a job sequence.

**Table 17-33: Job connection info properties**

Field	Description
<b>Job Repositories</b>	
<b>Add</b>	<p>Click <b>Add</b> to access the Choose Repositories page.</p> <p>The system displays a list of available repositories. Select the repositories in which you want to run jobs, click <b>Add</b>, then click <b>OK</b>.</p> <p>If a repository where you want to run a job is not listed, add a connection broker to which that repository projects. <a href="#">“Creating or modifying connection broker projections” on page 39</a> contains more information on adding a connection broker.</p>
<b>Remove</b>	To remove a repository from the list, select the repository and click <b>Remove</b> . If jobs in the repository are part of the sequence, you must remove the jobs first.
<b>Repository</b>	The name of the repository where you want to run the job. By default, the current repository is listed with the currently-connected superuser, but you are not required to run any jobs in the current repository.
<b>User Name</b>	The login name for the repository.
<b>Password</b>	The password for the repository.
<b>Domain</b>	Specify the domain for any repository running in domain-required mode.
<b>Job Sequence Information</b>	

Field	Description
<b>Add</b>	<p>Click <b>Add</b> to add jobs to the sequence.</p> <p>The system validates the connection information entered in the Job Repositories. When all connection information is valid, the system displays the Choose Jobs page for one of the repositories. It lists jobs in that repository that can be included in the job sequence. Select the jobs to run in the sequence, click <b>Add</b>, then <b>OK</b>.</p> <p>The selected jobs must be inactive or the job sequence fails when it runs. If you select any active jobs, set them to inactive before the job sequence runs for the first time.</p>
<b>Job Name</b>	The name of the job that are in the job sequence.
<b>Job Dependencies</b>	<p>Specifies the dependencies the job has on other jobs.</p> <p>Click <b>Edit</b> to designate the job dependencies for each job that must run after another job completes. Select the listed job(s) that must run before the current job runs, then click <b>OK</b>. Each job sequence must include one job that has no predecessors. This job is the first job to run. The jobs in the sequence run in parallel except when a job has a predecessor.</p> <p>To remove a dependency, click <b>Edit</b> in the Job Sequence section to access the Choose jobs dependency page, clear the checkbox for any selected job, then click <b>OK</b>.</p>
<b>Repository</b>	The name of the repository where the job sequence is run.

*OpenText Documentum Content Management - Administrator User Guide*  
*(EDCAC250400-UGD)* contains the instructions on providing connection and job information for a job sequence.

#### 17.4.12.2 Selecting jobs for a job sequence

To access the Choose jobs page, click **Add** in the Job Sequence Information section on the Connection Info tab of the New Job Sequence or Job Properties page.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on selecting jobs for a job sequence.

#### 17.4.12.3 Setting dependencies for a job sequence

You can designate job dependencies in a job sequence. A dependency defines which job(s) must run before the current job is run.

Access the Choose jobs dependency page by clicking **Edit** in the Job Sequence Information section on Connection Info tab of the New Job Sequence or Job Properties page.



**Note:** Each job sequence must include one job that has no predecessors. This job is the first to run. The jobs in the sequence run in parallel except when a job has a predecessor.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on setting job dependencies.

### 17.4.13 Running jobs

Jobs typically run at predetermined intervals. The jobs that exist in all repositories have default schedules when they are created. “[Changing the schedule of a job](#)” on page 422 contains the instructions on modifying the schedule of job.

Most jobs pass standard arguments to the method executed by the job. The arguments are set on the Method tab for each job, and can be modified in most cases.

You can run a job manually (at a time other than the scheduled run time). Note that a job invoked in this fashion runs when the agent exec process starts the job, not when you click **Run**. The agent exec process polls the repository every five minutes, so the start of the job is delayed up to five minutes, depending on when you clicked **Run** and when the agent exec process last polled the repository.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on running a job.

#### 17.4.14 Viewing the status of a running job

To view the status of a running job after you start it, click **View > Refresh**.

The list page refreshes and the Status column for the job is updated. You may need to click **View > Refresh** several times because the job does not run immediately after you click **Tools > Run**.

#### 17.4.15 Viewing job reports

When a job runs, it generates a report. The report summarizes the results of the job. You can view the reports for one or more jobs.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing jobs reports.

#### 17.4.16 Setting the trace level for a job

Trace logs contain status information logged by a job. The trace level set for a particular job determines the amount of information logged. The default trace level for a job is 1 (minimal trace information), with a maximum level of 10 (debug-level tracing). A trace level of 4 through 6 provides a medium level of debugging.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on setting the trace level for a job.

#### 17.4.17 Viewing job trace logs

Trace logs contain status information logged by a job. The trace level set for a particular job determines the amount of information logged. The default trace level for a job is 1 (minimal trace information), with a maximum level of 10 (debug-level tracing). “[Setting the trace level for a job](#)” on page 441 contains the information on setting a different trace level.

You can view the trace log for a job.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing job trace logs.

## 17.4.18 Deleting jobs

Use the instructions in this section to delete a job.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting jobs.

## 17.4.19 Managing jobs

This section contains information and procedures for managing jobs and job sequences.

### 17.4.19.1 Activating or inactivating a job

When you set a job to inactive, the agent exec process ignores the job when it polls the repository and the job is never started by agent exec. When you set a job to active, the agent exec examines the job when it polls the repository and executes the job on the schedule defined in the job.

The activation status of a job is recorded in its `is_inactive` property. Use Documentum Administrator to change the status.

A job can be set to inactive automatically if you have set a maximum number of executions for the job. In such cases, the job is inactivated after the specified number of executions are completed. Similarly, if you specify an expiration date for a job, it is inactivated on that date.

### 17.4.19.2 Disabling all jobs

To disable all job executions, set the `agent_launcher` property in the server configuration object to an empty string ("") and stop and restart the server. Stopping the server stops the current running agent exec process. When you restart the server, the `agent_exec` process is not launched.

### 17.4.19.3 Modifying agent exec behavior

The agent exec process controls the job execution. It runs continuously, polling the repository at intervals for jobs to execute. By default, only three jobs are allowed to execute in a polling cycle and tracing for the process is turned off.

You can change these default parameters, including the polling interval. The behavior is controlled by command line arguments in the `method_verb` argument of the `method` object that invokes the agent exec process. The arguments can appear in any order on the command line. You must have Superuser privileges to change the `agent_exec_method`.

#### 17.4.19.3.1 Setting the polling interval

The agent exec process runs continuously, polling the repository at specified intervals for jobs to execute. The default polling interval is controlled by the setting in the database\_refresh\_interval key in the server.ini file. By default, this is set to 1 minute (60 seconds).

To change the polling interval without affecting the database refresh interval, add the -override\_sleep\_duration argument with the desired value to the agent\_exec\_method command line. Use Documentum Administrator to add the argument to the command line. For example:

```
.\dm_agent_exec -override_sleep_duration 120
```

The polling interval value is expressed in seconds (120 is 2 minutes expressed as seconds). The minimum value is 1 second.

#### 17.4.19.3.2 Setting the number of jobs in a polling cycle

By default, the agent exec executes up to three jobs in a polling cycle. You can configure only to a maximum of 500 jobs in a polling cycle. To change the maximum number of jobs that can run in a polling cycle, add the -max\_concurrent\_jobs argument with the desired value to the agent\_exec\_method method command line. For example:

```
.\dm_agent_exec -max_concurrent_jobs 5
```

#### 17.4.19.3.3 Enabling the high-availability feature

You can load balance at the job scheduling level. By default, this feature is disabled. Valid values are either 0 (false) or 1 (true). For example:

```
.\dm_agent_exec -enable_ha_setup 1
```

#### 17.4.19.3.4 Setting the job interval

The agent exec always sleeps for 30 seconds between launching jobs. This value can be changed using an argument. By default, the value is 30 seconds. For example:

```
.\dm_agent_exec -job_launch_interval 10
```

Use Documentum Administrator to modify the command line.

#### 17.4.19.3.5 Turning on tracing for the agent exec process

Tracing for the agent exec process is turned off by default (trace level = 0). To turn it on, use Documentum Administrator to add the -trace\_level argument to the agent\_exec\_method method command line. For example:

```
.\dm_agent_exec -trace_level 1
```

Setting the trace level to any value except zero turns on full tracing for the process.

The log file is named agentexec.txt and is stored in the %DOCUMENTUM%\dba\log\repository\_id\agentexec (\$DOCUMENTUM/dba/log/repository\_id/agentexec) directory.

#### 17.4.19.4 Creating and maintaining a repository connection file for job sequences

A repository connection file contains connection information used by the dm\_run\_dependent\_jobs method to connect to the repositories that contain the jobs in the sequence. When the dm\_run\_dependent\_jobs method executes, it searches the repository connection file to find an entry that specifies the server connection string, user, and domain identified in the job sequence object. If such an entry is found, it uses the password specified for that entry to make the connection to run the job.

Each entry in the file appears on a separate line and has the following format:

```
server_connect_string,[domain],user_name,password
```

Using this file is optional. If the dm\_run\_dependent\_jobs method does not find a matching entry in the file or if the file does not exist, the method attempts to use a trusted login to invoke the sequenced job.

The file is typically maintained by Documentum Administrator when you edit or modify a job sequence. You can, however, use the dcf\_edit utility to edit the file directly. Refer to “[dcf\\_edit utility](#)” on page 445 for instructions.

##### 17.4.19.4.1 Specifying the server connect string

The dm\_run\_dependent\_jobs method matches the value in the server\_connect\_string portion of the entry to the value in the job\_docbase\_name property of job sequence object when looking for a matching entry in the repository file.

The value can be any valid value used to designate a repository or server when connecting to a repository. For example, the following are valid formats for the values:

```
repository_name
```

```
repository_name.documentum_server_name
```

```
repository.documentum_server_name@host_name
```

The only requirement is that the value you define for the server connection string in the file must match the value specified in the job\_docbase\_property for the job in the sequence.

#### 17.4.19.4.2 Commas and backslashes in the entries

You can use commas or backslashes in the values specified for the server connection string, domain, and user name by escaping them with a backslash. For example, “doe\,john” is interpreted as “doe, john”, and “doe\\susie” is interpreted as “doe\\susie”.

You cannot use a backslash to escape any characters except commas and backslashes.

#### 17.4.19.4.3 dcf\_edit utility

The dcf\_edit utility allows you to add, remove, or replace entries in a repository connection file. It also allows you to backup the entire file. The utility is installed with Documentum CM Server as a method implemented using a Java class. The class is:

```
documentum.ecs.docbaseConnectionFile.DCFEdit
```

You can run the utility as a method from Documentum Administrator or as a Java command line utility. [“dcf\\_edit utility arguments” on page 445](#) lists the arguments accepted by the method or on the command line.

**Table 17-34: dcf\_edit utility arguments**

Argument	Description
-server_config <i>server_config_name</i>	Identifies the repository to which the utility will connect.  This argument is required for Add and Remove operations, but is invalid for Backup operations.
-login_domain <i>domain_name</i>	The domain of the user identified in the -login_user argument  This argument is optional for the Add and Remove operations, but is invalid for Backup operations.
-login_user <i>user_name</i>	Identifies the user as whom to connect.  This argument is optional for the Add and Remove operations, but is invalid for Backup operations.

Argument	Description
<p>-password <i>user_password</i></p>	<p>The clear-text password for the user identified in -login_user.</p> <p>This argument is required for the Add operation, but is invalid for Remove and Backup operations.</p>
<p>-f <i>repository_filepath</i></p>	<p>Path to the repository connection file.</p> <p>This parameter is a required parameter for all operations.</p>
<p>-operation <i>operation_name</i></p>	<p>Identifies the operation being performed. Include only one operation on each execution of the utility. Valid operation names are:</p> <ul style="list-style-type: none"> <li>• add</li> <li>• remove</li> <li>• backup</li> </ul> <p>Use add to add the connection information specified in the server_config, user, and password arguments to the file. If the entry already contains an entry with a matching server configuration value, this information replaces that entry. The password is encrypted before being added to the file. You must include the -password argument for an add operation. Including the -login_user argument is optional.</p> <p>Use remove to remove an entry from the file. The utility removes the entry with a value matching the -server_config name. Including the -login_user or -password arguments for a remove operation is optional.</p> <p>Use backup to create a backup of the file. The backup file is created in the same directory as the original file. The name is the name of the file with an appended time stamp, in the format:</p> <p style="padding-left: 20px;"><i>file_name-time_stamp</i></p> <p>Do not include the -login_user or -password arguments for backup operations.</p>

When the utility executes an Add operation, it looks for an entry in the file that matches the values you provide as arguments for -server\_config, -login\_user, and -login\_domain. If a match is not found, the utility creates a new entry. If a match is found, the utility replaces the existing entry with the values in the arguments.

### 17.4.19.5 Recovering from a job sequence failure

If the controlling job exits with a status of 1, it typically means that one or more jobs in the sequence failed to complete successfully. To recover from that situation, take the following steps:

1. Examine the status report of controlling job to determine which jobs failed. Use Documentum Administrator to view the status report of job. [“Interpreting a job sequence status report” on page 447](#) describes the entries in the report.
2. Examine the job reports of the failed jobs and the session and repository log files to determine the cause of the failure.
3. Correct the problem.
4. Run `dm_run_dependent_jobs` as a method, with the `-skip` argument, to re-execute the failed jobs. [“Executing dm\\_run\\_dependent\\_jobs independently” on page 448](#), describes the arguments that you can include when you run the method independently of the job.

### 17.4.19.6 Interpreting a job sequence status report

The `dm_run_dependent_jobs` method, called by controlling job of a job sequence, generates a status report. You can view the status report using Documentum Administrator. [“Entries in a job sequence status report” on page 447](#) lists the events recorded in the report and describes their format.

**Table 17-35: Entries in a job sequence status report**

Event	Entry Format
Start	<i>Date Time start-sequence=job_sequence_name</i>
Start Job	<i>Date Time start job - docbase=repository_name job=job_id attempt=1 2 3</i>
End Job	<i>Date Time end job - docbase=repository_name job=job_id result=succeed fail lastReturnCode=a_last_return_code lastDocumentID=ID_of_job_report lastJobStatus=a_current_status</i>
End	<i>Date Time end - job_sequence=controlling_job_id result=succeed fail</i>
Error	<i>Date Time error - docbase=repository_name job=job_id msg=error_message</i>

### 17.4.19.7 Executing dm\_run\_dependent\_jobs independently

You can execute the dm\_run\_dependent\_jobs method independently of the controlling job. Use Documentum Administrator to run the method manually.

[“dm\\_run\\_dependent\\_jobs arguments” on page 448](#), lists the arguments accepted by the method. Some arguments are required and some are optional.

**Table 17-36: dm\_run\_dependent\_jobs arguments**

Argument	Required?	Description
<code>-docbase <i>repository_name</i></code>	Yes	Identifies the repository that contains the job sequence.
<code>-user_name <i>user_name</i></code>	Yes	Identifies the user executing the job sequence.
<code>-job_sequence <i>sequence_name</i></code>	Yes	Identifies the job sequence to be executed.
<code>-method_trace_level <i>trace_level</i></code>	No	Defines a trace level for the dm_run_dependent_jobs method. The two valid values are 0 and 10. 0 records status messages only. 10 provides debugging messages in addition to status messages.  The default trace level is 0.
<code>-skip <i>list_of_jobs</i></code>	No	Identifies the jobs in the sequence that you do not want to execute. Provide a comma-separated list of job object IDs.
<code>-dcf</code>	See description	Specifies the location of the repository connection file.  This is not required if the method is using trusted login to connect to the repositories in which the jobs in the sequence reside.

## 17.4.20 Deactivating jobs that fail

You can configure a job so that it becomes inactive if it fails.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on deactivating jobs that fail.



# Chapter 18

## Alias sets

### 18.1 Alias sets and aliases

An *alias set* is an object that defines one or more aliases and their corresponding values. An *alias* is a placeholder for user names, group names, or folder paths. Documentum CM Server provides various alias sets that are installed by default. In Documentum Administrator, all alias sets for a repository are located in the **Administration > Alias Sets** node.

Aliases can be used in:

- SysObjects or SysObject subtypes, in the owner\_name, acl\_name, and acl\_domain properties
- ACL template objects, in the r\_accessor\_name property
- Workflow activity definitions (dm\_activity objects), in the performer\_name property
- A Link or Unlink method, in the folder path argument

Any user can create an alias set. However, only the owner of the alias set or a superuser can change or delete an alias set. If the server API is used, the constraints are different:

- To change the owner of an alias set, you must be either the owner of the alias set or have superuser privileges.
- To change other properties or to delete an alias set, you must be the owner of the alias set or a user with system administrator or superuser privileges.

### 18.2 Creating or modifying alias sets

Any user can create an alias set.

**Table 18-1: Alias set properties**

Field	Description
Name	The name of the alias set.
Description	A description of the alias set.
Owner	The name of the alias set owner. Click <b>Select</b> to select and assign an owner to the alias set.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on creating or modifying alias sets.

## 18.3 Viewing or removing aliases

You can view or remove aliases from an alias set.

Field	Description
Name	The name of the alias.
Category	The category to which the alias belongs.
Value	The value assigned to the alias.
Description	A description of the alias.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on viewing or removing aliases.

## 18.4 Adding or modifying aliases

You can add an alias to an alias set or modify an existing alias set.

You must be the owner of the alias set or have superuser privileges to add, modify, or delete aliases.

**Table 18-2: Alias properties**

Field	Description
Name	The name of the alias. For an existing alias, the name is a read-only value and cannot be modified.
Category	The category to which the alias belongs. The category can have the following values: <ul style="list-style-type: none"><li>• Permission Set</li><li>• Cabinet Path</li><li>• Folder Path</li><li>• Group</li><li>• User</li><li>• User or Group</li><li>• Unknown</li></ul> For an existing alias, the category is a read-only value and cannot be modified.

Field	Description
<b>Value</b>	The value for the category property. Click <b>Get Value</b> to select a value from a list of values associated with the category you previously selected.  If you selected <b>Unknown</b> as the category, you must type a value in the Value field.
<b>User Category</b>	A user-defined integer value for the Value property. Optional property.
<b>During DocApp Installation</b>	Select <b>Prompt Alias value</b> to indicate to prompt for the alias value when a OpenText Documentum CM application is installed.  If the category is a folder path or cabinet path, you can select between prompting for the value during application installation or creating the folder or cabinet if it does not exist.
<b>Description</b>	A description for the alias.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on adding or modifying aliases.

## 18.5 Deleting alias sets

You must be the owner of the alias set owner or have superuser privileges to delete an alias set. The constraints are different if you are using the API. *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting alias sets.



# Chapter 19

## Formats

### 19.1 Formats

Format objects define file formats. Documentum CM Server only recognizes formats for which there is a format object in the repository. When a user creates a document, the format of the document must be a format recognized by the server. If the format is not recognized by the server, the user cannot save the document into the repository.

The Documentum CM Server installation process creates a basic set of format objects in the repository. You can add more format objects, delete objects, or change the properties of any format object. In Documentum Administrator, all formats are located on the **Administration > Formats** node.

### 19.2 Viewing, creating, or modifying formats

You can view, create, or modify formats.

**Table 19-1: Format properties**

Field	Value
<b>Name</b>	The name of the format (for example: doc, tiff, or lotmanu).
<b>Default File Extension</b>	The DOS file extension to use when copying a file in the format into the common area, client local area, or storage.
<b>Description</b>	A description of the format.
<b>Com Class ID</b>	The class ID (CLSID) recognized by the Microsoft Windows registry for a content type.
<b>Mime Type</b>	The Multimedia Internet Mail Extension (MIME) for the content type.
<b>Windows Application</b>	The name of the Windows application to launch when users select a document in the format represented by the format object.
<b>Macintosh Creator</b>	Information used internally for managing Macintosh resource files.
<b>Macintosh Type</b>	Information used internally for managing Macintosh resource files.

Field	Value
<b>Class</b>	<p>Identifies the classes or classes of formats to which a particular format belongs. The class property works with all search engines.</p> <p>To assign a class to a format, click <b>Edit</b> to access the Format Class page. Type a value in the <b>Enter new value</b> box and click <b>Add</b>.</p> <p>Two values are used by the full-text indexing system to determine which renditions of a document are indexed:</p> <ul style="list-style-type: none"> <li>• <b>ft_always</b> All renditions of a document are indexed.</li> <li>• <b>ft_preferred</b> If a document has multiple renditions in indexable formats and one format is set to <b>ft_preferred</b>, the rendition in that format is indexed as well as any formats with the class value set to <b>ft_always</b>. If more than one rendition of a document is set to <b>ft_preferred</b>, the first rendition processed for indexing is indexed and the other renditions are not.</li> </ul>
<b>Asset Class</b>	Used by applications. Identifies the kind of asset (video, audio, and so on) represented by this format.
<b>Filename Modifier</b>	The modifier to append to a filename to create a unique file name.
<b>Default Storage</b>	Identifies the default storage area for content files in this format. Click <b>Select</b> to access the Choose a Storage page.
<b>Re-Initialize Server</b>	Select to reinitialize the server so changes occur immediately.
<b>Rich Media</b>	Indicates whether thumbnails, proxies, and metadata are generated for content in this format. You must have OpenText™ Documentum™ Content Management - Media installed to generate the thumbnails, proxies, and metadata.
<b>Hide</b>	Determine whether the format object should appear in the WorkSpace list of formats. Select to hide the object.
<b>Full-Text Indexing</b>	Select to enable the format for full-text indexing.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing, creating, or modifying formats.

## 19.3 Deleting formats

You can delete formats. However, you cannot delete a format if the repository contains content files in that format.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on deleting formats.



# Chapter 20

## Types

### 20.1 Object type categories and properties

OpenText Documentum CM is an object-oriented system. An object is an individual item in the repository. An object type represents a class of objects. The definition of an object type consists of a set of properties, whose values describe individual objects of the type. Object types are similar to templates. When an object is created in a repository, Documentum CM Server uses the type definition as a template to create the object and then sets the properties for the object to values specific to that object instance.

#### 20.1.1 Type categories

Object types are sorted into the following categories:

- Standard object type

Standard object types are all types that are not aspect, lightweight, or shareable types.

- Aspect property object type

Aspect property object types are internal types used by Documentum CM Server and Foundation Java API to manage properties defined for aspects. These types are automatically created and managed internally when properties are added to aspects. They are not visible to users and user applications.

- Lightweight object type

Lightweight object types are a special type used to minimize the storage footprint for multiple objects that share the same system information. A lightweight type is a subtype of its shareable type.

- Shareable object type

Shareable object types are the parent types of lightweight object types. A single instance of a shareable type object is shared among many lightweight objects.

### 20.1.2 Lightweight object types

A lightweight object type requires less storage space in the database. All lightweight object types are subtypes of a shareable type. When a lightweight object is created, it references a shareable supertype object. As additional lightweight objects are created, they can reference the same shareable object, also called a parent object. Each lightweight object shares the information in its shareable parent object. Instead of having multiple nearly identical rows in the database tables to support all the instances of the lightweight type, a single parent object exists for multiple lightweight objects. Lightweight objects are useful for object groups with many identical attribute values. A single copy of the shared parent object shares all the redundant information among the lightweight objects.

### 20.1.3 Type properties

Properties are the fields that comprise an object definition and the field values describe individual instances of the object type. When an object is created, its properties are set to values that describe that instance of the object type. All properties have a data type that determines what values can be stored in the property.

## 20.2 Managing types

In Documentum Administrator, types are managed on the Types page under the **Administration > Types** node. On the Types page, you can filter types using the **All**, **DCTM Types**, or **Custom Types** from the list box. Types whose names are displayed as underlined links have subtypes. If you click the name, the subtypes are displayed. To navigate back to a previous list page, click a link in the breadcrumb at the top of the page. The Category and Parent Type columns appear on the Types page with OpenText™ Documentum™ Content Management High-Volume Server and Documentum CM Server version 6 or later.

From the Types page, you can:

- Create, modify, and delete shareable object types.
- Create, modify, and delete lightweight SysObject types.
- Convert heavyweight object types to a shareable object type.
- Convert heavyweight object types to a lightweight SysObject type.
- Convert heavyweight object types to a shareable type and lightweight SysObject type.

Assignment policies determine the correct storage area for content files. A new type inherits a default assignment policy from the nearest supertype in the type hierarchy that has an active assignment policy associated with it. After the type is created, associate a different assignment policy with the type.

*OpenText Documentum Content Management - Server Fundamentals Guide (EDCCS250400-GGD)* contains more information on types. *OpenText Documentum*

*Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* contains the information on the system-defined object types, including the properties of each type.

## 20.3 Creating or modifying types

To create a type, you must have superuser, system administrator, or Create Type user privileges. If you have superuser privileges, you can create a subtype with no supertype. Only a superuser or the owner of a type can update the type.

Properties are stored as columns in a table representing the type in the underlying RDBMS. However, not all RDBMSs allow you to drop columns from a table. Consequently, if you delete a property, the corresponding column in the table representing the type may not actually be removed. In such cases, if you later try to add a property to the type with the same name as the deleted property, you receive an error message.

Any changes made to a type apply to all objects of that type, to its subtypes, and to all objects of any of its subtypes.

**Table 20-1: Type properties**

Field	Value
<b>Info</b>	
Type Name	The name of the object type. This field is read-only in modify mode.
Model Type	This field is read-only in modify mode. Options are: <ul style="list-style-type: none"> <li>• <i>Standard</i>: This is the default and is for heavy types.</li> <li>• <i>Shareable</i>: Defines a shareable SysObject model type for SysObject supertypes and their subtypes.</li> <li>• <i>Lightweight</i>: The system checks for the existence of shareable types in the current repository. If there are no shareable types in the current repository, this option is not available. If selected, the Parent Type, Materialize, and FullText fields become available and the Super Type Name field is not displayed.</li> </ul>

Field	Value
<b>Super Type Name</b>	<p>The name of the supertype. The default supertype is dm_document. This field is:</p> <ul style="list-style-type: none"> <li>• Not available if the Model Type is Lightweight.</li> <li>• Read-only in modify mode.</li> </ul> <p>Unless you have superuser privileges, you must identify the supertype of type. If you do have superuser privileges and want to create the type without a Supertype, select NULL as the supertype.</p>
<b>Default Storage</b>	A default file store for the object type.
<b>Default Group</b>	A default group for the type. Click <b>Select Default Group</b> to access to add or change the default group.
<b>Default Permission Set</b>	A default permission set for the type. Click <b>Select Default Permission Set</b> to add or change the default permission set.
<b>Default Assignment Policy</b>	<p>The system displays the default assignment policy for the type, if there is one. This field appears only when modifying a type and if Content Storage Services is available for the repository.</p> <p>Click the link to access the assignment policy. Use the information in <a href="#">"Assignment policies" on page 516</a> to modify the assignment policy or to remove the type from the assignment policy. Use the instructions in the Assignment Policy section to associate a different policy with a particular type.</p>

Field	Value
<b>Enable Indexing</b>	<p>The system displays the Enable Indexing checkbox if:</p> <ul style="list-style-type: none"> <li>• The type is dm_sysobject or its subtype and you are connected as a superuser to a 5.3 SP5 or later repository. If neither of these conditions is met, the system does not display the checkbox.</li> <li>• A type and none of its supertypes are registered. The system displays the checkbox cleared and enabled. You can select the checkbox to register the type for full-text indexing.</li> <li>• A type is registered and none of its supertypes are registered. The system displays the Enable Indexing checkbox selected and enabled.</li> <li>• A supertype of the type is registered for indexing. The system displays the Enable Indexing checkbox selected but disabled. You cannot clear the checkbox.</li> </ul> <p>The system does not display the Enable Indexing checkbox when you create a type. You must first create the type and save it.</p> <p>If you are registering a particular type for indexing, the system automatically selects all of its subtypes for indexing. When you are registering a type for indexing, the system checks for any of its subtypes that are registered. If a subtype is registered, the system unregisters it before registering the type.</p>
<b>Partitioned</b>	<p>Displays whether a type that can be partitioned is or is not partitioned. This field:</p> <ul style="list-style-type: none"> <li>• Does not appear if the type cannot be partitioned.</li> <li>• Displays <i>False</i> if the type can be partitioned but is not.</li> <li>• Displays <i>True</i> if the type is partitioned.</li> </ul>
<b>Parent Type</b>	<p>This option is available only when creating a type and Model Type is Lightweight. This field is read-only in modify mode. This field appears with OpenText Documentum Content Management (CM) High-Volume Server and if the Documentum CM Server version is 6 or later.</p>

Field	Value
<b>Materialize</b>	<p>This option is available only when creating a type and Model Type is Lightweight. This field is read-only in modify mode.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <i>Auto materialize</i>: The lightweight object will be automatically materialized to a full object when the object is saved with changes to some attributes of the parent object.</li> <li>• <i>Materialize on request</i>: The lightweight object can only be materialized by explicitly calling the materialize API. Any changes to the parent object by the lightweight object before materialization will result in an error.</li> <li>• <i>Do not materialize</i>: The lightweight object is not allowed to be materialized. Call the materialize API will result in an error. Any changes to the parent object by the lightweight object will result in an error.</li> </ul>
<b>Full Text</b>	<p>This option is available only when creating a type and Model Type is Lightweight. This field is display-only in modify mode.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• No fulltext: This is the default.</li> <li>• Light fulltext: No attributes inherited from the shared parent will be full-text indexed.</li> <li>• Full fulltext</li> </ul>
<b>Attribute</b>	
<b>Attribute Name</b>	The name of the attribute. This field is display-only in modify mode.
<b>Type</b>	The property type.
<b>Size</b>	The size of the property, if the property is the String type.
<b>Inherited</b>	Yes indicates that a property is inherited from a supertype. No indicates that the property is user-defined. You cannot remove a property inherited from the supertype.
<b>Repeating</b>	If selected, the property is a repeating property.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on creating or modifying types.

## 20.4 Selecting a type

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on selecting types.

## 20.5 Deleting types

You can only remove a user-defined type from the repository if:

- You are the owner of the type or have superuser privileges.
- The type has no subtypes.
- There are no existing objects of that type in the repository.

You cannot remove system-defined types from the repository. If you delete an object type with an associated assignment policy, the assignment policy is not removed.  
You can delete it manually.

You cannot delete a shareable type that is shared by a lightweight SysObject. Delete the dependent lightweight objects first.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on deleting types.

## 20.6 Viewing assignment policies

The Assignment Policy Inheritance page displays a type, its supertypes, and the assignment policy for each type and supertype with an active assignment policy associated with it.

Use the Assignment Policy Inheritance page to view the assignment policies defined for a type or to understand policy inheritance and gauge the impact of changes to any policies. Knowing the inheritance hierarchy helps with troubleshooting if content files are not saved in the correct storage area for that type.

The page displays a type and its supertypes in descending order, with the type highest in the type hierarchy at the top of the list. The assignment policy associated with each type is displayed, if the assignment policy is active. If the selected type does not have an active assignment policy associated with it, the assignment policy associated with its immediate supertype is applied. If its immediate supertype does not have an active assignment policy, the policy associated with the next supertype in the hierarchy is applied until the SysObject supertype is reached.

An assignment policy is associated with a type in one of two ways:

- Direct association, when the type is specified in the policy

- Inheritance from a supertype

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing assignment policies associated with types.

## 20.7 Converting types to shareable object types

If a type is a SysObject or subtype of SysObject, you can convert the type to a shareable type, even if its supertype is shareable. However, you cannot convert a type to shareable if any of its children are shareable types. This option is available only on 6.5 repositories with High-Volume Server.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains instructions on converting types to shareable object types.

## 20.8 Converting types to lightweight object types

You can convert dm\_sysobject types and their subtypes to shareable object types for 6.5 repositories. This option is available only on 6.5 repositories with High-Volume Server.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on converting types to lightweight object types.

## 20.9 Converting types to shareable and lightweight object types

A heavy type object type can be converted to both a shareable object type and lightweight SysObject type. This option is available only on 6.5 repositories with High-Volume Server.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on converting types to shareable and lightweight object types.

# Chapter 21

## Storage management

### 21.1 Storage management areas

In Documentum Administrator, the Storage Management node is located under the **Administration** node and includes three main areas:

- Storage

The storage area contains pages for creating various store types, such as file stores, retention stores (Centera and NetApp SnapLock), blob stores, turbo stores, Atmos stores, S3-compatible stores, mount point objects, location objects, and storage plug-ins.

- Assignment Policies

The Assignment Policies area contains pages for creating assignment policies. These pages only appear with Content Storage Services.

- Migration policies

The Migration Policies are contains pages for creating jobs to move content files among storage areas based on user-defined rules and schedules. These pages only appear with Content Storage Services.

### 21.2 Storage

The storage area contains information about existing stores and pages for creating various store types. To access the storage area, select **Administration > Storage Management > Storage**. The Storage list page displays with a list of existing stores and location objects. If a storage system complies with the NFS or Linux file system or CIFS (Windows) file system protocols and standards, OpenText Documentum CM can use this storage system. The first ten storage areas in the repository are displayed in the order in which they were created.

A repository can contain the following storage objects:

**Table 21-1: Repository storage objects**

Storage	Description
File Store	File stores hold content as files.
Linked Store	Linked stores do not contain content, but point to the actual storage area, which is a file store.
Blob Store	Blob stores store files directly in the repository in a special table.

Storage	Description
Mount Point	Mount point objects represent directories that are mounted by a client.
External File Store	External file stores do not store any content. They point to the actual file system.
External Free Store	External free stores do not store any content. They point to a CD-ROM or user-defined storage.  For example, the XML file store is an external free store used specifically to optimize performance with XML content files.
External URL Store	External URL stores do not store any content. They point to a URL.
Plug-in	Plug-ins are required for access to external stores.
NetApp SnapLock Store	The NetApp SnapLock Store is a retention store for content that is retained for a specified time. Retention stores are often used for storing massive amounts of unchanging data, such as email archives or check images.
EMC Centera Store	The EMC Centera Store is a retention store for content that is retained for a specified time. Retention stores are often used for storing massive amounts of unchanging data, such as email archives or check images.
Atmos Store	The Atmos store is a storage system comprised of several distributed services running on hardware nodes connected via a network. The nodes run a collection of services to store, retrieve, categorize, and manage the data in the system or cloud.
Amazon S3 Store	Amazon Simple Storage Service (Amazon S3) is a highly durable and available store that can be used to reliably store application content. It allows you to offload your entire storage infrastructure and offers better scalability, reliability, and speed than just storing files on the file system.
	 <b>Note:</b> Documentum CM Server supports all S3 compatible stores.
OpenStack Swift Store	OpenStack Swift store offers cloud storage software to store and retrieve lots of data with a simple API. It is optimized for durability, availability, and concurrency across the entire data set.

Storage	Description
REST Store	Documentum CM Server supports Microsoft Azure Blob and Google Cloud storage types as REST object store.
Distributed Store	Distributed stores do not contain content, but point to component storage areas that store the content.  The component storage areas in a distributed store can be any mixture of the file store and linked store storage types, provided that all have the same value in the media_type property.
Location	Location objects represent directories or files that are accessed by Documentum CM Server.

## 21.2.1 File stores

A file store is a directory that contains content files. It is the basic storage type of a repository. Each file store has a corresponding location object. You can create a location object pointing to the file system directory that corresponds to the file store before creating the file store or you can select the location while creating the file store. In the latter case, Documentum Administrator creates the location object for you.

### 21.2.1.1 Creating, viewing, or modifying file stores

You can create, view, or modify file stores.

**Table 21-2: File store properties**

Field	Description
<b>Info</b>	
Name	The name of the file store. The name must be unique within the repository.
Description	The description of the file store.  The description can be up to 128 bytes in length if in English, German, Italian, Spanish, or French. The description can be up to approximately 64 bytes in Japanese.

Field	Description
<b>Location</b>	<p>Select the location on the server host.</p> <p> <b>Caution</b> Be sure that the storage path you specify does not point to the same physical location as any other file stores. If two file stores use the same physical location, it may result in data loss.</p>
<b>Media Type</b>	<p>The media type to store in the storage area. Options are:</p> <ul style="list-style-type: none"> <li>• Regular Content</li> <li>• Thumbnail Content</li> <li>• Streaming Content</li> </ul> <p>Media type cannot be changed for an existing file store.</p>
<b>Base URL</b>	<p>The base URL used to retrieve content directly from a storage area.</p>
<b>Encrypted</b>	<p>Indicates if the files store is encrypted. This option is only available in repositories with Trusted Content Services and cannot be changed for an existing file store.</p>
<b>Make Public</b>	<p>Indicates if the area is accessible to the public with no restrictions.</p>
<b>Add Extension</b>	<p>Indicates whether the server appends an extension to the file when writing it into the storage area. This option cannot be changed for an existing file store.</p>
<b>Require Ticket</b>	<p>Indicates whether the server generates a ticket when returning the URL to a content file.</p>
<b>SurrogateGet Method</b>	<p>Installs a custom SurrogateGet method. This field only displays for an existing file store.</p> <p>To install the method, click <b>Select Method</b> and browse to the method on the server host file system.</p>
<b>Offline Get Method</b>	<p>Indicates whether the server uses an offline Get method. This field only displays for an existing file store.</p>

Field	Description
<b>Status</b>	<p>Select a radio button to change the status of the file store to on line, off line, or read-only. This field only displays for an existing file store.</p>
<b>Digital Shredding</b>	<p>Select to enable digital shredding.</p> <p>Digital shredding is a security feature that removes deleted content files and their associated content objects. It overwrites the addressable locations of the file with a character, then its complement, and finally a random character. Digital shredding requires Trusted Content Services.</p> <p> <b>Caution</b></p> <p>The Documentum Administrator interface for version 6 and later displays the <b>Digital Shredding</b> check box for all file stores. If the file store is a component of a distributed store, files are not digitally shredded even when it appears that digital shredding is enabled for the file store.</p>
<b>Content Compression</b>	<p>Select to compress all content in the file store. This option is only available in 5.3 SP1 and later repositories with Content Storage Services.</p> <p>Content compression is a feature that automatically compresses a file to a smaller size when the file is created. Content compression requires Content Storage Services. You cannot enable content compression after the file store is created.</p>

Field	Description
<b>Content Duplication</b>	<p>Select to enable content duplication checking. This option is only available in repositories with Content Storage Services.</p> <ul style="list-style-type: none"> <li>When <b>Generate content hash values only</b> is selected, for each piece of content checked in to the repository, Documentum CM Server calculates the value needed to determine whether or not it is duplicate content.</li> <li>When <b>Generate content hash values and check for duplicate content</b> is selected, for each piece of content checked in to the repository, Documentum CM Server calculates the value needed to determine whether or not it is duplicate content and then checks for duplicate content.</li> </ul> <p>Content duplication minimizes the amount of content file duplication in the file store. Content duplication checking requires Content Storage Services.</p> <p>You cannot enable content duplication checking after the file store is created.</p>
<b>Space Info</b>	The Space Info tab only displays for an existing file store.
<b>Active Space/Files</b>	The space used by the file store and the number of files.
<b>Orphaned Space/Files</b>	The amount of orphaned space in the file store and the number of orphaned files.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on the following:

- Creating, viewing, or modifying file stores
- Moving file store storage area

### 21.2.1.2 Configuring NAS file stores

This section describes the instructions to configure Data Domain and Isilon NAS file stores.



**Note:** Data Domain does not allow creation of files with Alternate Data Stream (ADS).

Before configuring, ensure the following for Windows:

- Documentum CM Server host and NAS storage host should be in same domain.
- Domain Administrator only can install Documentum CM Server on the Documentum CM Server host.

#### To configure NAS file stores:

1. Log in to the Documentum CM Server Windows host as the domain administrator.
2. Install Documentum CM Server on the Documentum CM Server host. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains the installation instructions.
3. After the Documentum CM Server installation is complete, you will be prompted to configure the repository using the Documentum CM Server configuration program. Perform the following steps:
  - a. In the configuration options screen, choose **Repository** and click **Next**.
  - b. Enter the **installation owner password** where the password is the password of Domain Administrator and click **Next**.
  - c. Choose **Add a new repository** and click **Next**.
  - d. Specify a **data directory** for storing content files and indicate whether it resides on a **SAN or NAS device**.
    - For Windows: Data directory path is the CIFS share path of the NAS storage device.
    - For Linux: NAS storage device NFS share path is mounted on the Linux host as root and used as the data directory path.

```
root$ mount -t nfs <IP address of DD store>
:<shared NFS path><local mount path>
```



**Note:** The data directory must not be a top-level directory on a SAN or NAS device such as `\<ip_address>`. For SAN or NAS, enter the complete path including a shared device and at least one level of directory. Here is an example of a valid data directory on a SAN or NAS device: `\<ip_address>\Documentum\data`. The default data directory is `<$DOCUMENTUM>/data`.

Click **Next**.

- e. Select **Yes** for the **Is this a NAS or SAN device** option and click **Next**.
- f. Continue with the options in the Documentum CM Server configuration program and complete it. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed instructions.

After the Documentum CM Server configuration program is complete, the NFS file store share is created.

## 21.2.2 Linked stores

A linked store is a storage area that does not contain content files. Instead, it contains a logical link to the actual storage area, which is a file store.

Linked stores are not available in a OpenText Documentum CM 6 or later repository. However, linked stores are available in a 5.3x repository. On Windows hosts, the actual storage area is implemented as a shared directory. On Linux hosts, the linked store contains a logical link to the actual storage area.

### 21.2.2.1 Creating, viewing, or modifying linked stores

You can create, view or modify a linked store.

**Table 21-3: Linked store properties**

Field	Value
<b>Name</b>	The name of the storage object. This name must be unique within the repository.
<b>Location</b>	The name of the directory containing the logical link.
<b>Linked Store</b>	The name of the storage area to which the link is pointing.
<b>Use symbolic links</b>	If selected, symbolic links are used.
<b>Get Method</b>	To install a custom SurrogateGet, click <b>Select Method</b> and browse to the method on the server host file system.  This option only appears if you are modifying an existing linked store.
<b>Offline Get Method</b>	Select to use an offline Get method.  This option only appears if you are modifying an existing linked store.
<b>Status</b>	Select a radio button to change the status of the file store to on line, off line, or read only.  This option only appears if you are modifying an existing linked store.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying linked stores.

### 21.2.3 Blob stores

The content in a blob store is stored directly in the repository rather than on the host file system of the server. The content in a blob store is stored in rows in an RDBMS table. The content stored in a blob store must be less than or equal to 64 KB.

Content stored in a blob store is ASCII or arbitrary sequences of 8-bit characters. This is designated when creating the blob store. To allow arbitrary sequences of 8-bit characters, you can store ASCII in the store, but if you decide on ASCII, you cannot store 8-bit characters.

You cannot define a blob storage area as the underlying area for a linked store or as a component of a distributed storage area. That is, blob storage cannot be accessed through a linked store storage area or through a distributed storage area.

#### 21.2.3.1 Creating, viewing, or modifying blob stores

You can create, view or modify a blob store.

**Table 21-4: Blob store properties**

Field	Description
<b>Name</b>	The name of the storage object. This name must be unique within the repository and must conform to the rules governing type names.
<b>Content Type</b>	Valid values are: <ul style="list-style-type: none"> <li>• ASCII</li> <li>• 8-bit Characters</li> </ul>
<b>Get Method</b>	To install a custom SurrogateGet, click <b>Select Method</b> and browse to the method on the server host file system.  This option only displays for existing blob stores.
<b>Offline Get Method</b>	Select to use an offline Get method.  This option only displays for existing blob stores.
<b>Status</b>	Select a radio button to change the status of the file store to on line, off line, or read only.  This option only displays for existing blob stores.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on creating, viewing, or modifying blob stores.

## 21.2.4 Mount points

A mount point object represents a directory that is mounted by a client. It is a useful way to aggregate multiple locations that must be mounted.

### 21.2.4.1 Creating or modifying mount points

You can create a mount point object.

**Table 21-5: Mount point properties**

Field	Value
Name	The name of the mount point object. Some names, such as “events” or “common”, are reserved for Documentum CM Server use.
Host Name	The hostname for the machine on which this directory resides.
File System Path	The location of the directory or file represented by the location object. The path syntax must be appropriate for the operating system of the server host.  For example, if the server is on a Windows NT machine, the location must be expressed as a Windows NT path.   <b>Caution</b> Be sure that the combination of the host and path you specify does not point to the same physical location as any other file stores. If two file stores use the same physical location, data loss may result.
Security	The security level for this directory location. Options are: <ul style="list-style-type: none"><li>• Public Open</li><li>• Public</li><li>• Private</li></ul> The default value is Private.

Field	Value
<b>Unix Preferred Alias</b>	Set to the directory name used to mount the directory.
<b>Macintosh Preferred Alias</b>	Set to the volume name chosen for the mounted directory.  The volume name of the mounted directory is set when the directory is exported through the file-sharing system. It is the name that will appear in the Chooser for that directory.
<b>Windows Preferred Alias</b>	Set to the alias drive letter used to mount the directory.  For example, t:\ or k:\ .
<b>Comments</b>	Enter any comments about the mount point.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on creating or modifying mount points.

### 21.2.5 External stores

External storage areas do not store content. Instead, external stores point to the actual storage area, which can be a CD-ROM, a file system, a URL, or a user-defined store.

Data in an external store is not physically managed by Documentum CM Server. There are significant limitations on content in an external store. For example, you cannot index content or the properties of content in an external store.

External stores require a plug-in that you must create before you create an external store. The plug-in can run on the server side or client side, although a client-side plug-in could provide better performance. OpenText Documentum CM provides code for sample plug-ins in the DM\_HOME/unsupported/plugins directory.

There are three types of external stores:

- External file store

Use external file stores for legacy files in external file systems, optical disks, and CD-ROM files.

- External free store

External free store storage areas allow users to specify a token that is not a file path or a URL. An external free store enables you to define your own token standard and means of retrieving the content associated with the token. Write your own content retrieval mechanism through a DLL plug-in, which is described by a plug-in object.

You can also use the external free store pages to manually create OpenText™ Documentum™ Content Management XML Store. Use OpenText Documentum

Content Management (CM) XML Store to store and query large volumes of XML content. An XML Store is a native XML database that is fully optimized for XML content.

- External URL store

External URL stores provide support for token-mode operation where the token is a URL. The tokens specified in the Setpath operation must follow the URL standard. The client and the server do not validate the format of the URL.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* and *OpenText Documentum Content Management - XML Store Administration Guide (EDCCFMTXML250400-AGD)* provide more information about external XML file stores.

#### **21.2.5.1 Creating, viewing, or modifying external stores**

Create the appropriate plug-ins before configuring the external store. You can create, view, or modify an external file store, external free store, XML Store, or external URL store.

**Table 21-6: External store properties**

Field	Description
<b>Info</b>	
<b>Name</b>	The name of the new external store.
<b>Windows</b>	Indicates the plug-in that is used on Windows.
<b>Solaris</b>	Indicates the plug-in that is used on Solaris.
<b>AIX</b>	Indicates the plug-in that is used on AIX.
<b>HP-UX</b>	Indicates the plug-in that is used on HP-UX.
<b>Macintosh</b>	Indicates the plug-in that is used on Macintosh.
<b>Linux</b>	Indicates the plug-in that is used on Linux.
<b>HP-UX-Itanium</b>	Indicates the plug-in that is used on HP-UX-Itanium.
<b>Current Client Root</b>	The name of the location object that represents the default root of the content for executing plug-ins on the client when the mount is not executed. This option is only for external file stores.

Field	Description
<b>Client Root</b>	<p>The name of the location object that represents the default root of the content for client side plug-in execution when mount is not executed. The default is NULL. This option is only available for external file stores.</p> <p><b>Client Root:</b> Click <b>Browse</b> and select a client root.</p>
<b>Server</b>	The Server tab only displays for external file stores.
<b>Add</b>	Click <b>Add</b> or select the server on which the external file store resides, then click <b>Edit</b> to access the <b>Choose a server config</b> page.
<b>Server</b>	The name of the server where the external store resides.
<b>Location</b>	The location object that points to the external file store. Click <b>Select Location</b> to select a location object.
<b>Path</b>	Specifies the file system path to the external file store. The path displays automatically after you selected the location object.

### 21.2.5.2 Editing a server root location

The Select Root Location for Server page displays the server, location, and path that is the default root of the content for server side plug-in execution.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on editing a server root location.

## 21.2.6 Plug-ins

A plug-in is a shared library (on Linux) or DLL file (on Windows) for retrieving content when an external store is in use.

You must create the plug-in. OpenText Documentum CM provides code for sample plug-ins in the DM\_HOME/unsupported/plugins directory. The sample plug-ins are examples and are not supported.

The API interface between the shared library or DLL and the server consists of C functions for the plug-in library.

### 21.2.6.1 Creating or modifying plug-ins

You can create the plug-in object that represents the plug-in.

**Table 21-7: Plug-in properties**

Field	Value
Name	The name of the plug-in object.
Hardware Platform	Specifies one or more hardware platforms on which the plug-in can run.  Click <b>Edit</b> to access the <b>Hardware Platforms</b> page. Enter the hardware type in the <b>Enter a new value</b> field, then click <b>Add</b> . When all types are entered, click <b>OK</b> .
Operating System	Specifies one or more operating systems on which the plug-in can run.  Click <b>Edit</b> to access the <b>Host Machine</b> page. Enter the operating system in the <b>Enter a new value</b> field, then click <b>Add</b> . When all operating systems are entered, click <b>OK</b> .
Type	Select a file type. Options are: <ul style="list-style-type: none"><li>• <b>DLL (Windows)</b></li><li>• <b>SO (UNIX)</b></li></ul>
Usage	Type a comment on how the plug-in is used.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating or modifying plug-in objects.

### 21.2.7 NetApp SnapLock stores

A Network Appliance SnapLock (NetApp SnapLock) store stores large amounts of unchanging data such as email archives. NetApp SnapLock provides storage level retention capability through the creation of Write Once Read Many (WORM) volumes on Network Appliance storage systems. These WORM volumes enable users to prevent altering or deleting content until a specified retention date. NetApp SnapLock does not have advanced retention management features such as retention hold, event based retention, or privileged delete, which is available on a Centera store. You can define a retention date or, with Documentum CM Server 5.3 SP6 or later, a retention period for the content in a NetApp SnapLock store. You can also enable content compression for a SnapLock store.

There are two types of NetApp SnapLock stores:

- SnapLock Compliance store handles data retention to meet SEC regulations.

- SnapLock Enterprise store handles data retention to help customers meet their self-regulated date retention requirements.

The SnapLock documentation provided by Network Appliance contains more information about the two types of stores.

SnapLock requires:

- A Documentum CM Server version 5.3 SP6 or later
- A SnapLock storage device
- A connector

### 21.2.7.1 Creating, viewing, or modifying NetApp SnapLock stores

A repository can have multiple SnapLock stores. For ease of administration, maintenance, and management, it is recommended that you use the same plug-in for all the SnapLock stores.

On Linux, mount the SnapLock store to local disk using NFS. Use the mount point path in the SnapLock store object path. For example:

```
<snaplockhost:/path/to/use> </local/mount/point>
mount snapdisk:/u01/disk1 /dctm/snapstore
```

When you create the SnapLock store, use the name of the local mount path, /dctm/snapstore.

**Table 21-8: NetApp SnapLock store properties**

Field	Description
Name	The name of the NetApp SnapLock store.
Description	A description of the NetApp SnapLock store.

Field	Description
<b>Plug-in Name</b>	<p>The name of the plug-in for the NetApp SnapLock store. Options are:</p> <ul style="list-style-type: none"> <li>• Default Plugin: Select to set a null ID (0000000000000000) in the a_plugin_id property of the NetApp SnapLock store object.</li> <li>• Select Plugin: Select to use the default Snaplock Connection plug-in.</li> </ul> <p>When a repository is created, a default plug-in object is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> <li>– Windows: %DM_HOME%\bin\emcplugin.so</li> </ul> <p>When a repository is created, a default plug-in object is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> <li>• Windows: %DM_HOME%\bin\emcplugin.so</li> </ul>
<b>Snaplock Volume Path</b>	The directory path of the NetApp SnapLock storage system.
<b>Enable Content Compression</b>	<p>Specifies whether content compression is used. Select this option to compress all content in the store.</p> <p>Compression cannot be modified for existing NetApp SnapLock stores.</p>
<b>Configure Retention Information</b>	<p>Enables content retention.</p> <p>Content retention cannot be modified for existing NetApp SnapLock store.</p>
<b>Retention Attribute Name</b>	<p>The name of the retention attribute. The value must <i>not</i> be one of the values specified as a content attribute name.</p> <p>The retention attribute name cannot be modified for an existing NetApp SnapLock store.</p>

Field	Description
<b>Fixed Retention</b>	<p>Specifies a fixed value for the retention property value, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Choose a retention period:</b> Sets a period of days as the retention period for all content in the NetApp SnapLock store. Enter the date and time of the retention date.</li> <li>• <b>Choose default retention days:</b> Select and then type the number of retention days.</li> </ul> <p>Both default retention date and default retention days can be specified. If both are specified, the default retention days takes precedence over default retention date. If default retention date is selected but no value is specified, the system ignores the retention date option.</p>
<b>Event Based Retention</b>	<p>When Configure Retention Information is selected, the system automatically selects and inactivates this checkbox to prevent changing the event based retention option status.</p>
<b>Application Provides Retention</b>	<p>Requires that a client application supplies the retention date when content is saved to the NetApp SnapLock store.</p>

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying NetApp SnapLock stores.

### 21.2.8 Centera stores

A Centera store is a retention store for large amounts of unchanging data such as email archives or check images. Centera requires Content Services for EMC Centera (CSEC).

Use only the supported storage systems.

In a Centera store:

- Store metadata values with a piece of content.
- Store files created on Macintosh.

Both, Documentum CM Server and Foundation Java API must be on version 6.7 and there is no backward compatibility to older versions of Documentum CM Server and Foundation Java API. Any attempt to store resource forks into a Centera store using either an earlier Documentum CM Server or Foundation Java API version results in an exception/error message.

- Define a retention date or, with Documentum CM Server 5.3 SP3 or later, a retention period for the content.
- Index content.
- Enable content compression in 5.3 SP1 and later repositories.

A repository can have multiple Centera stores. For ease of administration, maintenance, and management, it is recommended that you use the same plug-in for all the Centera stores.

Set the C-clip buffer size or configure use of embedded blob storage by using optional storage parameters. Setting the C-clip buffer size is available only in 5.3 SP3 and later repositories.

Documentum CM Server supports distributed Centera clusters in 5.3 SP3 and later repositories. The Centera store plug-in must be stored depending on different server locations:

- If all Documentum CM Servers are running on the same computer, the Centera store plug-in must be in a file store.
- If the Documentum CM Servers are running on different hosts, the Centera store plug-in must be stored in a file store that is shared by all Documentum CM Server instances or in a distributed store in which each Documentum CM Server has at least one component defined as a near store.

#### 21.2.8.1 Creating, viewing, or modifying Centera stores

To create a Centera store, you must know the connection string of the Centera storage system.

**Table 21-9: Centera store properties**

Field	Description
Name	The name of the Centera store.
Description	A description of the Centera store.

Field	Description
<b>Plug-in Name</b>	<p>Specifies the plug-in that is used for the Centera store. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Default Plugin:</b> Sets a null ID (0000000000000000) in the a_plugin_id property of the Centera store object.</li> <li>• <b>Select Plugin:</b> Enables the default CSEC plug-in. To use a plug-in other than the default CSEC plug-in, click the <b>Select Plugin</b> link, locate the plug-in in the repository, select it, and click <b>OK</b>.</li> </ul> <p>When a repository is created, a default plug-in object for CSEC is created. If the plug-in object is deleted from the repository, no plug-in is displayed. Create a new plug-in object with the content of the plug-in object set as follows:</p> <ul style="list-style-type: none"> <li>• Windows: %DM_HOME%\bin\emcplugin.dll</li> <li>• Linux: \$DM_HOME/bin/libemcplugin.so</li> </ul>
<b>Storage Parameters</b>	<p>Specifies the storage parameters, such as the connection string, C-clip buffer size, and embedded blob storage.</p> <p>Click <b>Edit</b> to configure storage parameters.</p>
<b>Enable Content Compression</b>	<p>Specifies whether content compression is used. Select this option to compress all content in the store.</p> <p>Compression cannot be modified for existing Centera stores.</p>
<b>Configure Retention Information</b>	<p>Enables content retention.</p> <p>Content retention cannot be modified for existing Centera stores.</p>
<b>Retention Attribute Name</b>	<p>The name of the retention attribute. The value must <i>not</i> be one of the values specified as a content attribute name.</p> <p>The retention attribute name cannot be modified for an existing Centera store.</p>

Field	Description
<b>Fixed Retention</b>	<p>Specifies a fixed value for the retention property value, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Choose a retention period:</b> Sets a period of days as the retention period for all content in the Centera store. Enter the date and time of the retention date.</li> <li>• <b>Choose default retention days:</b> Select and then type the number of retention days.</li> </ul> <p>Both default retention date and default retention days can be specified. If both are specified, the default retention days takes precedence over default retention date. If default retention date is selected but no value is specified, the system ignores the retention date option.</p>
<b>Event Based Retention</b>	<p>When Configure Retention Information is selected, the system automatically selects and inactivates this checkbox to prevent changing the event based retention option status.</p>
<b>Application Provides Retention</b>	<p>Requires that a client application supplies the retention date when content is saved to the Centera store.</p>
<b>Add</b>	<p>Click <b>Add</b> to add a content attribute, or select an attribute from the list and click <b>Edit</b>. The Content Attribute window displays.</p> <p>Enter or modify the following information:</p> <ul style="list-style-type: none"> <li>• <i>Attribute Name:</i> The name of the content attribute. The content attribute name can be an arbitrary name. It does not have to correspond to any existing properties of the objects stored in the Centera store.</li> <li>• <i>Attribute Description:</i> A brief description of the content attribute.</li> </ul>

*OpenText Documentum Content Management - Administrator User Guide*  
*(EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying Centera stores.

### 21.2.8.2 Defining the storage parameters for a Centera store

You can add or modify storage parameters for the Centera store.

#### To define the storage parameters for a Centera store:

1. On the **Info** tab of the **EMC Centera Store Properties**, scroll to the **Storage Parameters** field and click **Edit**.  
The **Storage Parameters** page displays.
2. In the **Enter new value** field, type the connection string for the Centera storage system.

The connection string has the following format:

```
<IP_address>|<hostname>{,<IP_address>|<hostname>}?<Centera_profile>
```

where:

- *IP\_address* is the IP address of the Centera host.
- *hostname* is the host name of the Centera machine.
- *Centera\_profile* is a full-path specification of a Centera profile and must begin with “path=”.

The path must be accessible from the Documentum CM Server host machine and the specified directory must be readable by the Documentum CM Server installation owner.

The following example describes a connection string with multiple Centera profiles:

```
10.241.35.27,10.241.35.28?name=profA,secret=foo,10.241.35.27,10.241.35.28?  
name=profB,  
secret=bar,10.241.35.110,10.241.35.111?path=C:\Temp\auth.xml
```

In the following example, the SDK parses the passed-in connection string with the resulting elements going in the `outConnectionStrings` array, as follows:

```
outConnectionStrings [0] = 10.241.35.27?name=profA,secret=foo  
outConnectionStrings [1] = 10.241.35.28?name=profA,secret=foo  
outConnectionStrings [2] = 10.241.35.27?name=profB,secret=bar  
outConnectionStrings [3] = 10.241.35.28?name=profB,secret=bar  
outConnectionStrings [4] = 10.241.35.110?path=C:\Temp\auth.xml  
outConnectionStrings [5] = 10.241.35.111?path=C:\Temp\auth.xml
```

The following rules apply to the syntax of a connection string with multiple profiles:

- The IP address position must precede the listing of credentials and/or path for that profile.
- If the connection string includes a path that does not use the `path=` prefix but points to a PEA file and a set of credentials, the path must precede the

credentials. Conversely, when using the path= prefix, there is no restriction as to where the path appears in the connection string in relation to the set of credentials.

- The credentials that appear in a connection string override those that are held in a PEA file.
- It is best practice to use the optional path= prefix hint to specify the path to a PEA file, to avoid confusion when evaluating the connection string. Do not mix credential data in a connection string.

If configuring Centera clusters, the connection string format identifies primary and secondary Centera clusters for one or more Documentum CM Servers:

```
<server_config_name>="primary=<cluster_id>{,<cluster_id>},secondary=<cluster_id>{,<cluster_id>}[?<Centera_profile>]"
```

where:

- The primary *<cluster\_id>* is the name or IP address of the Centera cluster to which the Documentum CM Server writes.
- The secondary *<cluster\_id>* is the name or IP address of the Centera cluster from which the Documentum CM Server reads if it cannot read from the specified primary cluster.

Including a Centera profile is optional. The storage parameter property has a length of 1024 characters. Assign names to the Centera cluster nodes that are short enough to allow the full connection string to fit within the property.

3. Click **Add** to move the value to the **Storage Parameters** section.
4. Enter more storage parameters, as necessary.

For example :

- To enable embedded blob use, enter the following parameter:

```
pool_option:embedded_blob:<size_in_KB>
```

where *size\_in\_KB* is the maximum size in kilobytes of the content that you want to store as embedded blobs. For example, if you want to store all content that is 60 KB or smaller as embedded blobs, set the storage parameter value as:

```
pool_option:embedded_blob:60
```

If embedded blob use has been enabled and content is written to a compressed Centera store, Documentum CM Server writes the content as linked blob if the original content size is greater than the embedded blob threshold. This restriction still applies if the eventual compressed content size is less than or equal to the embedded blob threshold. If the original content size is less than the embedded blob threshold, the content is stored as embedded blob.

- To set the C-clip buffer size, enter the following parameter:

```
pool_option:clip_buffer_size:<integer>
```

where *<integer>* is an integer number representing the number of kilobytes. For example, to set the buffer size to 200 KB, set the storage value parameter as:

```
pool_option:clip_buffer_size:200
```

- To change the maximum number of socket connections that the Centera SDK can establish with the Centera host, enter the following parameter:

```
pool_option:max_connections:<integer>
```

where *<integer>* is an integer number from 1 to 999 specifying the maximum socket connections. By default, the maximum number of socket connections is 99 on Windows, and 1 on Linux.

5. Use the up and down arrows to sort the storage parameters.



### Caution

If you have entered multiple parameters, the Centera connection string must be in the first position.

6. When finished, click **OK**.

#### 21.2.8.3 Defining Centera store content attributes

Centera stores allow you to save up to 62 metadata values with each piece of content saved in the system.

##### To define the content attributes saved in a Centera store:

1. On the **Info** tab of the **EMC Centera Store Properties**, scroll to the Content Attribute section and click **Add**.  
The **Content Attribute** page displays.
2. Type the name of an attribute.  
The attribute name can be an arbitrary name. It does not have to correspond to any existing properties of the objects stored in the Centera store.
3. Type a description.
4. Click **OK**.
5. Repeat step 1 through step 4 to configure more attributes, if applicable.

## 21.2.9 Atmos stores

An Atmos store is a software storage system that consists of several distributed services running on a network of connected hardware nodes. Each node is attached to one or more disk enclosures. The nodes run a collection of services to store, retrieve, categorize, and manage the data in the system or cloud.

Documentum CM Server uses the Accelerated Content Services connector to communicate with the Atmos store. The Accelerated Content Services module supports storing and retrieving of content through an HTTP interface.

### 21.2.9.1 Creating, viewing, or modifying Atmos stores

**Table 21-10: Atmos store properties**

Field	Description
Name	The name of the Atmos store. The name must be unique within the system. The name of an existing Atmos store cannot be modified.
URL	The URL the server uses to communicate with the Atmos store.
Full Token ID	A combination of subtenant ID and a UID within that subtenant, both in the Atmos system that is being targeted. The format is subtenant ID/UID.
Shared Secret	The password of the user accessing the Atmos store.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying Atmos stores.

#### 21.2.9.1.1 Managing authentication

The Web service uses a combination of the Token ID, and other request headers to produce a signature that authenticates the user accessing the web service. It uses a combination of various pieces of the message to validate the identity of the sender, integrity of the message, and non-repudiation of the action. The Token ID that you received via e-mail from the portal agent administrator consists of the subtenant ID, and the UID separated by a slash (/). The subtenant ID is a randomly generated, 32 character alphanumeric string, which is unique to each customer. The UID, however, is unique to a web-based application. The UID, which appears after the slash, is comprised of a portion of the customer name, and a randomly generated string. For example, if the customer name is ACME, then the UID string appends the additional random characters. The whole Token ID contains 53 uppercase characters including the slash (for example: 5f8442b515ec402fb4f39ffab8c8179a/ACME03GF52E8D8E581B5).

To complete the authentication operation, you must generate a signature using the shared secret, which is associated with the UID. The shared secret is a value

generated by the Storage Utility Agent responsible for managing this application. The shared secret appears in the same e-mail message that contains the Token ID. The following sample represents a typical shared secret:  
MBqhzSzhZJCQHE9U4RBK9ze3K7U=

### 21.2.9.2 Storing content in Atmos store

The prerequisite for plug-in enabled stores is that Accelerated Content Services should always be running. Accelerated Content Services read/write may be disabled through configurations, but Accelerated Content Services service itself should not be stopped. Make sure that local Accelerated Content Services is running for storing content in Atmos store. When you stop the Accelerated Content Services/Java Method Server services, Foundation Java API assumes normal content transfer operation. However, the Documentum CM Server understands that the content belongs to the plug-in enabled store and uses Accelerated Content Services connector to communicate to Accelerated Content Services for storing content. The Accelerated Content Services connector identifies the dm\_acs\_config object for the local Accelerated Content Services to access the acs\_base\_url for communicating with the Accelerated Content Services. If you stop the Accelerated Content Services services, it will fail and Atmos storage will be shown as offline.

### 21.2.10 ViPR stores

ViPR is a software-defined storage platform that abstracts, pools, and automates the underlying physical storage infrastructure of a data center. It provides a single control plane to data center administrators for heterogeneous storage systems. Above the control plane, administrators can deploy ViPR Services (Object, HDFS, and Block Services) on array- and commodity-based storage that enable users to:

- Use ViPR file-managed storage as an object store
- Perform analytics on ViPR-managed storage
- Dynamically provision block commodity storage

ViPR enables software-defined data centers by providing the following features:

- Storage automation capabilities for multi-vendor block and file storage environments (control plane or ViPR Controller).
- Object data management and analytic capabilities through ViPR Object and HDFS Services, which creates a unified pool (bucket) of data across file shares and commodity servers (data path).
- Management of multiple data centers in different locations with Single sign-on data access from any data center.
- Data replication between geographically dispersed data centers to protect against data center failures with active-active functionality.

### 21.2.10.1 Creating, viewing, or modifying ViPR stores

Before creating, viewing, or modifying ViPR stores, make sure that you complete the following tasks:

- Install the license for ViPR Object on ViPR, including Amazon S3.
- Enable data services for object-based storage services and make sure that the Amazon S3 store is accessible.
- Create a bucket for data services to be used by the Documentum CM Server.

**Table 21-11: ViPR store properties**

Field	Description
Name	The name of the ViPR store. The name must be unique within the system. The name of an existing ViPR store cannot be modified.
URL	The URL that the server uses to communicate with the ViPR store. The URL format is <code>http://&lt;xx.xx.xx.xx&gt;:9020/&lt;&lt;bucket-name&gt;&gt;</code> . For example, <code>http://10.31.4.172:9020/csstore</code> .
Access Key ID	The user name of the user accessing the ViPR store. Use the ViPR Tenant Owner as the Access Key ID.
Shared Secret	The password of the user accessing the ViPR store. Use the Object Access Key as the Shared Secret.

The ViPR plugin is not provided with Documentum CM Server from the 21.4 release. Instead, you can use the S3 store plug-in updated with performance enhancements to configure ViPR store, as both the plugins use Amazon AWS SDK for the content transfer operations.

Optionally, you can update all metadata information from the existing ViPR store to the new S3 store.



**Note:** You can migrate only the metadata information but not the content.

To update all metadata information, perform the following tasks:

1. Obtain the details of existing ViPR store object using the following DQL query:

```
select * from dm_vipr_store
```

2. Obtain the count of dm\_sysobject and dmr\_content in the existing ViPR store to validate the count after migration using the following DQL query:

```
select count(*) from dmr_content where storage_id='<existing vipr store id>'  
select count(*) from dm_sysobject where a_storage_type='<existing vipr store name>'
```

3. Create a new S3 store object using Documentum Administrator or using the following API commands:

```
create,c,dm_s3_store
set,c,1,name
<new s3 store name>
set,c,1,base_url
<existing vipr url>
set,c,1,credential_id
<existing credential id>
set,c,1,credential_key
<existing credential key>
save,c,1
```

4. Update all metadata information to refer to the new S3 store object created in **step 3** using the following API command:

```
execsql,c,update dm_sysobject_s set a_storage_type='<new s3 store name>' where
a_storage_type='<existing vipr store name>'
execsql,c,update dmr_content_s set storage_id='<new s3 store id>' where
storage_id='<existing vipr store id>'
```

5. Verify if all objects are updated successfully using the following DQL query:

```
select count(*) from dmr_content where storage_id='<new s3 store id>'
select count(*) from dm_sysobject where a_storage_type='<new s3 store name>'
```

6. Compare the results in **step 2** and **step 5** and make sure both are equal.

### 21.2.11 Amazon S3 stores

Amazon Simple Storage Service (Amazon S3) is a highly durable and available store that can be used to reliably store application content such as media files, static assets and user uploads. It allows you to offload your entire storage infrastructure and offers better scalability, reliability, and speed than just storing files on the file system. You can use it as a content store for Documentum CM Server.

The following functions are supported:

- Push or pull of data
- Migration of data to or from S3 store: You can use the content migration job to perform the migration. Migration of data is supported as follows:
  - File store to S3 store
  - S3 store to file store
  - EMC Centera store to S3 store
  - S3 store to EMC Centera
  - XML Store to S3 store
  - S3 store to XML Store
  - Encrypted S3 store to file store
  - File store to encrypted S3 store
  - Encrypted S3 store to XML Store

- XML Store to encrypted S3 store
  - Encrypted S3 store to EMC Centera store
  - EMC Centera store to encrypted S3 store
  - Encrypted file store to encrypted S3 store
  - Encrypted S3 store to encrypted file store
  - External file store to S3 store
  - External file store to encrypted S3 store
- Configuring the store to use SSL: S3 store can be configured to use SSL communication between S3 plug-in and S3 storage service. Default SSL is achieved by providing SSL URL in the `base_url` attribute (for example, `https://<storageservice-hostname>:443/<bucketname>`). If you want to use your certificates, import those certificates to the Java keystore of JDK that is used by the S3 plug-in.
  - Encrypted store: To use S3 store as an encrypted store (similar to other OpenText Documentum CM stores), set the value of `crypto_mode` to 1. When `crypto_mode` is set to 1, Documentum CM Server (Accelerated Content Services connector module of Documentum CM Server) encrypts the content before pushing it to the store. When content is retrieved, Documentum CM Server decrypts and sends it back to the client.



### Notes

- Trusted Content Services is required to use OpenText Documentum CM S3 store as an encrypted store.
  - If you use S3 store as the default object store, compression and de-duplication are not supported.
- Retention: Documentum CM Server supports SysObject level retention on all S3-compatible stores.

Documentum CM Server operations such as insertion, modification, and deletion of content is controlled by the object retainers. The retention date on the retainer object is applied on the SysObject which is pushed to the file for WORM-enabled stores. If the maximum retention date given in the retainer is later than the default retention date (if it exists), the default retention date is overridden. The object cannot be modified or deleted until the specified retention date expires.

- WORM support: Documentum CM Server leverages store level retention on the WORM-enabled S3-compatible stores. The following table lists the certified storage:

Storage	Fixed retention	Conditional retention
IBM Cloud Object Storage (COS)	Supported from the 16.7 release	Supported from the 20.4 release

Storage	Fixed retention	Conditional retention
Amazon S3	Supported from the 16.7.1 release	Not supported
Hitachi Content Platform (HCP)	Supported from the 16.7.1 release	Not supported
Dell EMC Elastic Cloud Storage (ECS)	Supported from the 21.1 release	Not supported
NetApp StorageGRID (supported version is 11.5 or later)	Supported from the 21.4 release	Not supported

S3 stores are cloud-based services and hence PUT/GET or POST operations are used to manage retentions. Documentum CM Server acts as an HTTP client that generates POST request with appropriate headers for pushing the retention to the S3 store.

Common request headers are: Content-Length, Content-Type, Date, Host, and so on.

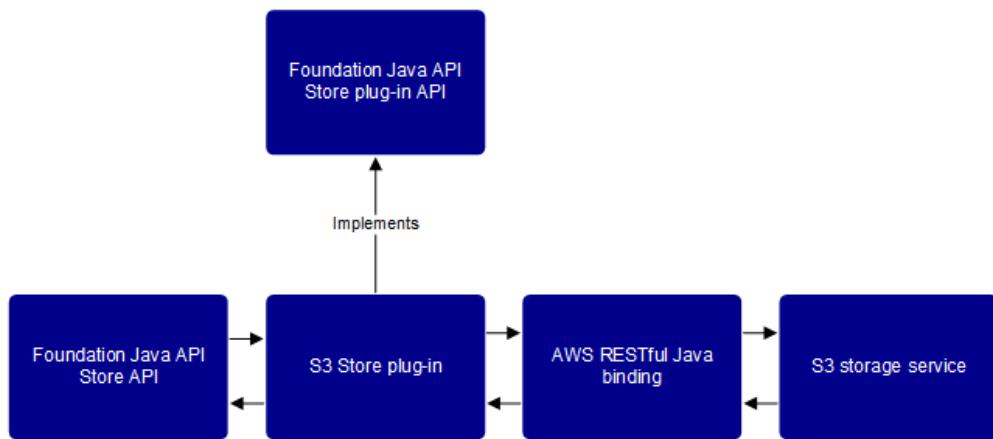
HTTP authorization header is the most common method of authenticating an Amazon S3 request. AWS Signature Version 4 (v4) is the process to add authentication information to AWS requests sent by HTTP. [AWS documentation](#) contains detailed information about v4 signing.

### 21.2.11.1 Using the S3 store plug-in

A store plug-in is used to make the communication between OpenText Documentum CM and External Store (S3). The store plug-in implements the contract defined by Foundation Java API store plug-in interface and provides content transfer capability. This implementation acts as a bridge or adaptor between the Foundation Java API store plug-in and the Amazon S3 RESTful Java API binding.



**Note:** The prerequisite for plug-in-enabled stores is that the Accelerated Content Services must always be running. Accelerated Content Services read/write may be disabled through configurations, but Accelerated Content Services itself must not be stopped.



**Figure 21-1: Authentication flow using S3 store plug-in**

The plug-in modules are deployed as BOF modules. The S3 plug-in is available in the `java_access` attribute of the `dm_store` subtype object (`dm_s3_store`). The plug-in needs the support of other external libraries. These external libraries are deployed as Java libraries with the BOF modules. All the deployment rules pertaining to BOF modules and TBOs apply as is. Also, all the required BOF modules (`s3-tbo-api.jar` and `s3-tbo-impl.jar`) and dependent Java libraries (`aws s3 client libs`) are packaged as part of the `S3Plugin.dar` file.

The following operations are supported:

- Read Content: Calls the `readObjectAsStream` call of the RESTful API and pulls the content from the S3 store.
- Write Content: Uses the RESTful API to write the content to S3 with the supplied metadata. The returned object identifier is passed to the upper layer wrapped as a `StoreResult` Object implementation of `IStoreWriteResult`.
- Delete Content: Calls the S3 Delete Content API.
- Write or Update Metadata: Metadata is passed to the plug-in by Foundation Java API. Adds the content id as metadata to the objects or content that are being pushed to S3. The metadata is a key value pair. For example, the key is `dmr_content_id` and the value is [The Content Object Id].

The store is configured with the following information:

- `java_access`: Name of the module (S3 plug-in) that the store object represents. The default value is `S3 Plugin` for the `dm_s3_store` type objects.
- `base_url`: S3 storage service URL. Format is `http://<X.X.X.X>/<BUCKET>` where
  - `X.X.X.X`: URL of S3 store service and the URL format is `http://hostname:port`.

- BUCKET: Name of the S3 bucket used to push the content. This name is mandatory. Bucket must be preconfigured in the S3 storage service and accessible using the following credentials:
  - o credential\_id: Access Key (user ID or access key to access the store service). If you want to use the S3 role-based access, make sure that you do not set any value.

In cloud platforms, if Vault is enabled, make sure that you have stored the following secret in Vault:

**Table 21-12: Secret and key name**

Secret name	Key name	Description
S3_STORE_CREDENTIAL_ID	<store name>	S3 store credential ID. For example, S3_STORE_CREDENTIAL_ID/s3storename.

- o credential\_key: Password for accessing the store. Foundation Java API encrypts or decrypts this password before storing and passing it on to the plug-in. If you want to use the S3 role-based access, make sure that you do not set any value.

In cloud platforms, if Vault is enabled, make sure that you have stored the following secret in Vault:

**Table 21-13: Secret and key name**

Secret name	Key name	Description
S3_STORE_CREDENTIAL_KEY	<store name>	S3 store credential key. For example, S3_STORE_CREDENTIAL_KEY/s3storename.

- store\_params: Configuration parameters for the WORM support. The configuration parameters are stored as key-value pair with the following optional pre-defined keys:
  - o proxy\_host: The IP address of the proxy server.
  - o proxy\_port: The port reserved for the proxy server.
  - o region: The region where S3 bucket is configured.
  - o query\_parameter: The URL query parameter that the corresponding S3 store vendor expects for extending retention. This is specific to the compatible store.
  - o retention\_header\_name: Header used for specifying the new retention date. The date format must be in accordance to the ISO 8601 format (YYYYMMDDThhmmssZ). This is specific to the compatible store.

- `ecs_allow_copies`: By default, for the Dell EMC ECS store, Documentum CM Server allows adding the retention on sysobject only once as it requires storage copy. However, setting the value to a finite number allows multiple copies for fixed retention.
- `mode`: Retention mode that applies to different levels of protection.
- `vendor`: Specifies the storage vendor.



**Note:** The `query_parameter` and `retention_header_name` configuration parameters are deprecated for the WORM-enabled S3 stores from the 20.4 release.

After it is configured, the store is accessible as any other Documentum CM Server store. A new TBO is created for the plug-in. The `dm_s3_store` object cannot be updated after it is created. All the contents uploaded to the Amazon S3 store have an unique key. This key is derived from the content-id.

### 21.2.11.2 Creating, viewing, or modifying S3 stores

**Table 21-14: S3 store properties**

Field	Description
<b>Name</b>	The name of the S3 store. The name must be unique within the system. The name of an existing S3 store cannot be modified.
<b>URL</b>	The URL that the server uses to communicate with the S3 store. The URL format is <code>http://&lt;X.X.X.X&gt;/&lt;&lt;BUCKET&gt;&gt;</code> .
<b>Access Key ID</b>	The user name of the user accessing the S3 store. Use the S3 Tenant Owner as the Access Key ID. This is an optional field.
<b>Shared Secret</b>	The password of the user accessing the S3 store. Use the Object Access Key as the Shared Secret. This is an optional field.
<b>Proxy Host</b>	The IP address of the proxy server. This is an optional field. However, you must provide a value if Documentum CM Server host is behind the proxy server and s3 object store in the public cloud.
<b>Proxy Port</b>	The port reserved for the proxy server. This is an optional field. However, you must provide a value if Documentum CM Server host is behind the proxy server and s3 object store in the public cloud.
<b>Region</b>	The region where S3 bucket is configured. This is an optional field.

Field	Description
<b>Query Parameter</b>	The URL query parameter that the corresponding S3 store vendor expects for extending retention. This is specific to the compatible store. This is an optional field.
<b>Retention Header Name</b>	Header used for specifying the new retention date. The date format must be in accordance to the ISO 8601 format (YYYYMMDDThhmmssZ). This is specific to the compatible store. This is an optional field.
<b>Mode</b>	Retention mode that applies to different levels of protection. This is an optional field used for the <b>AmazonS3</b> vendor only. Valid values are: <ul style="list-style-type: none"> <li>• null</li> <li>• COMPLIANCE</li> <li>• GOVERNANCE: This is the default value for Amazon S3.</li> </ul>
<b>Vendor</b>	Specifies the storage vendor. This is an optional field. Valid values are: <ul style="list-style-type: none"> <li>• null</li> <li>• AmazonS3</li> <li>• NetAppStorageGRID</li> <li>• HCP</li> <li>• IBMCOS</li> <li>• EMCECS</li> </ul>

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying S3 stores.

### 21.2.11.3 Configuring S3 store properties

Set the appropriate configuration values in the `s3.properties` file available in `%DM_JMS_HOME%\webapps\ACS\WEB-INF\classes`.

- For use of v4 signing for all S3 requests, set the value of `enable-v4signing` to `true`. The default value is `false`.
- To include MD5 checksum value to verify the integrity of the object, set the value of `enable-md5` to `true`. The default value is `false`.



**Note:** When md5 is enabled, the default value of `mds-multipart-threshold` is 10 MB.

- To randomize the beginning component of the object name to increase performance, set the value of `use-random-in-filename` to `true`. The default value is `false`.
- When multipart upload is chosen, the part-size reflects the size of the portion of content that needs to be uploaded to the S3 store. Set the value of `part-size` to `5`. The part size is considered as megabytes. The default value is `5 MB`.
- To enable multipart download, update the `dm_s3_store` object. Do the following:
  - Set the value of `multipart_download` to `true`.
  - Set the value of `multipart_download_min_size` to `100` (minimum file size in MB).
  - Set the value of `multipart_download_max_size` to `1024` (maximum file size in MB).
- To perform parallel multipart processing, set the value of `multipart-parallel-processing` to `true`. The default value is `false`.
- To set the number of threads to be used during multipart parallel processing, set the value of `multipart-processing-thread.pool-size` to `5`. The default value is `5`.
- To allow temporary credentials for authenticating S3 store users to access Amazon S3 resources and within a specific time period, use the following parameters:
  - `use-tempcredentials`: Used to enable temporary credentials to access Amazon S3 resources using Security Token Service (STS). Valid values are `true` and `false`. If you set the value to `true`, temporary credentials are used for authentication. If you set the value to `false`, permanent credentials are configured and used for authentication.
  - `s3-sessiontoken-duration`: Used to configure the temporary token duration interval (in seconds). After the duration, the temporary token is refreshed and a new token is created. The minimum value is `900` seconds and the maximum value is `86400` seconds.



**Note:** If you set the value lesser than the minimum value, then the Documentum CM Server takes the minimum value as `900` seconds. If you set the value greater than the maximum value, then the Documentum CM Server takes the maximum value as `86400` seconds.

#### 21.2.11.4 Logging

Tracing is in line with the Foundation Java API tracing activity. However, there are additional log statements at the DEBUG level that appears in the log. The DEBUG level can be enabled using `log4j2.properties` in Accelerated Content Services.

- Windows: `%DM_JMS_HOME%\webapps\ACS\WEB-INF\classes\log4j2.properties`
  - Linux: `$DM_JMS_HOME/webapps/ACS/WEB-INF/classes/log4j2.properties`
1. Open `log4j2.properties`.
  2. Update the `rootCategory` tracing to DEBUG. For example, `log4j.rootCategory=DEBUG, A1, F1`.
  3. Control the log level for external stores such as S3 and REST as follows:

```
logger.store.level=<log level>
```

#### 21.2.11.5 Troubleshooting

The logging and tracing information generated by Foundation Java API and Accelerated Content Services is sufficient for troubleshooting. To verify if store plugins for S3 and TBO for S3 store are installed, run the queries in IAPI to get the expected results.

- To verify if the plug-in module and its dependencies are installed, use the following query format:

```
API> ?,c,select r_object_id,object_name from dm_sysobject  
where FOLDER('/System/Modules/S3_Plugin',DESCEND)
```

Result:

r_object_id	object_name
09xxxxxxxxxxxxxx	S3 Plugin
0bxxxxxxxxxxxxxx	External Interfaces
0bxxxxxxxxxxxxxx	Miscellaneous
0bxxxxxxxxxxxxxx	S3 Plugin Libraries
09xxxxxxxxxxxxxx	aws-java-sdk-s3
09xxxxxxxxxxxxxx	commons codec-s3
09xxxxxxxxxxxxxx	commons logging-s3
09xxxxxxxxxxxxxx	http client-s3
09xxxxxxxxxxxxxx	http core-s3
09xxxxxxxxxxxxxx	jackson-annotations-s3
09xxxxxxxxxxxxxx	jackson-core-s3
09xxxxxxxxxxxxxx	jackson-databind-s3
09xxxxxxxxxxxxxx	joda-time-s3
(14 rows affected)	

- To verify if the TBO for `dm_s3_store` is installed, use the following query format:

```
API> ?,c,select r_object_id,object_name from dm_sysobject  
where FOLDER('/System/Modules/TBO/dm_s3_store',DESCEND)
```

Result:

r_object_id	object_name
08xxxxxxxxxxxxxx	RuntimeEnvironment.xml

```
09xxxxxxxxxxxxxx s3-tbo-api
09xxxxxxxxxxxxxx s3_tbo_impl
0bxxxxxxxxxxxxxx External Interfaces
0bxxxxxxxxxxxxxx Miscellaneous
(5 rows affected)
```



**Note:** The xxxxxxxxxxxxxxxx is the object id of the repository.

## 21.2.12 OpenStack Swift stores

The OpenStack Swift store offers cloud storage software to store and retrieve lots of data with a simple API. It is optimized for durability, availability, and concurrency across the entire data set. It is ideal for storing unstructured data that can grow without bound. You can use OpenStack Swift as a content store for Documentum CM Server.

A store plug-in using REST APIs is used to allow Documentum CM Server to configure OpenStack Swift as a data store. This plug-in is available as dm\_swift\_store type in Documentum CM Server.

The store is configured with the following information:

- `base_url`: OpenStack Swift authentication endpoint (for example, `http://10.0.0.1:35357/v2.0`)
- `credential_id`: Format is `tenantName:username` (for example, `(admin:admin)`)
- `credential_key`: password
- `container`: Name of the container to store the content
- `region`: (optional) Name of the preferred region to store the content

After it is configured, the store is accessible as any other Documentum CM Server store. A new TBO is created for the plug-in. All the contents uploaded to the OpenStack Swift store have an unique key. This key, which is in the form of a Linux path, is derived from the content-id.

### 21.2.12.1 Creating, viewing, or modifying OpenStack Swift stores

**Table 21-15: OpenStack Swift store properties**

Field	Description
<b>Name</b>	The name of the OpenStack Swift store. The name must be unique within the system. The name of an existing OpenStack Swift store cannot be modified.

Field	Description
<b>Authentication endpoint URL</b>	The URL that the server uses to communicate with the OpenStack Swift store. API version v2.0 and auth/v1.0 endpoints are supported for OpenStack Keystone integration and /v1 endpoint is supported for basic authentication. For example, http://10.0.0.1:35357/v2.0.
<b>Account Owner</b>	The user name of the user accessing the OpenStack Swift store.
<b>Password</b>	The password of the user accessing the OpenStack Swift store.
<b>Container</b>	The name of the container to store the content.
<b>Region</b>	The name of the preferred region to store the content. This is an optional field.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying OpenStack Swift stores.



**Note:** To perform operations in Docker, you must provide the hostname details in /etc/hosts of the OpenStack Swift store in Docker host and containers.

### 21.2.13 REST stores

Documentum CM Server supports Azure Blob and Google Cloud storage types as REST object store. The two main components are REST store plug-in and Accelerated Content Services connector.

The following functions are supported:

- Push and pull of data.



**Note:** The push and pull operations do not work with the HTTP mode in `base_url`.

- Migration of data to or from REST store: You can use the content migration job to perform the migration. Migration of data is supported as follows:
  - File store to REST store
  - REST store to file store
  - File store to encrypted REST store
  - Encrypted REST store to file store
  - Encrypted file store to encrypted REST store

- Encrypted REST store to encrypted file store
  - Encrypted file store to REST store
  - REST store to encrypted file store
  - File store to compressed REST store
  - Compressed REST store to encrypted file store
  - Encrypted file store to compressed REST store
  - Compressed REST store to file store
  - Compressed REST store to encrypted file store
  - S3 store to REST store
  - REST store to S3 store
  - Compression-enabled file store to compression-enabled REST store
  - Compression-enabled REST store to compression-enabled file store
  - External file store to REST store
  - REST store to external file store
- Configuring the store to use SSL: REST store can be configured to use SSL communication between REST plug-in and REST storage service. Default SSL is achieved by providing SSL URL in the `base_url` attribute. If you want to use your certificates, import those certificates to the keystore that is used by the REST plug-in.
  - Encrypted store: To use REST store as an encrypted store (similar to other OpenText Documentum CM stores), set the value of `crypto_mode` to 1. When `crypto_mode` is set to 1, Documentum CM Server encrypts the content before pushing it to the store. When content is retrieved, Documentum CM Server decrypts and sends it back to the client.
  - Documentum CM Server supports container level retention on Azure Blob and Google Cloud REST stores. Documentum CM Server operations such as modification and deletion of content is controlled by Azure Blob and Google Cloud storage types' time-based retention policy at container level. The retention days applied on the container decides if content can be modified or deleted. The object cannot be modified or deleted until the specified retention days are over for that particular object. REST stores are cloud-based services and hence PUT/GET or POST operations are used to manage retentions.
  - Compressed store: To use REST store as a compressed store, set the value of `compression_mode` to 1. When `compression_mode` is set to 1, Documentum CM Server (Accelerated Content Services REST plug-in module) compresses the content before pushing it to the store. When the content is retrieved, the REST plug-in module decompresses the content and sends it back to the client.
  - De-duplication: To support de-duplication for the REST store and save storage space for duplicate contents, set `content_dupl_pref` and `content_hash_mode` as a non-zero value as described in *OpenText Documentum Content Management -*

*Server System Object Reference Guide (EDCCS250400-ORD)*. You must set the value of `content_dupl_pref` and `content_hash_mode` to 4 as only SHA3-384 is supported. When the same content is pushed to the REST store, and if deduplication is enabled, the REST plug-in does not push content to the store again. However, the REST plug-in references the endpoint to the content to which it matches and already available. In addition, the content is deleted only if there are no other sysobjects referenced.

### 21.2.13.1 Using the REST store plug-in

The REST store plug-in is used to make the communication between OpenText Documentum CM and External Store (Azure Blob and Google Cloud storage types). The store plug-in implements the contract defined by the Foundation Java API `IStoreAccessor` interface and provides content transfer capability. This implementation acts as a bridge or adaptor between the Foundation Java API store plug-in and the RESTful API binding of the cloud store (Azure Blob or Google Cloud).



**Note:** The prerequisite for plug-in-enabled stores is that the Accelerated Content Services must always be running. Accelerated Content Services read/write may be disabled through configurations, but Accelerated Content Services itself must not be stopped.

The plug-in modules are deployed as BOF modules. The REST plug-in is available in the `java_access` attribute of the `dm_store` subtype object (`dm_rest_store`). This plug-in needs the support of other external libraries. These external libraries are deployed as Java libraries with the BOF modules. All the deployment rules pertaining to BOF modules and TBOs apply as is. In addition, all the required BOF modules (`rest-tbo-api.jar` and `rest-tbo-impl.jar`) and dependent Java Spring Boot libraries (web client, beans, and so on) are packaged as part of the `reststore.jar` file.

The following operations are supported:

- Read Content: Calls the `readContent` BOF module API and pulls the content from the REST store.
- Write Content: Uses the RESTful API to write the content to Azure with the supplied metadata. The returned object identifier is passed to the upper layer wrapped as a `StoreResult` (implementation of `IStoreWriteResult`).
- Delete Content: Calls the `deleteContent` API which makes a delete API call to the REST store.
- Write or Update Metadata: Metadata is passed to the plug-in by Foundation Java API. Adds the content id as metadata to the object that is being pushed to the REST store. The metadata is a key value pair. For example, the key is `dmr_content_id` and the value is [The Content Object Id].



**Note:** The *page blob* and *append blob* blob types of Azure Blob storage type are not supported.

The store is configured with the following information:

- `java_access`: Name of the module (REST plugin) that the store object represents. The default value is `rest plugin` for the `dm_rest_store` type objects.
- `base_url`: REST storage service URL.
  - For Azure Blob storage type: Format is `https://<name of storage account>.blob.core.windows.net/<name of container>` where
    - `<name of storage account>`: Azure Blob storage account name.
    - `<name of container>`: Name of the Azure Blob container used to push the content. This name is mandatory. The container may or may not be preconfigured in the Azure Blob Storage's service and is accessible using the following credentials:
  - `credential_id`: Azure Blob storage account name.

In cloud platforms, if Vault is enabled, make sure that you have stored the following secret in Vault:

**Table 21-16: Secret and key name**

Secret name	Key name	Description
AZURE_STORE_CREDENTIAL_ID	<store name>	Azure store credential ID. For example, AZURE_STORE_CREDENTIAL_ID/azurestorename.

- `credential_key`: Azure provided key for accessing the store. Foundation Java API encrypts or decrypts this password before storing and passing it on to the plug-in.

In cloud platforms, if Vault is enabled, make sure that you have stored the following secret in Vault:

**Table 21-17: Secret and key name**

Secret name	Key name	Description
AZURE_STORE_CREDENTIAL_KEY	<store name>	Azure store credential key. For example, AZURE_STORE_CREDENTIAL_KEY/azurestorename.

- `rest_store_type`: You must set the value to 0.



**Note:** Any value other than 1 for `rest_store_type` is considered for Azure Blob storage type only.

- For Google Cloud storage type: The format is `https://storage.googleapis.com/<name of container>` where `<name of container>` is the name of the Google Cloud storage container used to push the content. This name is mandatory. The container may or may not be preconfigured in the Google Cloud Storage's service and is accessible using the Google Cloud storage type service account credentials exported in the JSON format.
- `rest_store_type`: You must set the value to 1.
- `credential_id`: Google Cloud storage type service account credentials. If Vault is enabled, make sure that you have stored the following secret in Vault:

**Table 21-18: Secret and key name**

<b>Secret name</b>	<b>Key name</b>	<b>Description</b>
GCP_CREDENTIALS	<code>&lt;repository name&gt;_&lt;filestore name&gt;</code>	Google Cloud storage type service account credentials. For example, <code>GCP_CREDENTIALS/gcprepo_gcpstorename</code> .

In addition, configure the Vault information as follows:

- o `store_params`: Configuration parameters for the Vault support. The configuration parameters are stored as key-value pair with the following pre-defined keys:
  - `is_vault_enabled`: To enable the Vault configuration. Set the value to `true`.
  - `dsis_url`: URL to connect to the DSIS daemon agent. The format is `http://localhost:<dsis.dctm.port>/dsis`.
  - `dsis_token`: Token to authenticate with the DSIS daemon agent. Set the value to the same value provided for `dsis.dctm.token`.

For more information about the preceding keys, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

If Vault is not enabled, create a `dm_document` object in the repository with the credentials JSON file as content-file. Then, set the value of `r_object_id` to `credential_id`.



**Note:** The authentication file in the JSON format that you export must be explicitly saved to the local filestore, even if your default store is S3 or Azure Blob or Google Cloud.

After it is configured, the store is accessible as any other Documentum CM Server store. A new TBO is created for the plug-in. The `dm_rest_store` object cannot be updated after it is created. All the contents uploaded to the REST store using Azure Blob or Google Cloud storage type have an unique key. This key is derived from content-id.

OpenText Documentum CM clients (for example, Documentum Administrator) uses the **UCF > ACS > Store Plugin > REST** path to store and retrieve content from the REST store.

### 21.2.13.2 Creating, viewing, or modifying REST stores

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying REST stores.

### 21.2.13.3 Configuring REST store properties

Set the appropriate configuration values in the `rest.properties` file available in `%DM_HOME%\webapps\ACS\WEB-INF\classes`.



**Note:** If you are upgrading from an earlier version (for example, 20.4), you must manually copy the values of `rest.properties` available from `%DM_HOME%\bin` (earlier version environment) to `rest.properties` available in `%DM_HOME%\webapps\ACS\WEB-INF\classes` (upgrade environment).

- For proxy settings, set the appropriate values for the following properties:
  - `PROXY_HOST`: The IP address of the proxy server.
  - `PROXY_PORT`: The port reserved for the proxy server.
- To enable the MD5 checksum value to verify the integrity of the object while sending requests to the REST store, set the value of `enable-md5` to `true`. The default value is `false`.
- When multipart upload is chosen, the part-size reflects the size of each portion of content that needs to be uploaded to the REST store. Set the value of `part-size` as needed. The part-size is considered as megabytes. It is an optional field and the default value is 5 MB.
- To perform parallel multipart processing in Azure Blob storage type, set the value of `multipart-parallel-processing` to `true`. The default value is `false`.



#### Notes

- Parallel multipart processing is not supported for Google Cloud storage type.
- If you set `multipart-parallel-processing` to `true`, multipart processing works sequentially for the Google Cloud storage type.
- To perform the sequential multipart processing, set the value of `multipart-sequential-processing` to `true`. The default value is `false`.



**Note:** To perform the sequential multipart processing, the value of `multipart-parallel-processing` must be set to `false`.

- To set the number of threads to be used during multipart parallel processing, specify a value for `multipart-processing-thread.pool-size`. The default value is 20.

#### 21.2.13.4 Logging

Tracing is in line with the Accelerated Content Services tracing activity. However, there are additional log statements at the DEBUG level that appears in the log. The DEBUG level can be enabled using `log4j2.properties` in Accelerated Content Services.

- Windows: `%DM_JMS_HOME%\webapps\acs\WEB-INF\classes\log4j2.properties`
  - Linux: `$DM_JMS_HOME/webapps/acs/WEB-INF/classes/log4j2.properties`
1. Open `log4j2.properties`.
  2. Update `rootLogger.level` tracing to DEBUG.
  3. Append the following lines at the end of the file:

```
appender.rest.type=RollingFile
appender.rest.fileName=%DM_JMS_HOME%/logs/rest.log
appender.rest.name=RestFile
appender.rest.filePattern=${filename}.%d{yyyy-MM-dd}
appender.rest.layout.type=PatternLayout
appender.rest.layout.pattern=%d{ABSOLUTE} %5p [%t] %c - %m%n
appender.rest.policies.type=Policies
appender.rest.policies.time.type=TimeBasedTriggeringPolicy
appender.rest.policies.time.interval=1
appender.rest.policies.time.modulate=true
appender.rest.policies.size.type=SizeBasedTriggeringPolicy
appender.rest.policies.size.size=10MB
appender.rest.strategy.type=DefaultRolloverStrategy
appender.rest.strategy.max=5

logger.rest.name = com.documentum.content.store.plugin.rest
logger.rest.level = <DEBUG/INFO/WARN>
logger.rest.additivity = false
logger.rest.appenders = rest
logger.rest.appenders.rest.ref = RestFile
```

4. If you want the information about the call stack during any exception, set the value of `REST_STORE_STACK_TRACE` to 1. This records the call stack information in `rest.log`.

### 21.2.13.5 Troubleshooting

The logging and tracing information generated by Foundation Java API and Accelerated Content Services is sufficient for troubleshooting. To verify if the REST plug-in and TBO for the REST store are installed, run the queries in IAPI to get the expected results.

- To verify if the plug-in module and its dependencies are installed, use the following query format:

```
API> ?,c,select r_object_id,object_name from dm_sysobject where FOLDER('/System/Modules/TBO/dm_rest_store',DESCEND)
```

- To verify if the TBO for dm\_rest\_store is installed, use the following query format:

```
API> ?,c,select r_object_id,object_name from dm_sysobject where FOLDER('/System/Modules/rest plugin',DESCEND)
```

## 21.2.14 Distributed stores

A distributed store storage area does not contain content. Instead, it points to component storage areas containing the content. The component storage areas in a distributed store can be any mixture of the file store and linked store storage types, but all the components must store the same kind of content.

Distributed storage areas are useful when repository users are located in widely separated locations. You can define a distributed storage area with a component in each geographic location and set up the appropriate content replication jobs to make sure that content is current at each location.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* describes how to implement and administer a distributed storage area. *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* lists the properties defined for the distributed store object type.

### 21.2.14.1 Creating, viewing, or modifying distributed stores

You can create, view, or modify, a distributed store.



**Note:** When a repository is configured to use distributed storage, it cannot be converted back to non-distributed storage.

**Table 21-19: Distributed store properties**

Field	Description
Info	

Field	Description
<b>Name</b>	The name of the distributed store. This name must be unique within the repository and must conform to the rules governing type names. This field is read only in modify mode.
<b>Fetch Content Locally Only</b>	Indicates whether the server fetches content locally or from far stores that are not available locally.
<b>Get Method</b>	<p>To install a custom SurrogateGet, click <b>Select Method</b> to access the Choose a method page to select a method on the server host file system.</p> <p>Generally, when users attempt to fetch a document that is stored in an inaccessible far storage area, the server returns an error message. In such cases, the system administrator has to replicate the content into a storage area that is accessible. To automate this administrative task, OpenText Documentum CM provides the surrogate get feature, which allows the server to automatically replicate content when a fetch fails.</p> <p>Implement this feature using the surrogate get method provided by default with the Documentum CM Server system administration tool suite (named dm_SurrogateGet), or write your own surrogate get program. If you write your own, fill in the method name here.</p>
<b>Offline Get Method</b>	<p>Controls whether the server regards retrieved content as immediately available or awaiting restoration.</p> <p>This field is only meaningful when the Get Method field contains a value.</p>
<b>Status</b>	Indicates whether the storage area is on line, off line, or read only.
<b>Components</b>	
<b>Add</b>	<p>Adds stores to the distributed store.</p> <p>Click <b>Add</b>. The <b>Choose a storage:</b> page displays. Select the stores in the left column you want to add and move them to the right column, using the right arrow button.</p>

Field	Description
<b>Remove</b>	Removes stores from the distributed store. Select a store in the store list and click <b>Remove</b> to remove the store from the distributed store.

*OpenText Documentum Content Management - Administrator User Guide* (*EDCAC250400-UGD*) contains the instructions on creating, viewing, or modifying distributed stores.

## 21.2.15 Locations

The directories that a Documentum CM Server accesses are defined for the server by location objects. A location object can represent the location of a file or a directory.

### 21.2.15.1 Creating or modifying locations

A location object contains a file system location for a specific file or directory. The server uses the information in location objects to find the files and directories that it needs for successful operation. Create the directory on the file system before creating a location object.

**Table 21-20: Location object properties**

Field	Value
<b>Name</b>	The name of the location object. Some names, such as “events” or “common”, are reserved for Documentum CM Server use.
<b>Choose a Mount Point for this Location</b>	Identifies the mount point underneath which this location resides. Use the name of the mount point object that describes the mount point.
<b>Mount Point Path</b>	Specifies the mount point path. Valid values are: <ul style="list-style-type: none"><li>• <i>Existing</i>: Uses the current mount point path. Select <b>Null</b> to specify that the mount point is not shared, or select <b>share</b> to use this mount point as a shared mount point.</li><li>• <i>Create Mount Point Path</i>: Select to create a mount point path, then click <b>Select Path</b> to browse to a mount point on the file system.</li></ul>

Field	Value
<b>Path</b>	<p>Specifies the file system or UNC path.</p> <ul style="list-style-type: none"> <li>• <i>File System Path</i>: The location of the directory or file represented by the location object. The path syntax must be appropriate for the operating system of the server host. For example, if the server is on a Windows NT machine, the location must be expressed as a Windows NT path.</li> <li>• <i>UNC</i>: Indicates the UNC path.</li> </ul> <p> <b>Caution</b></p> <p>Be sure that the combination of the mount point and path you specify does not point to the same physical location as any other file store. If two file stores use location objects that point to the same physical location, data loss may result.</p>
<b>Path Type</b>	Indicates whether the location points to a directory or file.
<b>Security Type</b>	<p>The security level for the directory or file. Valid values are:</p> <ul style="list-style-type: none"> <li>• publicopen</li> <li>• public</li> <li>• private</li> </ul> <p>If the security type is not set, the default value is the security level of the referencing object, such an associated storage object.</p>

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on creating or modifying locations.

## 21.2.16 Deleting storage areas, locations, mount points, and plug-ins

You must have system administrator or superuser privileges to delete a storage area.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on deleting storage areas.

## 21.2.17 Setting or updating a retention date or retention period

A Centera store or NetApp SnapLock store is retention-enabled when a default retention date is required for all objects saved to that store.

You can assign specific retention dates for content stored in a retention-enabled store. A retention date is the date to which the content file must be retained. If a retention date is defined for content in the storage system, the file cannot be removed from the repository until that date. For example, if you set the retention date for an object to February 15, 2011, the content cannot be removed until that date.

When a retention date is set for an object, it is set for all renditions associated with page 0 (zero) of the object. Documentum CM Server moves the selected object and all of its associated renditions to a retention-enabled storage area. If there are multiple retention-enabled storage areas in the repository, you must select the target storage area. To set a retention date, you must belong to the Webtop administrator role and have at least WRITE permission on the object, and the Centera or SnapLock store must be retention-enabled.

You can alternatively assign a *retention period* for content stored in a retention-enabled store. A retention period is the amount of time for which the content must be retained. If a retention period is defined, you cannot remove the file from the repository until that period has expired. For example, if the retention period is set to five years and the current date is January 1, 2007, the content file cannot be removed before January 1, 2012.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on setting or updating a retention period or retention date for a document or other repository object.

## 21.2.18 Supporting WORM for Data Domain and Isilon stores

Documentum CM Server uses the Write Once Read Many (WORM) functionality provided by Data Domain and Isilon stores for applying retention at the file system level. The WORM functionality is applicable only for dm\_filestore objects. The dm\_location object for Data Domain and Isilon have paths mounted as CIFS (Windows) or NFS (Linux) share locations. Retentions can be applied on the file system as follows:

- *Apply WORM automatically:* By default, the documents in the file share location are set to WORM with a default retention date as defined by the storage administrator. Only Isilon supports the default retention using SmartLock containers.
- *Control retention using retainers:* The retention date on the retainer object is applied to the files. If the maximum retention date given in the retainer is greater than the default retention date (if it exists), default retention date will be overridden. Only fixed retention is supported.

The files with retention and also enabled with WORM cannot be modified or deleted until the expiration of the retention date.

### 21.2.18.1 Enabling WORM

To enable WORM at the filestore:

1. Use the following DQL to set the status of filestore to WORM:

```
EXECUTE set_storage_state with store='<store_name>',worm=[true | false]
```

2. Set the native\_access attribute of dm\_filestore to <isilon> (for Isilon) or <datadomain> (for Data Domain) using the IAPI commands.

For example, to set to isilon, use the following command:

```
retrieve,c,dm_filestore where name = '<store_name>'  
set,c,l/native_access  
isilon  
save,c,l
```



**Note:** WORM and non-WORM data cannot be combined on same filestore because WORM feature cannot be applied automatically on existing content files. Instead, create new WORM store and migrate existing contents to new store using the RPC, MIGRATE\_CONTENT.

### 21.2.18.2 Configuring SmartLock containers in Isilon

You need to configure the SmartLock containers (WORM folder) with the default retention date in Isilon. Use the following command:

```
isi worm mkdir --path=<complete path for the new directory>  
-d=<default retention offset>
```

To view the WORM status of a file or directory, use the following command:

```
isi worm info --path=<complete path of the file or directory> --verbose
```

## 21.3 Assignment policies

Assignment policies are sets of rules that Foundation Java API-based applications apply to determine the correct file store or retention store for each new content file added to the repository. Assignment policies require Content Storage Services (CSS). Any client application built on Foundation Java API applies assignment policies automatically if CSS is enabled in the repository.

Assignment policies can only be applied to the SysObject type and its subtypes, and are represented in the repository by persistent objects. A particular object type can have only one associated assignment policy. When a new content file is added to the repository, the assignment policy engine determines whether the object type of the file has an active associated assignment policy. If there is no active assignment policy for the type, the assignment policy engine determines whether the supertype of the object has an active associated assignment policy. If there is an active assignment policy for the file type or a supertype, the system applies the policy and stores the file accordingly. If no policy is found or if none of the rules match in an applicable policy, the system uses the default algorithm to determine the correct storage area. If none of the rules match in the applicable assignment policy, the policy engine does *not* further search the type hierarchy.

Assignment policies consist of rules that define the criteria for storing content files in the correct storage area. There are two types of rules:

- Standard rules

Standard rules determine storage area based only on the object format and content size. Standard rules can have one to five criteria.

- Custom rules

Custom rules can be based on the values of any standard or custom SysObject property, provided those values are present before an object is saved. There are no restrictions on the number of conditions in a custom rule. The properties and values are specified using methods, such as `getString()`, `getInt()`, or `getRepeatingString()`. Custom rules follow the Java syntax for any conditional statements in the rule.

There is no syntactical difference between the two types of rules. During rule validation, a standard rule is translated into the same syntax used for custom rules.

Assignment policies are applied only to new content files, whether they are primary content files or renditions. Rules of an assignment policy are applied in the order in which they are listed within a policy. If a rule is met, the remaining rules are ignored. To match a rule, all conditions in the rule must be satisfied. An assignment policy is applied when

- A content file is first saved or imported into the repository.
- A new version of a document is created, because versioning creates a new content file.
- A document is checked out and checked in and a new version results, the policy is applied to the new version of the content file.
- An existing document is modified and saved as the same version of the document.

Assignment policies are not applied or enforced under the following conditions:

- An application sets the `a_storage_type` SysObject property.  
If `a_storage_type` is set by an application, assignment policies do not execute for any of the primary content pages (content added using a Setfile). OpenText Documentum CM client applications do not generally set this property.
- The application specifies the storage location for a secondary rendition during an addrendition call.  
If a storage location is already provided, the policy engine does not execute the policy for this particular secondary rendition.
- Assignment policies are not enabled.
- The properties of an existing documents are modified and saved the changes without checking out and versioning the document. The content is saved into its current storage location.
- The Foundation Java API policy engine is turned off.
- Assignment policies are enabled but a policy does not exist for an object type or for any of the types supertypes.
- A document does not satisfy any of the conditions in the applicable policy.
- The content is replicated (content associated with a replica object).
- The content is loaded into a repository with dump and load.
- The content generated by a refresh API.
- The content is associated with storage policies.

If the assignment policy engine encounters an error in a rule at runtime (for example, if a property name is invalid), the assignment policy engine returns an error and the save operation on the document or object fails. This behavior can be overridden by setting the Foundation Java API client-preference flag in the `dfc.properties` file on the application server host where Documentum Webtop or Documentum Administrator is installed:

```
dfc.storagepolicy.ignore.rule.errors=true
```

If this flag is set to `true`, the assignment policy engine ignores the faulty rule and attempts to apply the next rule in the policy.

### 21.3.1 Viewing a list of assignment policies

You can view a list of all assignment policies defined for a particular repository and select any of the listed policies for viewing or modifying properties.

The assignment policy list page displays a list of all assignment policies in the current repository.

The following information is displayed for each policy:

- Policy name
- A brief description of the policy
- Whether the policy is currently Active or Inactive
- The object types to which the policy applies

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing a list of assignment policies in a repository.

### 21.3.2 Creating, viewing, or modifying assignment policies

To create an assignment policy, you must have the role of Administrator or, if there are no Administrators in the repository, the user privilege level of system administrator or superuser. Policies can only be created in repositories with Content Storage Services.

**Table 21-21: Assignment policy properties**

Field	Description
<b>Name</b>	The name and a description for the assignment policy. The name must be unique in the repository and can be modified after the policy is saved.
<b>Description</b>	A description of the policy. Optional property.
<b>Status</b>	Specifies whether the assignment policy is active. The default status is <b>Inactive</b> . Select <b>Active</b> to enable the policy and automatically validate the rule syntax. The validation process does not check whether property names in the rules are valid.

Field	Description
<b>Validate all of the rules defined for this policy</b>	<p>Validates the rules for the policy if the policy is active. The default is selected. If the policy is created in the active state, the checkbox is selected and grayed out.</p> <p>If the policy is created in the inactive state, optionally clear the checkbox.</p>
<b>Object types</b>	<p>Select the object types to which the policy applies.</p> <p>A policy can be applied to multiple object types. If the chosen object type has subtypes, the policy is inherited automatically at runtime by the subtypes, except those subtypes that are already associated with a different assignment policy.</p> <p>Click <b>Select</b> then select the object types to which the policy applies and click <b>&gt;</b>.</p>
<b>Create/Edit Rules</b>	Specifies the rules for storing content.
<b>Standard Rule</b>	<p>The Standard Rule option is selected by default. To create a custom rule, select the Custom Rule option.</p> <p>A policy can have up to five rules, which can be any combination of standard and custom rules. Each rule can have up to five criteria.</p> <p>Create or edit rules using the If and Then operands and drop-down lists to specify formats, content size, and storage areas.</p>
<b>Add Criteria</b>	<p>Click to add additional conditions to the rule.</p> <p>A standard rule can have up to five criteria.</p>
<b>Insert Rule</b>	Click to insert the completed rule.
<b>Cancel Rule</b>	Click to delete text that has been entered in the text box.
<b>Custom Rule</b>	Type the custom rule in the text box.
<b>Policy Rules</b>	Displays the existing rules defined for this policy. Click a rule to select it, then rearrange the order in which the rules are executed by clicking the <b>Up</b> and <b>Down</b> links. Edit or delete a rule by clicking the associated <b>Edit</b> and <b>Remove</b> links.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying assignment policies.

### 21.3.3 Modifying the permissions of an assignment policy

You can modify the permissions of an assignment policy. An assignment policy permission set must grant at least READ permissions to World.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on modifying assignment policy permissions.

### 21.3.4 Custom assignment policy rule examples

Custom rules define assignment policies based on values of properties of an object. Specify these properties in the rule using the methods available on IDfSysObject of Foundation Java API, such as `getString()`, `getInt()`, or `getRepeatingString()`.

Custom rules follow Java syntax for the conditional statement in the rule. The following are examples of valid custom rules:

 **Example 21-1: Custom rules for assignment policies**

Example Rule 1:

```
sysObj.getString("owner_name").equals("JSmith") --> filestore_02
```

Example Rule 2:

```
sysObj.getString("subject").equals("Policies and Procedures") &&  
sysObj.getOwnerName().equals("JSmith") --> filestore_03
```

Example Rule 3:

```
sysObj.getString("subject").equals("smith") &&  
sysObj.getOwnerName().equals("john") --> filestore_03
```

 Note that --> is the correct and required syntax.

For assistance in creating, implementing, or debugging custom rules, contact OpenText Global Technical Services for service and support options to meet your customization needs.

### 21.3.5 Associating an assignment policy with an object type

Assignment policies are inherited and only one policy can be associated with an object type.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on associating assignment policies with object types.

### 21.3.6 Deleting assignment policies

You can delete assignment policies.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting assignment policies.

## 21.4 Migration policies

Migration policies move content files from one storage area to another, based on the rules (conditions) defined in the policy. Files are selected for migration based on format, content size, or date criteria. The target storage area of a migration policy can be a file store or a retention store (Centera or NetApp SnapLock).

Migration policies are jobs that execute the MIGRATE\_CONTENT administration method. The conditions are stored as job arguments. Content Storage Services is required to create content migration jobs.

### 21.4.1 Creating, viewing, or modifying migration policies

Migration policies can be created and used only in repositories with Content Storage Services.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying migration policies.

**Table 21-22: Migration policy info tab properties**

Field	Description
Name	The name of the job. Mandatory property.
Job Type	The type of job. Optional property. The default value is <b>Content</b> .
Trace Level	The trace level from 0 (no tracing) to 10 (a debugging level of tracing).

Field	Description
<b>Designated Server</b>	The server on which the migration policy is run. Select a server from the drop-down list. The list displays each registered servers. The default value is <b>Any Running Server</b> .
<b>State</b>	Specifies whether the policy is active or inactive. The default value is <b>Active</b> .
<b>Options</b>	
<b>Deactivate on Failure</b>	Select to deactivate the job after a run fails to execute correctly.
<b>Run after Update</b>	Select to run the job immediately after it was updated.
<b>Save if Invalid</b>	Select to save the job even if it is invalid.

#### 21.4.1.1 Configuring a migration policy schedule

The migration policy schedule determines when the migration job is executed.

**Table 21-23: Migration policy schedule tab properties**

Field	Description
<b>Next Run Date and Time</b>	Specifies the next start date and time for the job. The default is the current date and time.
<b>Repeat</b>	Specifies the time interval in which the job is repeated.
<b>Frequency</b>	Specifies how many times the job is repeated. For example, if Repeat is set to Weeks and Frequency is set to 1, the job repeats every week. If Repeat is set to weeks and Frequency is set to 3, the job repeats every three weeks.
<b>End Date and Time</b>	Specifies the end date and time for the job. The default end date is 10 years from the current date and time.
<b>After</b>	Specifies the number of invocations after which the job becomes inactive.

### 21.4.1.2 Configuring migration policy rules

Rules can be standard rules, created by making choices from drop-down lists, or they can be custom rules, which use DQL predicates. Custom rules can select content to be migrated only from dm\_sysobject and dmr\_content objects. SysObject subtypes are not supported.

**Table 21-24: Migration policy rules tab properties**

Field	Description
<b>Selected Objects</b>	
<b>Simple selection</b>	Creates a migration rule based on preset values, such as format, creation date, modification date, access date, or size.
<b>Move objects where</b>	<p>Specifies which objects to move. Select one of the criteria from the drop-down list, as follows:</p> <ul style="list-style-type: none"> <li>• <b>format:</b> Migrates objects of a particular format. Click <b>Select</b> and then select the correct format.</li> <li>• <b>created:</b> Migrates objects according to creation date.</li> <li>• <b>modified:</b> Migrates objects according to their modification date.</li> <li>• <b>accessed:</b> Migrates objects according to the date they were last accessed.</li> <li>• <b>size:</b> Migrates objects according to their size in bytes. Enter the number of bytes.</li> </ul> <p>For the created, modified and accessed operands, the number of days is always in relation to the date the job is scheduled to run. Valid operands are:</p> <ul style="list-style-type: none"> <li>• <b>Exactly:</b> Migrates objects modified exactly the number of days before.</li> <li>• <b>More than:</b> Migrates objects modified more than the number of days before.</li> <li>• <b>Less than:</b> Migrates objects modified less than the number of days before.</li> </ul>
<b>Renditions to include</b>	Specifies whether to migrate <b>Primary</b> or <b>Secondary</b> renditions or both. The rendition option is only available in conjunction with the created, modified, or accessed selection criteria.

Field	Description
<b>DQL query selection</b>	Creates a migration rule based on a DQL query. Custom rules can select content to be migrated from dm_sysobject, its subtypes, and dmr_content objects.
<b>Move specified type</b>	Select to migrate the content associated with SysObjects (dm_sysobject) and its subtypes. When selected, you must also select to migrate primary or secondary renditions, or both.
<b>Move content objects only</b>	Select to migrate the content associated with content objects (dmr_content).
<b>Where</b>	Type a rule into the text box. Specify a DQL predicate and whether the predicate runs against content associated with SysObjects, its subtypes, or content objects.
<b>Renditions to include</b>	If you selected <b>Move specified types</b> , select to migrate <b>Primary</b> or <b>Secondary</b> renditions or both.
<b>Move options</b>	
<b>Target Store</b>	The destination storage area to which the content files migrate. Select a store from the drop-down list. The list includes file stores and retention stores (Centera and NetApp SnapLock).
<b>Batch Size</b>	The number of content files to include in a single transaction during the migration operation. The default value is 500.
<b>Maximum Count</b>	The maximum number of content files to transfer. To specify an unlimited number of documents, type a zero [0] or leave the field blank.
<b>Content Migration Threads</b>	<p>The number of internal sessions to use to execute the migration policy. The default value is 0, indicating that migration executes sequentially.</p> <p>This field displays only if you have Content Storage Services on Documentum CM Server. The Content Migration Threads value cannot exceed the Maximum Content Migration Threads value in the server configuration object (dm_server_config).</p>

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating, viewing, or modifying migration policies.

## 21.4.2 Configuring migration policy SysObject information

The SysObject information typically consists of metadata associated with the object.

**Table 21-25: Migration policy SysObject tab properties**

Field	Description
Title	The title of the object.
Subject	The subject of the object.
Keywords	Keywords that describe the object. Click <b>Edit</b> to access the Keywords page. Enter a new keyword in the <b>Enter new value</b> box and click <b>Add</b> .
Authors	The author of the object. Click <b>Edit</b> to access the Authors page. Type a new author in the <b>Enter new value</b> box and click <b>Add</b> .
Owner Name	The owner of the object. Click <b>Edit</b> to access the Choose a user page and select an owner.
Show more	Click to view more SysObject properties of the migration policy.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on configuring migration policy SysObject information.

## 21.4.3 Viewing migration policy job reports

A job report contains information about the job, such as when the job was started and whether the job ran successfully.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on viewing migration policy job reports.

## 21.4.4 Deleting migration policies

You can delete migration policies.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting migration policies.

## 21.5 Orphaned content objects and files

Destroying a document or other object does not destroy any content files or content objects associated with that document. Therefore the orphaned files and content objects should be removed on a regular basis.

An orphaned content object is a content object that is not referenced by another object. Objects have a property called `i_contents_id` that contains the object ID of the content object representing their content. An orphaned content file is a content file that has no associated content object.

Documentum CM Server provides the following system administration tools for removing orphaned content objects and files:

- `dmclean`

The `dmclean` utility scans a repository and finds all orphaned content objects and, optionally, orphaned content files. It generates a script that removes these objects and files from the repository.

- `dmfilescan`

The `dmfilescan` utility scans a specified storage area (or all storage areas) and finds all orphaned content files. It generates a script that removes these files from the storage area. The `dmfilescan` should be used as a backup to `dmclean`.

- `dmextfilescan`

The `dmextfilescan` utility scans a specific S3 or S3-compatible stores for any content files that do not have associated content objects and generates a report.

There are multiple options to run the `dmclean` and `dmfilescan` utilities:

- Documentum Administrator
- System administration tools
- DQL EXECUTE statement
- An `IDfSession.apply()` method
- From the operating system prompt

Executing either utility through a DQL EXECUTE statement, an `IDfSession.apply` method, or the operating system prompt is a two-step process. First, the utility must be executed to generate a script, and the script is run to perform the actual operations. Executing the operation in two parts allows checking which objects and files are going to be deleted before the work is actually performed.



**Note:** Only the superuser can retrieve the path of the orphaned content objects. In general, the system prevents any user to get access to the user content that has been orphaned due to version or checkin of the objects.

## 21.5.1 dmclean utility

The dmclean utility can be run in Documentum Administrator, using the DQL EXECUTE statement, an IDfSession.apply method, or from the operating system prompt. The syntax varies slightly, depending on how the utility is executed. Running dmclean requires system administrator or superuser privileges.

By default, dmclean operates on content objects representing content stored in any type of storage area except external storage, Centera storage, and NetApp SnapLock storage. It also removes the associated content files from the storage areas. You can include an argument on the command line to include orphaned content objects representing files in Centera and NetApp SnapLock storage in its processing. If you include that argument, it handles the associated orphaned content according to the retention requirements set for the storage area and the particular content.

["Removing orphaned content from retention type storage areas" on page 528](#) contains more information.

The following table describes the arguments for the dmclean utility:

**Table 21-26: dmclean arguments**

Argument	Description
-no_note	Directs the utility not to remove annotations.
-no_acl	Directs the utility not to remove orphaned ACLs.
-no_content	Directs the utility not to remove orphaned content objects and files.
-no_wf_templates	Directs the utility not to remove orphaned SendToDistribution templates.
-include_ca_store	Directs the utility to include orphaned content objects representing files stored in Centera or NetApp SnapLock storage.  Note: This argument is not supported when dmclean is run through Documentum Administrator.
-clean_aborted_wf	Directs the utility to remove aborted dm_workflows and all related runtime objects.
-clean_deleted_lwso	Directs the utility to remove deleted lightweight SysObjects and their parents.
-clean_wf_method_exec_result	Directs utility to delete workflow method output for finished workflows.
-clean_content_in_parallel	Directs the utility to delete orphaned content objects running in parallel.

Argument	Description
-parallel_degree	Directs the utility to define the degree of parallelism. It is an integer type value and it cannot be a negative value.   <b>Note:</b> The default value of parallel_degree argument is 5.

If you need syntax help, enter the name of the utility with the -h argument at the operating system prompt. “[Running jobs](#)” on page 440 and “[Dmclean](#)” on page 372 contain information on running dmclean using Documentum Administrator.

The executable that runs dmclean is launched by a method that is created when you install Documentum CM Server. By default, the dmclean executable is assumed to be in the same directory as the Documentum CM Server executable. If you moved the server executable, modify the method\_verb property of the method that launches dmclean to use a full path specification to reference the executable. You must be in the %DM\_HOME%\bin (\$DM\_HOME/bin) directory when you launch the dmclean executable.

### 21.5.1.1 Removing orphaned content from retention type storage areas

The dmclean utility does not operate on content stored in Centera or NetApp SnapLock storage areas by default. If you want to remove orphaned content files from these retention type storage areas, and their associated content objects, you must use run the dmclean utility from the command line and include the -include\_ca\_store argument.

Removing the content object and content file fails if the storage system does not allow deletions or if the content retention period has not expired. To find and remove the repository objects that have expired content, use the RemoveExpiredRetnObjects administration tool. Then use dmclean with the -include\_ca\_store argument to remove the resulting orphaned content files and content objects.

### 21.5.1.2 Running dmclean with an EXECUTE statement

To run dmclean with the EXECUTE statement, use the following syntax:

```
EXECUTE do_method
WITH method = 'dmclean',
arguments = '<list of constraining arguments>'
```

The dmclean utility can remove a variety of objects in addition to content files and content objects. These objects include orphaned annotations (note objects), orphaned ACLs, and unused SendToDistributed workflow templates. These objects are removed automatically unless you include an argument that constrains the utility not to remove them. For example, including -no\_note and -no\_acl arguments directs dmclean not to remove orphaned annotations and unused ACLs. If you include multiple constraints in the argument list, use a space as a separator.

The utility automatically saves the output to a document that is stored in the Temp cabinet. The utility ignores the SAVE argument in the DO\_METHOD. The output is saved to a file even if this argument is set to FALSE. The output is a generated IAPI script that includes the informational messages generated by the utility.

### 21.5.1.3 Running dmclean from the operating system prompt

To run dmclean from the operating system prompt, use the following syntax:

```
dmclean -docbase_name <name> -init_file <init_file_name> [<list of constraining arguments>]
```

Where <name> is the name of the repository against which to run the utility and <init\_file\_name> is the name of the server.ini file for the server or repository. The name and init\_file\_name arguments are required.

As dmclean is executing, it sends its output to standard output. To save the output (the generated script) to a file, redirect the standard output to a file in the command line when you execute dmclean.

The dmclean utility can remove a variety of objects in addition to content files and content objects. These objects include orphaned annotations (note objects), orphaned ACLs, and unused SendToDistributed workflow templates. These objects are removed automatically unless you include an argument that constrains the utility not to remove them. For example, including -no\_note and -no\_acl arguments directs dmclean not to remove orphaned annotations and unused ACLs. If you include multiple constraints in the argument list, use a space as a separator.

### 21.5.2 dmfilescan utility

The dmfilescan utility locates content files that have no associated content object. By default, the utility looks for all orphaned files that are older than one week. The utility ignores content files that have a content object. The dmfilescan utility ignores the content file if it has a content object in the repository if it has an associated content object, even if the content object is not referenced by other objects. Executing the utility generates a script that contains commands to remove the orphaned files found by the utility. The utility does not actually remove the files itself. After the utility completes, run the script to remove the files.

The dmfilescan utility should be used as a backup to the dmclean utility. It can be executed in Documentum Administrator, using the DQL EXECUTE statement, an IDfSession.apply() method, or from the operating system prompt. On Windows, the utility generates a batch file (a .bat script). On Linux, the utility generates a Bourne shell script. The executing syntax and the destination of the output vary, depending on how the utility is executed.

The executable that runs dmfilescan is launched by a method that is created during Documentum CM Server installation. By default, Documentum CM Server looks for the dmfilescan executable in the same directory the Documentum CM Server executable is stored. If you moved the server executable, modify the method\_verb property of the method that launches dmfilescan to use a full path specification to

reference the executable. You must be in the %DM\_HOME%\bin (\$DM\_HOME/bin) directory when you launch the dmfilescan executable.

[“Running jobs” on page 440](#) and [“Dmfilescan” on page 375](#) contain the information on running dmfilescan in Documentum Administrator.

The following table describes the dmfilescan arguments:

**Table 21-27: dmfilescan utility arguments**

Argument	Meaning
-s storage_area_name	The name of the storage object that represents the storage area to clean. If this argument is not specified, the utility operates on all storage areas in the repository, except far stores.
-from directory1	Subdirectory in the storage area at which to begin scanning. The value is a hexadecimal representation of the repository ID used for subdirectories of a storage area.  The utility starts at the specified directory and scans the specified directory and all its subdirectories or to the directory specified in the -to directory2 argument.
-to directory2	Subdirectory in the storage area at which to end scanning. The value is a hexadecimal representation of the repository ID used for subdirectories of a storage area.  The utility starts at the top directory or the directory specified in the -from directory1 argument.
-force_delete	Removes content files that are younger than 24 hours. If the -force_delete argument is not included, content files younger than 24 hours are not removed.
-no_index_creation	Prevents Documentum CM Server from creating indexes. If the -no_index_creation argument is not included, Documentum CM Server uses the default behavior for creating indexes.
-grace_period	An integer that defines the grace period for allowing orphaned content files to remain in the repository. The default is one week, expressed in hours. The integer value for this argument is interpreted as hours.

### 21.5.2.1 Running dmfilescan using an EXECUTE statement

To run dmfilescan with the EXECUTE statement, use the following syntax:

```
EXECUTE do_method WITH method = 'dmfilescan',
[arguments = '[-s<storage_area_name>] [-from <directory1>]
[,-to <directory2>]'
```

The utility automatically saves the output to a document that is stored in the Temp cabinet. The utility ignores the SAVE argument of the do\_method. The output is saved to a file even if this argument is set to FALSE. The output is a generated script that includes the informational messages generated by the utility.

### 21.5.2.2 Running dmfilescan from the operating system prompt

To run the utility from the operating system, use the following syntax:

```
dmfilescan -docbase_name <name> -init_file <init_file_name>
[-s <storage_area_name>] [-from <directory1>] [-to <directory2>]
```

The dmfilescan utility sends the output to standard output. To save the generated script to a file, redirect the standard output to a file on the command line when you run the utility.

The two arguments, -docbase\_name and -init\_file, are required, where name is the name of the repository that contains the storage area or areas to clean and init\_file\_name is the name of Documentum CM Server server.ini file.

### 21.5.2.3 generated script

Executing dmfilescan generates a script. The script comprises a series of remove commands that remove orphaned files found by the utility. For each file, the script lists its data ticket and storage ID. The script also contains a template DQL SELECT statement that can be used with the data ticket and storage ID values.

The following example describes a script that was generated on a Windows host:

```
rem Documentum, Inc.
rem
rem This script is generated by dmfilescan for later verification
rem and/or clean-up. This script is in trace mode by default. To
rem turn off trace mode, remove '-x' in the first line.
rem
rem To see if there are any content objects referencing a this file
rem listed below, use the following query in IDQL:
rem
rem c:> idql <docbase> -U<user> -P<pwd>
rem 1> select r_object_id from dmr_content
rem 2> where storage_id = '<storage_id>' and data_ticket =
<data_ticket>
rem 3> go
rem
rem If there are no rows returned, then this is an orphan file.
rem
rem storage_id = '280003c980000100' and data_ticket = -2147482481
del \dm\dmadmin\data\testora\content_storage_01\000003c9\80\00\04\8f
rem storage_id = '280003c980000100' and data_ticket = -2147482421
del \dm\dmadmin\data\testora\content_storage_01\000003c9\80\00\04\cb
rem storage_id = '280003c980000100' and data_ticket = -2147482211
```

```
del \dm\dmadmin\data\testora\content_storage_01\000003c9\80\00\05\9d  
.
```

#### 21.5.2.4 Executing the dmfilescan script

Run the dmfilescan script from the operating system prompt.

On Windows:

```
c:> <script_file_name>
```

On Linux:

```
% <script_file_name>
```

Make sure that you have the user permission to execute this file. On Windows, use File Manager to add appropriate permission to your user account. On Linux, use the following command:

```
% chmod ugo+x <script_file_name>
```

#### 21.5.3 dmextfilescan utility

The following table describes the dmextfilescan arguments:

**Table 21-28: dmextfilescan utility arguments**

Argument	Meaning
-docbase_name docbase name	Name of the repository.
-user user name	Name of the user to connect to the repository.
-password user password	Password of the user to connect to the repository.
-s target file store	The name of the S3 and S3-compatible store.
-from scan from directory1	Subdirectory in the storage area at which to begin scanning. The value is a hexadecimal representation of the repository ID used for subdirectories of a storage area.  The utility starts at the specified directory and scans the specified directory and all its subdirectories or to the directory specified in the -to directory2 argument.
-to scan upto directory2	Subdirectory in the storage area at which to end scanning. The value is a hexadecimal representation of the repository ID used for subdirectories of a storage area.  The utility starts at the top directory or the directory specified in the -from directory1 argument.

Argument	Meaning
-force_delete	Removes content files that are younger than 168 hours. If the -force_delete argument is not included, content files younger than 168 hours are not removed.
-grace_period	An integer that defines the grace period for allowing orphaned content files to remain in the repository. The default is one week, expressed in hours. The integer value for this argument is interpreted as hours.

### 21.5.3.1 Running dmextfilescan from the operating system prompt

To run the utility from Linux, use the following syntax:

```
java -cp "$DOCUMENTUM/dfc/*:$DOCUMENTUM/config:$DM_HOME/bin/dmextfilescan.jar" App - docbase_name <docbase> -user <user> -password <password> [-s <filestore>][-from <dir1>][-to <dir2>] [-force_delete][-grace_period <hours>]
```



**Note:** Use a semicolon instead of colon in the preceding syntax as a separator for Windows.

The dmextfilescan utility sends the progress to standard output and generates a report named `DMExtFilescanDoc.txt` at the `$DOCUMENTUM/dba/log/<repository ID>/sysadmin/` location.

## 21.6 Archiving and restoring documents

As repositories grow and age, you typically archive older or infrequently accessed documents to free up disk space for newer or more frequently used documents. There will also be occasions when you want to restore an archived document. OpenText Documentum CM provides a mechanism for archiving and restoring documents using the Archive and Restore methods and the Archive tool.



**Note:** If you want to archive fixed data such as email or check images that will not be changed and must be retained for a fixed period, use the content-addressed storage option, rather than the archiving capabilities described in this section. The content-addressed storage option is capable of storing massive amounts of data with a defined retention period.

## 21.6.1 How the process works

Five major components are involved in archive and restore functionality:

- The client requesting the operation
- The repository operator's inbox, where the requests are queued
- The Archive tool, which performs the actual operations
- The archive directory, a staging area for the dump files created by the archiving operations and read by the restoring operation
- The offline storage area, where archived files are moved for permanent storage

**When you archive a document, these components interact as follows:**

1. The client sends an archive request.  
The client can be a user selecting a custom menu item requesting archiving (which issues an Archive method) or an application issuing the Archive method.
2. The Archive method queues a DM\_ARCHIVE event in the repository operator's inbox.
3. The Archive tool reads the DM\_ARCHIVE event in the inbox and performs the archiving operation.  
When the tool is finished, it sends a completion message to the user requesting the operation and to the repository operator.
4. A user-defined DO\_METHOD procedure moves the file from the archive directory to permanent, offline storage.

**When you restore a document, these components interact as follows:**

1. The client sends a restore request.  
The client can be a user trying to open an archived document using a OpenText Documentum CM client or an application issuing the Restore method.
2. The Restore method queues a DM\_RESTORE event to the repository operator's inbox.
3. The Archive tool reads the DM\_RESTORE event in the inbox.
4. If necessary the server calls a DO\_METHOD function that moves the dump file containing the archived file back into the archive directory.
5. After the file is back in the archive directory, the Archive tool performs the restore operation.

When the tool is finished, it sends a completion message to the user requesting the operation and to the repository operator.

## Chapter 22

# InfoArchive integration with OpenText Documentum CM

InfoArchive, an enterprise archiving system for long-term or permanent preservation is designed to help address the complete information retention needs and achieve regulatory compliance.

The existing InfoArchive integration with OpenText Documentum CM uses separate standalone command line utilities such as OpenText Documentum CM Connector and InfoArchive where OpenText Documentum CM Connector is a command line data extraction and transformation utility that allows you to export content to archive it directly from the repository and generate Submission Information Packages (SIPs) to be ingested into InfoArchive. OpenText Documentum CM Connector executes a DQL query statement defined in a configuration file and extracts the persistent objects from the repository. InfoArchive utility allows you to ingest SIPs into the respective InfoArchive server.

The new OpenText Documentum CM Connector DAR file named `DCTM2IA.dar`:

- Helps to automate or schedule job archival
- Provides control to delete OpenText Documentum CM content after successful archiving

The new OpenText Documentum CM-triggered archival provides flexibility of running archival from any of the Foundation Java API-based clients such as OpenText™ Documentum™ Content Management client, xCP, and WDK or in Documentum CM Server Java Method Server as job or methods.

## 22.1 Prerequisites

You must have installed the following:

- Documentum CM Server
- Documentum Administrator
- InfoArchive server

## 22.2 Setting up OpenText Documentum CM connector

1. As part of the Documentum CM Server and internal DAR files installation, the new connector DAR file named DCTM2IA.dar is also installed. The connector DAR file is available at %DM\_HOME%\install\DARsInternal.

The dars.txt located at %DM\_HOME%\dba\config\db91\ provides the installation completion status information of all the internal DAR files.

2. Navigate to \$DM\_JMS\_HOME\webapps\dmMethods\WEB-INF\classes. This location contains the following sample properties files:
  - sample\_configuration\_Documentum.yml
  - sample\_eas\_documentum.extractor.properties
  - sample\_connection.properties
3. Take a copy of the sample\_configuration\_Documentum.yml file and rename the file as configuration\_Documentum.yml.
4. Open the configuration\_Documentum.yml file and provide the appropriate values for the variables as described in the following table:

Category	Name	Description
tenant	name	Specifies the name of the target application. For example, INFOARCHIVE.
	configure	The default value is use existing.
application	name	Specifies the name of the source application. For example, Documentum.
	configure	The default value is use existing.
holding	name	Specifies the name of the application where the data that needs to be migrated exists. For example, Documentum.
	configure	The default value is use existing.

5. Take a copy of the sample\_eas\_documentum.extractor.properties file and rename the file as eas\_documentum.extractor.properties.
6. Open the eas\_documentum.extractor.properties file and provide the appropriate values for the variables as described in the following table:

Name	Description
docbase	Specifies the name of the repository. The rest of the OpenText Documentum CM connection parameters must be specified in <code>dfc.properties</code> available in the <code>CLASSPATH</code> variable.
producer	Specifies the application that generates the SIP.
password	<p>Specifies the password to log in to the repository. <i>InfoArchive 4.3 Documentum Connector Guide</i> contains more information about password protection and encrypted password.</p> <p>By default, applications running on the Documentum CM Server host are allowed to make repository connections as the installation owner without a password. This is called a trusted login.</p> <p>If you use the installation owner account, and run the connector on your Documentum CM Server host, leave this field blank.</p>
sipXslt	Specifies the path to an XSL file to be applied to each SIP file.
pdicontentschema	Specifies the content schema that is written to Preservation Description Information (PDI) files.
extractTypes	<p>Specifies the object type information that must be extracted.</p> <p>If the objects belong to multiple object types (a subtype with its supertypes; for example, <code>dm_document</code> and <code>dm_sysobject</code>), all these types are extracted.</p> <p>When extracted, the object type information is stored in the <code>types</code> element in <code>element</code> in <code>eas_pdi.xml</code> as part of the generated SIP.</p> <p>The default value is <code>true</code>.</p>
username	Specifies the user name to log in to the repository.
holding	Specifies the name of the application where the data that needs to be migrated exists. For example, Documentum.
sipXsd	Specifies the XSD file for verifying each of the generated SIP file.

Name	Description
workingdir	<p>Specifies the complete path of the working directory in which to generate SIPs. If the directory does not exist, the utility creates it when executed. For example:</p> <pre>workingdir=C:\\Documentum\\IA</pre> <p> <b>Note:</b> Use the double backward slashes (\ \ ) as the delimiter in the path.</p>
xsdFileValidation	<p>Specify the path of XSD schema file, for example /Path/DctmDocbase.xsd (default schema) as the schema (.xsd) file against which the PDI file generated by the utility is validated.</p> <p>Validation is not done if you do not set a value for this parameter. If you use the XSL transformation to transform PDI files to your own schema, you can specify this schema to validate the result of the XSL transformation.</p>
maxCiSizePerSip	Specifies the maximum size in bytes for content files per SIP.
checksum_algorithm	Specifies the algorithm for calculating the hash value. The valid algorithms are MD5, SHA-1, or SHA-256. The default value is SHA-1.
application	Specifies the OpenText Documentum CM application that contains the data to be migrated and archived.
archiveId	Specifies a string that is used to generate a unique archive ID for each SIP. This string may contain a pattern that is a combination of static text, date value pattern, and UUID part for generating ID. In the pattern, a DateTime value is applied and it uses the same date/time format as it is specified in the <code>java.lang.String#format</code> in the Java method. <i>Oracle documentation</i> contains more information.

Name	Description
extractRelations	<p>Specifies the relationship (represented by dm_relation_type and dm_relation objects) information associated with selected objects, that must be extracted.</p> <p>Specifies to extract information of relationship (represented by dm_relation_type and dm_relation objects) associated with the selected objects. When extracted, relationship information is stored in the relations element in eas_pdi.xml as part of the generated SIP. The default value is true.</p>
entity	Specifies the application name that holds the migrated and archived data.
extractContents	Specifies the information about the content files associated with the selected objects, that must be extracted. When extracted, the content file information is stored in the contents element in eas_pdi.xml as part of the generated SIP. The default value is true.
sipschema	Specifies the SIP schema that is written to the SIP descriptor file.
pdischema	Specifies the PDI schema that is written to the SIP files.
maxObjectsPerSip	Specifies the maximum number of objects in a SIP.
dqlPredicate	<p>Specifies the partial DQL query string after the FROM clause. The string you specify here is automatically appended to the preset string "select r_object_id from" to form the complete DQL query statement when you execute the utility.</p> <p>For example, if you set dqlPredicate as follows:</p> <pre>dm_document where object_name like 'ABCD1%'</pre> <p>The complete DQL query statement that is constructed and executed is:</p> <pre>select * from dm_document where object_name like 'ABCD1%'</pre> <p>Only objects retuned by the query statement are extracted for archiving.</p>

Name	Description
enableLargeXMLprocessing	(Optional) Specifies that large XML files must be processed. If you set the value to true, it splits the large XML files in to chunks. The default value is false.
maxTablesPerSIP	Specifies the maximum number of registered table objects per SIP.
xslt	Specifies the path to the XSLT file.
includePDIHashInSIP	Specifies that a hash value of each PDI file is written to a SIP when set to true.
extractFolders	Specifies that the information about the folder (and from all the parent folders of the folder, if any) of the selected objects, must be extracted. When extracted, the folder information is nested in the folders element in eas_pdi.xml as part of the generated SIP. The default value is false.
extractACLs	Specifies that ACLs must be extracted. The default value is false.
priority	Specifies the ingestion priority of the SIP. The greater the value, the higher the priority.  The order in which SIPs are ingested is determined first by ingestion priority (higher-priority SIPs are ingested first, and then by ingestion deadline date (SIPs with earlier deadlines are ingested first).
extractContainments	Specifies the virtual documents must be extracted. The default value is true.
registeredTables	Specifies the DQL query parts after the FROM clause related to the registered tables that must be extracted.
shouldDeleteDCTMObjects	Specifies if the objects or data that is migrated and archived in InfoArchive must be deleted. The default value is false.
isDebugEnabled	Specifies if the debug mode is enabled. The default value is true and it retains the ZIP file that contains the SIP file contents in the working directory. If you do want to retain the ZIP file that contains the SIP file contents, set the value to false.

7. Take a copy of the sample\_connection.properties file and rename the file as connection.properties.

8. Open the `connection.properties` file and provide the appropriate values for the variables as described in the following table:

Name	Description
<code>ia.server.uri</code>	Specifies the URL of InfoArchive services.
<code>ia.server.authentication.gateway</code>	Specifies the IP address of the authentication gateway.
<code>ia.server.authentication.user</code>	Specifies the email ID of the user that must be authenticated.
<code>ia.server.authentication.password</code>	Specifies the password of the user that must be used for authentication.
<code>ia.server.client_id</code>	Specifies the client ID.
<code>ia.server.client_secret</code>	Specifies the encrypted information of the client.

## 22.3 Running archive job using Documentum Administrator

Log in to Documentum Administrator and perform the following steps:

1. Create a job.
2. Assign the `dm_InfoArchive_Java` method to the job.
3. Select the **pass standard argument** option.
4. Run the job.
5. Check the `server.log` file of Method Server for information about logs.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains detailed information.

The job migrates and archives the OpenText Documentum CM application data to InfoArchive.



**Note:** If you want to run the jobs in parallel, perform the following steps:

1. Create another copy of `eas_documentum.extractor.properties` and provide a unique name.
2. Provide appropriate values for all variables.
3. Log in to Documentum Administrator, create a job and then assign the `dm_InfoArchive_Java` method to the job (make sure that the **pass standard argument** option is selected).

4. Assign the argument using the `-file_name <name of the new properties file>` command.
5. Run the job.

## 22.4 Cleaning archived objects

All archived objects have the `iaaspect` aspect attached to them. This aspect also contains attributes to identify the InfoArchive server where the content is archived, the user, and the time of ingestion and so on. You can write a new job or method to search and clean the archived objects, as applicable.

# Chapter 23

## Content delivery

### 23.1 Content delivery services

Documentum Interactive Delivery Services (IDS) and Documentum Interactive Delivery Services Accelerated (IDSx) enable publishing and delivery of content directly from a repository to a website. Any content can be published and updated as documents are revised in the repository. Document versions and formats to publish can also be specified. Publication can occur on demand or automatically on a schedule.

IDS and IDSx offer the following capabilities:

- Replication of content and metadata that is published on an IDSx staging target to multiple replication targets. The replication process can occur through Documentum CM Server jobs or on demand.
- Bi-directional content delivery (publish/replicate) to a target and pulling content back to the repository. This process is known as Ingestion.

For publishing, IDSx must be installed on the computer where the repository is hosted (the source machine) and on the website host (the target machine). For replication, the IDSx target software must be installed on all the replication targets. IDSx uses accelerated data transfer technology for faster file transfer.

*OpenText Documentum Interactive Delivery Services Accelerated Installation Guide* and *OpenText Documentum Interactive Delivery Services Accelerated User Guide* provides additional information about Interactive Delivery Services Accelerated (IDSx).

*OpenText Documentum Interactive Delivery Services Installation Guide* and *OpenText Documentum Interactive Delivery Services User Guide* provides additional information about Interactive Delivery Services (IDS).

### 23.2 Locating content delivery configurations

You can locate the correct content delivery configuration.

**Table 23-1: Content delivery configuration information**

Field	Description
Initial Publishing Date	The date documents were first published using this configuration.
Refresh Date	The date of the last successful full refresh of the content delivery configuration.

Field	Description
<b>Last Increment Date</b>	The date of the last successful incremental publish event for the content delivery configuration.
<b>Increment Count</b>	The number of successful incremental updates since the initial publish operation or last full refresh.
<b>Publishing Status</b>	Indicates whether the last publishing event succeeded or failed.
<b>Event Number</b>	Unique number generated internally for each publishing operation.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on locating content delivery configurations.

### 23.3 Creating or modifying content delivery configurations

You can create content delivery configurations. You must have superuser privileges to create or modify a content delivery configuration. The user authentication is mandatory in IDSx. All fields required for publishing are on the Info tab of the Content Delivery Configuration page.

**Table 23-2: Content delivery properties**

Field	Value
<b>Info</b>	
<b>State</b>	Select <b>Active</b> to indicate using this content delivery configuration is active. The default state is Active.  Select <b>Inactive</b> to deactivate the configuration.
<b>Configuration Name</b>	Identifies the publishing configuration. The name appears in the list of existing configurations and the name of log files applying to the configuration.
<b>Publishing Folder</b>	The root repository folder from which you are publishing. The root folder and all subfolders are published.  If you change this setting after the initial publication, you must re-publish the configuration using the Full Refresh option.

Field	Value
<b>Version</b>	Defines which version of the document to publish. If unspecified, the default is the CURRENT version.  If you change this setting after you publish the configuration initially, you must republish the configuration using the Full Refresh option. If you specify a symbolic label, the case must match the label case in the repository. To allow documents with different version labels to be published, specify ANY VERSION.
<b>Target Host Name</b>	Identifies the target host machine to which documents are published. This is the target host, a host where the Interactive Delivery Services (IDS) target software is installed.
<b>Target Port</b>	The port number of the host machine of website to use for connections. This must be the port designated when the target software was installed.
<b>Target UDP Port</b>	Type the UDP port on the target host which is used for accelerated file transfer. Use unique UDP port for each IDSx configurations, irrespective of using the same or a different IDSx target.  <i>Note:</i> The Target UDP Port option is available only in IDSx.
<b>Connection Type</b>	Can be <b>Secure</b> or <b>Non-secure</b> . This is the type of connection used for connections from the source host to the target host. The default is <b>Secure</b> .
<b>Target Root Directory</b>	The physical directory on the target host where the transfer agent places the export data set for publication. Also known as the webroot.  If you change this setting after the initial publishing event for the configuration, you must re-publish the configuration using the Full Refresh option.  <b>CAUTION:</b> During initial publication or a full refresh, the contents of the target root directory are deleted. Make sure that you designate the correct directory as the target root directory.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on creating or modifying content delivery configurations.

## 23.4 Configuring the advanced properties of a content delivery configuration

Use the properties described in the [Advanced properties for content delivery](#) table to configure the advanced properties of a content delivery configuration.

**Table 23-3: Advanced properties for content delivery**

Field	Value
<b>Property Export Settings</b>	
<b>Add properties as HTML Meta Tags</b>	If selected, the system inserts document properties into HTML content files as META tags on the target host.  If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.
<b>Export Properties</b>	If selected, the system exports a default set of properties for each published document.  If this setting changes after the initial publishing event for the configuration, republish using the Full Refresh option.
<b>Include contentless properties</b>	If selected, documents in the publishing folder that without an associated content file are published. Only the properties associated with the contentless document are published.  By default, this option is not selected and is enabled only if <b>Export Properties</b> is also selected.
<b>Include folder properties</b>	If selected, folder properties are published to the website. This option is enabled only if <b>Include contentless properties</b> is also selected.
<b>Additional Properties</b>	Identifies additional properties to export to repository on target host. If <b>Export Properties</b> is selected, IDS exports a set of default properties for each published document.  If this setting changes after initial publishing event for the configuration, republish using the Full Refresh option.  Click <b>Select Attributes</b> to identify additional properties to export.

Field	Value
<b>Property Table Name</b>	The name to use when creating the database tables on the target host. Specify a table name if <b>Export Properties</b> is selected. The table name must not exceed 28 bytes.  If this setting changes after initially publishing the configuration, republish the configuration using the Full Refresh option.
<b>Content Selection Settings</b>	
<b>Formats</b>	The content formats to publish. If specified, only documents with the listed formats are published. If unspecified, all formats are published.  If this setting changes after publishing the configuration initially, republish the configuration using the Full Refresh option.
<b>Effective Label</b>	This field is used in conjunction with the <code>a_effective_label</code> document property to filter documents for publication. If Effective Label is specified, only documents with a matching <code>a_effective_label</code> value are examined as possible candidates for publication. If unspecified, all documents are examined as possible candidates.  If this setting changes after initially publishing the configuration, you must republish the configuration using the Full Refresh option.
<b>Miscellaneous Settings</b>	
<b>Export Directory</b>	The name of the local directory on the Documentum CM Server host where documents are placed after they are exported from the repository.  The default is a subdirectory of <code>\$DOCUMENTUM/share/temp</code> . When executing a publishing operation, the directory <code>\$DOCUMENTUM/share/temp/web_publish</code> is created.  On Windows, the length of the repository path to an object to publish, plus the length of the object name, plus the length of the export directory on the Documentum CM Server host is limited to 255 characters. There is no length limitation on Linux.
<b>Ingest Directory</b>	The name of the directory on the source where the documents are placed after being pulled from the target directory. The default is a subdirectory of <code>\$DOCUMENTUM/share/temp</code> . You can choose a different directory by clicking <b>Select Directory</b> .
<b>Trace Level</b>	Defines a tracing level for IDS operations. The trace levels correspond to the trace levels available using the Trace API methods. The default value is 0.

Field	Value
<b>Global Publishing Enabled</b>	Enables the global publishing feature of Web Publisher. Replaces the <code>global_publishing</code> extra argument that was added manually to the content delivery configuration in prior versions.
<b>Website Locale</b>	<p>Web Publisher only. Replaces the <code>global_locales</code> extra argument that was added manually to the content delivery configuration in prior versions.</p> <p>Select a locale from the drop-down list. If using Web Publisher and a document exists in more than one translation in the publishing folder, the locale code indicates which translation to publish and also points to the Web Publisher rules that define the second and subsequent choices of translation to publish.</p> <p>The drop-down list contains choices only when you are using Web Publisher and the publishing folder is configured for multilingual use.</p> <p>If you do not use Web Publisher or if your publishing folder is not configured for multilingual publishing, the drop-down list does not appear.</p>
<b>Web Server URL Prefix</b>	<p>This is the URL to the target root directory and is required if using Web Publisher.</p> <p>For example, if the target root directory is <code>d:\inetpub\wwwroot\webcache</code> and the website host is on a computer <code>host_name</code>, set the Web Server URL Prefix to <code>http://host_name/webcache</code>.</p> <p><i>Note:</i> <i>Web Server URL Prefix</i> is not applicable to replication targets.</p>
<b>Synchronization Settings</b>	
<b>Transfer is to live website</b>	<p>If selected, Interactive Delivery Services attempts to minimize user interruptions during publishing. Leave cleared if users do not have access to the site during publishing operations.</p> <p>If this setting changes after initial publication, republish the configuration using the Full Refresh option.</p>
<b>Online Synchronization Directory</b>	<p>The directory on the target host to be used as temporary storage for the backup copy of the Interactive Delivery Services repository during online updates. This must be specified if <b>Transfer is to live website</b> is selected.</p> <p>If this setting changes after you publish the configuration initially, republish the configuration using the Full Refresh option.</p>

Field	Value
<b>Pre-Synch Script on Target</b>	The name of a script, located in the product/bin directory of target host, to run before publishing takes place. If online synchronization is enabled, the script runs before online synchronization occurs. There is a 48-character limit for information typed into this field.
<b>Post-Synch Script on Target</b>	The name of a script located in the product/bin directory of target host to be run after publishing occurs. If online synchronization is enabled, the script runs after online synchronization takes place. There is a 48-character limit for information typed into this field.
<b>Ingest Settings</b>	
<b>Ingest</b>	Select this option if you want to ingest content from the target to the repository.
<b>Target Ingest Directory</b>	Enter the directory path of the target from where the content will be ingested.
<b>Transfer Authentication Settings</b>	
<b>Enable system authentication on target</b>	Select to require a transfer username and password for authentication. Not selected means the transfer username and password are not required for authentication before a data transfer occurs.
<b>User Name</b>	Identifies the user whose account will be used by the transfer agent to connect to the target host.
<b>Password</b>	The password for the user specified in <b>User Name</b> .
<b>Confirm Password</b>	Enter the password again for confirmation.
<b>Domain</b>	Identifies the domain of the user specified in <b>User Name</b> .

## 23.5 Configuring replication properties for a content delivery configuration

Use the properties described in the [content delivery replication properties](#) table to configure replication properties for a content delivery configuration.

**Table 23-4: Content delivery replication properties**

Field	Value
<b>Replication Target Host Settings</b>	

Field	Value
<b>State</b>	<p>You can select one of the following states:</p> <ul style="list-style-type: none"> <li>• <b>Active in-transaction:</b> Select this option if you want a replication target to participate in a transactional replication. This is the default value.</li> <li>• <b>Active not-in-transaction:</b> Select this option if you want the replication target to participate in a non transactional replication.</li> <li>• <b>Inactive:</b> Select this option if you want a replication target to go for system maintenance or out of commission.</li> </ul>
<b>Target Host Name</b>	<p>Identifies the target host machine to which documents are published. This is the replication target host, a host where the Interactive Delivery Services Accelerated (IDSx) target software is installed.</p>
<b>Target Port</b>	<p>The port number of the host machine of website to use for connections. This must be the port designated when the replication target software was installed.</p>
<b>Target UDP Port</b>	<p>The UDP port on the target host which is used for accelerated file transfer. Unique UDP port has to be used for every IDSx configurations, irrespective of using the same or different IDSx targets.</p>
<b>Connection Type</b>	<p>May be <b>Secure</b> or <b>Non-secure</b>. This is the type of connection used for connections from the source host to the target host. The default is <b>Secure</b>.</p>
<b>Target Root Directory</b>	<p>The physical directory on the target host where the transfer agent places the export data set for publication. Also known as the webroot.</p> <p>If you change this setting after the initial publishing event for the configuration, you must replicate the configuration again in order to synchronize the target root directory.</p>
<b>Export Properties</b>	<p>You can select this checkbox to export properties to the replication target.</p>
<b>Property Table Name</b>	<p>Type the target host property table name, which is required if you selected <b>Export Properties</b>.</p>

Field	Value
Ingest	Select this option if you want to ingest content from the replication target to the repository.
Target Ingest Directory	Enter the directory path of the source where the content will be stored.
<b>Transfer Authentication Settings</b>	
User Name	Enter the user name for the data transfer.
Password	Enter the password for the data transfer.
Domain	If the target host is on Windows, optionally type in a domain where the transfer user exists. If you type in a domain, it overrides domain information provided on the target host during installation.
addReplicationTarget	Adds multiple replication targets.

## 23.6 Configuring extra arguments for a content delivery configuration

You can configure extra arguments for a content delivery configuration using the properties described in the [extra arguments](#) table.

**Table 23-5: Extra arguments**

Key	Description	Default Value(s)
use_docbase_formats	Determines whether the default file format extensions set in the repository are used when files are published.  FALSE overrides the default file format extensions set in the repository. TRUE or no setting uses the extensions set in the repository format objects.	TRUE

Key	Description	Default Value(s)
use_text_file_extensions	When set to TRUE, text files that do not have a .txt extension in the object name are published with the .txt extension. For example, if a text file MyFile is published and the parameter is set to TRUE, the file is published as MyFile.txt. If the parameter is set to FALSE, the default value, the file is published as MyFile.	FALSE
agent_connection_timeout	The timeout interval in seconds for the IDS publish method connection to the target host. For example, to wait 90 seconds:  <code>agent_connection_timeout=90</code>  If the publishing operation takes longer, Documentum Administrator displays an error message and the publishing log files record that the publishing operation failed.	120
connect_thread_timeout	The timeout interval in seconds for the end-to-end tester connection to the target host. For example, to wait 90 seconds:  <code>connect_thread_timeout=90</code>	30
lock_sleep_interval	The number of seconds for which IDS waits for a webc lock object to be unlocked. For example, to wait 90 seconds:  <code>lock_sleep_interval=90</code>	10

Key	Description	Default Value(s)
lock_retry_count	<p>How many times IDS checks whether the webc lock object is unlocked. The value of this key multiplied by the value of lock_sleep_interval controls the total amount of time for which IDS waits to lock a configuration with a lock object.</p> <p>Since the default lock_sleep_interval value is 10 seconds, IDS retries for a total of 300 seconds (5 minutes) by default.</p>	30
disable_dctm_tag	Whether you want the Documentum META tag to appear when you use META tag merging.	TRUE
trace_passwords	Whether passwords appear in debug tracing output. FALSE causes passwords to be omitted from debug tracing output. TRUE causes passwords to be included in debug tracing output.	FALSE
error_threshold	The number of errors allowable on the source side during a single full-refresh, incremental, or force-refresh publishing operation.	0
max_cached_ssl_sockets	The number of cached SLL sockets between source and all targets that are retained for reuse. Does not restrict the maximum number of SLL sockets that can be open at one time. Used only in the scs_admin_config object in the IDS Administration sub-node.	30

Key	Description	Default Value(s)
publish_contentless_documents	<p>Whether documents can be published that do not have associated content files. TRUE causes publication of documents without associated content files. FALSE causes documents without associated content files not to be published.</p> <p> <b>Note:</b> This option can also be selected on the Advanced tab of the content delivery configuration.</p>	FALSE
publish_folder_properties	<p>Whether folder properties can be published. TRUE causes folder properties to be published. FALSE causes folder properties not to be published. If set to TRUE, requires that publish_contentless_documents is also set to TRUE.</p> <p> <b>Note:</b> This option can also be selected on the Advanced tab of the content delivery configuration.</p>	FALSE
compression	Whether file compression is enabled. TRUE causes files to be compressed. FALSE disables file compression.	TRUE
min_size_worth_compressing	The threshold in bytes beneath which compression of a particular file does not yield performance gains	5000
max_entries_per_zipfile	The number of files whose size is less than min_size_worth_compressing that are collected in a ZIP file for transfer to the target host.	128
extensions_to_compress	The file types to compress, by file extension.	html, jhtml, shtml, phtml, xhtml, htm, jht, sht, asp, jsp, xml, css, txt

Key	Description	Default Value(s)
publish_source_version_labels	When set to TRUE, all values of the r_version_label attribute are published to the repeating attribute table.	FALSE
mssql_store_varchar	SQL Server database only. When set to TRUE, string attributes are stored in the source catalog database and target database as varchar rather than nvarchar.  When set to true, you cannot publish multibyte data.	FALSE
store_log	Whether to store log files in the repository. Valid values are: <ul style="list-style-type: none"><li>• TRUE: The logs are stored in the repository.</li><li>• FALSE: The logs are not stored in the repository.</li></ul> The log is not stored in the repository for a single-item publishing operation when method_trace_level is set to 0.	TRUE
store_log_file	Determines whether publishing logs are deleted or retained on the source host. If the key is set to TRUE, publishing logs are preserved. If the key is set to FALSE, the trace level is less than 10; if the publishing operation succeeds, the log files are deleted.	
method_trace_level	The level of tracing output. 0 is the lowest level of tracing and 10 is the highest level of tracing.   <b>Note:</b> To get LDAPSync debug information, use method_trace_level 8. To get verbose debug information, use method_trace_level 10.	0

Key	Description	Default Value(s)
export_threshold_count	Indicates the number of items the export operation exports at one time.	100
use_format_extensions	<p>Use with format key to check for valid format extensions.</p> <p>If use_format_extensions is set to FALSE, files are published with the format extensions defined in the repository for the format.</p> <p>If use_format_extensions is set to TRUE and a particular extension is defined as valid for a particular format, files of that format with that extension are published with the extension.</p> <p>If use_format_extensions is set to TRUE and a particular extension is <i>not</i> defined as valid for a particular format, files of that format with that extension are published with the format extensions defined in the repository for the format.</p>	FALSE
format	<p>Use with use_format_extensions key.</p> <p>Takes the format:</p> <p>format.format_name=semicolon-separated_extensions</p>	
force_serialized	When set to TRUE, single-item publishes are performed serially rather than in parallel.	FALSE

Key	Description	Default Value(s)
sourceAttrsOnly	<p>By default, on each publish IDS creates a properties.xml file, which contains <i>all</i> the attributes of the objects published. If sourceAttrsOnly is set, IDS writes only the default attributes and any additional attributes that are published to the XML file.</p> <ul style="list-style-type: none"> <li>• r_object_id</li> <li>• r_modified_date</li> <li>• object_name</li> <li>• i_chronicle_id</li> <li>• r_version_label</li> <li>• content_id</li> <li>• i_full_format</li> <li>• r_folder_path</li> </ul>	FALSE
additionalMetatagFileExts	<p>Allows exported attributes to be added as metatags to file formats with the extensions asp, jsp, jht, and sht. Add them as a semicolon-separated list:</p> <p><code>additionalMetatagExtensions=asp;jsp;jht;sht</code></p>	No default value.
exportRelations	When set to TRUE and attributes are published, relation objects (dm_relation objects) are published to a database table on the target.	FALSE
cleanRepeatingTableNoAttrs	Deprecated.	
exportMediaProperties	When set to true, attributes of the dmr_content object and dm_format object are exported and published to the target.	FALSE

Key	Description	Default Value(s)
additional_media_properties	<p>When <code>export_media_properties</code> is set to true, used to specify additional attributes of <code>dmr_content</code> and <code>dm_format</code> objects to be published. The format is a semicolon-separated list:</p> <pre data-bbox="703 593 1013 656"><code>additional_media_properties=&lt;type1.attribute1;type2.attribute2&gt;</code></pre> <p>For example:</p> <pre data-bbox="703 720 1013 783"><code>additional_media_properties=dmr_content.x_range;dmr_content.z_range</code></pre>	FALSE
exclude_folders	<p>A semicolon-separated list of absolute repository paths, indicates the folders to be excluded from a publishing operation. When set, content files and attributes from folders indicated are not published. For example:</p> <pre data-bbox="703 1058 1013 1100"><code>exclude_folders=/acme.com/images;/acme.com/subdir</code></pre>	
pre_webroot_switch_script	<p>A script to be run before online synchronization takes place. <i>OpenText Documentum Interactive Delivery Services User Guide</i> contains more information.</p>	
post_webroot_switch_script	<p>A script to be run after online synchronization takes place. <i>OpenText Documentum Interactive Delivery Services User Guide</i> contains more information.</p>	
full_refresh_backup	<p>When set to TRUE, the content files and database tables on the target host are backed up before the synchronization phase in a full-refresh publishing operation.</p>	FALSE

Key	Description	Default Value(s)
exclude_formats	Takes a semicolon-separated list of format extensions and excludes content files with those extensions from publishing. For example to exclude .xml and .wml files: <code>exclude_formats=xml;wml</code>	Not set
check_valid_filename	If this parameter is set to TRUE, then the filename is checked for Windows illegal characters. Illegal characters are replaced as specified by the filename_replace_char parameter.  The default value of check_valid_filename is TRUE if the IDS source is on Windows; the default is set to FALSE for all other operating systems. This parameter should be used if the target is on a Windows host and the source is not on Windows.	TRUE (Windows only); FALSE for all other O/S
filename_replace_char	Windows only. Used in conjunction with check_valid_filename. Defines the character to use to replace invalid characters in file names on Windows.  For example: <code>filename_replace_char=0</code>	_ (underscore)
sync_on_zero_updates	When set to TRUE, database updates are made and pre- and post-synch scripts are run even if there is no new data to publish from the repository.	FALSE
transform_type	Used with Web Publisher Page Builder only.  Determines whether links in HTML pages are resolved at publication time to absolute or relative paths. Valid values are absolute and relative.	absolute

Key	Description	Default Value(s)
recovery_publish_retry_count	Controls the number of times IDSx tries to recover from a failed incremental publishing operation. The value is an integer that represents the number of times IDSx retries the publishing operation.	
set_tcp_delay	Determines TCP protocol behavior. With the default setting of FALSE, packets are sent to the target as soon as they are written on the source side; IDSx does not wait until the sockets buffer is filled or there is a timeout. For debugging purposes, this parameter can be set to TRUE. The setting must match the same key in agent.ini.	FALSE
ingest_workflow	<p>Used with Content Delivery web service only. Specifies a custom workflow to be used with the ingest operation. <i>OpenText Documentum Content Management - Enterprise Content Services Reference Guide (EDCPKSV250400-ARC)</i> contains the details on this web service.</p> <p> <b>Note:</b> This argument can be set at the repository (IDS Administration) level only. You cannot specify different ingest workflows for individual content delivery configurations.</p>	

Key	Description	Default Value(s)
wan_acceleration_ssh_port	<p>This is the TCP Port required for accelerated data transfer authentication. If the SSH port has to be changed, check the SSH service configuration (<code>sshd_config</code>) for Windows for changing the default port.</p> <p>The default value is applicable to all publishing configurations and can be overridden for each publishing configuration, by setting this as an extra argument for publishing.</p>	22
wan_acceleration_disabled	This parameter is used to disable the accelerated data transfer and use HTTP for file transfer.	False

Key	Description	Default Value(s)
wan_acceleration_policy	<p>This parameter defines the policy used for accelerated data transfer.</p> <ul style="list-style-type: none"> <li>• ADAPTIVE/FAIR (A): When set to this value, the file transfer monitors and adjusts the transfer rate to fully utilize the available bandwidth to the maximum limit. When there is congestion due to other file transfers, this mode shares bandwidth for other flows and utilizes a fair rate of transfer. In this mode, both the maximum and minimum transfer rates are required.</li> <li>• FIXED (F): When set to this value, the file transfer happens at a specified target rate, irrespective of the actual network capacity. In this mode, a maximum transfer rate is required.</li> <li>• TRICKLE/STEALTH (T): When set to this value, the file transfer uses the available bandwidth to the maximum rate. When there is congestion due to other file transfers, the transfer rate is reduced down to the minimum rate.</li> </ul>	A
min_file_transfer_rate	This is the minimum file transfer rate	0 Mbps
max_file_transfer_rate	This is the maximum file transfer rate	1000 Mbps
wan_acceleration_log_details	The file transfer process status are captured in the content delivery log files	FALSE

Key	Description	Default Value(s)
wan_acceleration_file_checks um	<p>This parameter is used to resume file transfer when there is a failure.</p> <ul style="list-style-type: none"><li>• FILE_ATTRIBUTES: When set to this value, checks for the file size of both files. If the file size is the same, then transfer does not take place.</li><li>• FULL_CHECKSUM: When set to this value, checks for the checksum of both files. If it matches, then transfer does not take place</li><li>• SPARSE_CHECKSUM: When set to this value, checks for the sparse checksum of both files. If it matches, then transfer does not take place</li><li>• OFF: When set to this value, the file gets replaced</li></ul> <p>When set to OFF, the rate of file transfer is high.</p>	OFF

Key	Description	Default Value(s)
decision_commit_rollback	<p>This parameter is used to set the threshold value for transaction capability. For example, if there are 10 replication targets, and if the DCR value reads as:</p> <pre data-bbox="687 530 1013 561">decision_commit_rollback 6</pre> <p>implies that if replication operation succeeds on a minimum of 6 replication targets, then a decision is taken to commit (File System and RDBMS) the changes performed by the replication operation.</p> <p>If the <i>number_of_failures</i> value is greater than the <i>decision_commit_rollback</i> value, a rollback is initiated on the replication targets.</p> <p>The value assigned to this attribute must be a positive integer.</p>	NA
tc_file_count	<p>The transaction capability is based on <i>tc_file_size</i> and <i>tc_file_count</i>.</p> <p>When the number of files replicated exceeds <i>tc_file_count</i>, transaction capability feature is disabled.</p> <p>The value assigned to this attribute must be a positive integer.</p>	500
tc_file_size	<p>The transaction capability is based on <i>tc_file_size</i> and <i>tc_file_count</i>.</p> <p>When the size of the files replicated exceeds <i>tc_file_size</i>, transaction capability feature is disabled. The units is specified in MB.</p> <p>The value assigned to this attribute must be a positive integer.</p>	100 MB

Key	Description	Default Value(s)
use_replication_time	Use this extra argument to make sure that after replication is complete, all the replication targets will display the same time stamp as when the replication was triggered.	TRUE
use_repository_time	Use this extra argument to make sure that after replication is complete, all the replication targets will display the same time stamp as when the content was last modified in the repository ( <code>r_modified_date</code> when the file was replicated).	TRUE
lock_exitifbusy_flag	During publishing or replication operations, IDSx locks a configuration using a webc lock object, so that only one publishing or replication operation can take place at a time for that configuration. If you want IDSx to exit rather than retry when the publishing configuration is locked, set the <code>lock_exitifbusy_flag</code> argument to TRUE.	TRUE

Key	Description	Default Value(s)
auto_replication	<p>Replication can be invoked automatically after a publishing operation by setting the extra argument auto_replication to TRUE in Documentum Administrator.</p> <p> <b>Note:</b> Concurrent single item publishing at the same time as auto replication causes a considerable load on the staging target. Hence, set the extra argument lock_exitifbusy_flag along with auto_replication to TRUE. The subsequent replication process will consider all the published batches that were left unused during the creation of the previous replication batch.</p>	TRUE
full_refresh_transactional_repli cation	<p>The replication process can start a transactional replication, even when the replication batch being replicated contains a full refresh publish. Replication Manager can be enhanced to start a transactional replication setting the extra arguments, full_refresh_transactional_repli cation and full_refresh_backup, to TRUE for full refresh publish.</p>	FALSE
post_replication_script_on_st aging_target	<p>Use this script to perform any arbitrary action on the staging target after replication is complete on all replication targets.</p>	No default value.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD) contains the instructions on creating or modifying extra arguments.*

## 23.7 Deleting content delivery configurations

If a content delivery configuration is no longer needed, you can delete it. To stop publishing using the configuration, make the content delivery configuration inactive.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on deleting content delivery configurations.

## 23.8 Testing content delivery configurations

After creating a content delivery configuration, test it by running the end-to-end tester, which simulates a publishing operation without publishing any documents. The end-to-end tester tests all parameters set in a publishing configuration and ensures that IDS/IDSx can make the necessary connections to the database and target host.

The end-to-end tester creates a log file in the repository whether the test fails or succeeds. View the resulting log file after running the tester. If the test fails, examine the log file to determine which element of your IDS/IDSx installation is not working. You can read the file from Documentum Administrator or retrieve it directly from the repository where IDS/IDSx log files are stored in the /System/Sysadmin/Reports/Webcache folder.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on testing content delivery configurations.

## 23.9 Duplicating a content delivery configuration

Create a new content delivery configuration by duplicating and then modifying a content delivery configuration that is thoroughly tested and successfully used in production. The IDS Configuration Template stores default values that you can use to create new content delivery configurations.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on duplicating content delivery configurations.

## 23.10 Deactivating a content delivery configuration

To suspend publishing operations without deleting the content delivery configuration, deactivate it using the instructions in this section.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on deactivating content delivery configurations.

## 23.11 Publishing objects

You can manually run a publishing job from the Interactive Delivery Services Configuration list page.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on the following:

- Publishing from content delivery configurations
- Replicating from content delivery configurations
- Ingesting from content delivery configurations

## 23.12 Content delivery configuration results

This page indicates whether a publishing or a replication operation succeeded or failed. For details on the publishing operation, on the *content delivery configuration publish result* page, click the links to view the publishing logs. Similarly, for details on the replication operation, click the links on the *content delivery configuration replicate result* page to view the replication logs. After viewing the log, click **OK** or **Cancel** to close the log, then click **OK** or **Cancel** to return to the **Interactive Delivery Services Configuration** list page.

Interactive Delivery Services version 6x can be configured for email notification of content delivery configuration results. *OpenText Documentum Interactive Delivery Services User Guide* and *OpenText Documentum Interactive Delivery Services Accelerated User Guide* documents contain more information.

## 23.13 Content delivery logs

Each publishing operation or end-to-end test generates a log file. View these files to determine whether publishing succeeded and to diagnose problems when a publishing operation fails. To navigate from the publishing log list page, click the **Content Delivery** breadcrumb.

### 23.13.1 Viewing content delivery logs

Each publishing event or publishing test generates a log file. Review the file after publishing or testing a content delivery configuration to determine if the operation succeeded.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing content delivery logs.

### 23.13.2 Deleting content delivery logs

After you examine logs or as they accumulate in the repository, you may want to delete them.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on deleting content delivery logs.

## 23.14 Effective labels

Use *effective labels* to enable IDS to determine which documents to publish based on effective and expiration dates.

The effective label specified in a content delivery configuration allows IDS to determine when to publish a particular document and when to delete it from the website. IDS does this by examining the repeating properties `a_effective_label`, `a_effective_date`, and `a_expiration_date`, which are properties of the `dm_sysobject` type. These properties are inherited by all subtypes of `dm_sysobject`.

Each `a_effective_label` corresponds to a matching `a_effective_date` and `a_expiration_date`. Because these are repeating properties, you can specify multiple effective labels, effective dates, and expiration dates for each document. IDS looks for the effective and expiration dates matching a particular effective label, and uses the dates to determine when to publish a document and when to withdraw the document from the website.

For example, a document might have the effective label, effective date, and expiration date properties set as follows:

**Table 23-6: Using effective labels**

<code>a_effective_label</code>	<code>a_effective_date</code>	<code>a_expiration_date</code>
DRAFT	03/05/08	03/15/08
REVIEW	03/16/08	03/26/08
COMMENT	03/27/08	04/10/08
APPROVED	04/10/08	04/10/09

Setting the effective label of document to REVIEW means the document will be published on March 16, 2008 and removed from the website on March 26, 2008.

Setting the effective label to APPROVED means the document will be published on April 10, 2008 and withdrawn on April 10, 2009.

Documents whose effective label does not match the effective label set in the content delivery configuration are published regardless of the values set for effective date and expiration date.

# Chapter 24

## Indexing management

### 24.1 Indexing

A full-text index is an index on the properties and content files associated with documents or other SysObjects or SysObject subtypes. Full-text indexing enables the rapid searching and retrieval of text strings within content files and properties.

Full-text indexes are created by software components separate from Documentum CM Server. The index agent prepares documents for indexing and xPlore creates indexes and responds to queries from Documentum CM Server. *OpenText Documentum xPlore Deployment Guide* contains the information on installing the index agent and xPlore.

You must have system administrator or superuser privileges to start, stop, or disable index agents, start or stop xPlore, and manage queue items. *OpenText Documentum xPlore Administration Guide* contains the information on editing the properties of the index agent configuration object and other full-text configuration objects.

### 24.2 Index agents and xPlore

The Index Agents and Index Servers list page shows the index agent and index queue associated with the repository.

The index agent exports documents from a repository and prepares them for indexing. A particular index agent runs against only one repository. xPlore creates full-text indexes and responds to full-text queries from Documentum CM Server.



**Note:** If you are using Documentum CM Server with xPlore, by default, sorting on attribute is performed by the database on results returned from xPlore. To alter the behavior, add dm\_ft\_order\_by\_enabled to dm\_docbase\_config:

```
retrieve,c,dm_docbase_config  
append,c,1,r_module_name  
dm_ft_order_by_enabled  
append,c,1,r_module_mode  
save,c,1  
reinit,c
```

Make sure that the subpath is configured correctly in `indexserverconfig.xml`. For example, set "sortable= true" for subpath "dmftmetadata//object\_name". Then, using DQL, you can let xPlore to order by attribute `object_name`. For example:

```
select r_object_id from dm_sysobject search document  
contains 'john' order by object_name
```

This is applicable for sorting results supported in xPlore with the appropriate index configuration.

## 24.3 Starting and stopping index agents

You can stop a running index agent or start an index agent that is stopped.

An index agent that is disabled cannot be started and is not started automatically when its Accelerated Content Services server is started. You must enable the index agent before starting it. “[Enabling index agents](#)” on page 573 contains the information on enabling a disabled index agent. If the status of index agent is **Not Responding**, examine the machine on which it is installed and make sure that the software is running.



### Caution

Stopping the index agent interrupts full-text indexing operations, including updates to the index and queries to the index. An index agent that is stopped does not pick up index queue items or process documents for indexing.



**Note:** If the Documentum CM Server is in a *projected to dormant* state, then starting or stopping the index agent works correctly. However, if the Documentum CM Server is in a *dormant* state, then starting or stopping the index agent using Documentum Administrator does not work correctly. The status of the index agent appears as **Not Responding**. The index agent logs contain the following error: [DM\_INDEX\_AGENT\_UNEXPECTED\_DFC\_EXCEPTION] Unexpected DfException: context: Init Connector cause: [DM\_SESSION\_E\_OP\_DISALLOWED\_IN\_STATE\_UNLESS\_ENABLED] error: “The operation (Opening a new transaction) is disallowed when the server is in Dormant state unless enabled by Data Center Managers on their sessions.”

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on starting or stopping index agents.

## 24.4 Disabling index agents

An index agent that is disabled cannot be started and is not started automatically when its Accelerated Content Services server is started. You can disable an index agent only after it has been stopped. To start a disabled index agent that is not running, you must enable the index agent first, using the instructions in “[Enabling index agents](#)” on page 573.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on disabling index agents.

## 24.5 Enabling index agents

An index agent that is disabled cannot be started (if it is stopped) and is not started automatically when its Accelerated Content Services server is started. You must first stop the index agent if it is running.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on enabling index agents.

## 24.6 Verifying indexing actions

You are asked to confirm stopping, starting, suspending, resuming, and reindexing index agents, and enabling or disabling index agents. The confirmation page displays the action you requested. Click **OK** to continue with the action or **Cancel** to stop the action.

## 24.7 Viewing or modifying index agent properties

You can view the properties of an index agent. You can modify the following index agent properties, but it is recommended that you do not change the values:

- Exporter Thread Count

This is the number of concurrent exporter threads run by the index agent. The default value is 3. If you change the exporter thread count, you must restart the index agent for the change to take effect.

- Polling Interval

This is the frequency, in seconds, at which the index agent polls for queue items. The default value is 60.

All other properties are read-only.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on viewing or modifying index agent properties.

## 24.8 Managing index queue items

Creating, versioning, or deleting a SysObject or SysObject subtype creates a queue item indicating that the full-text indexes must be updated to account for the changes. The index agent reads items from the queue and ensures that the required index updates take place.

If the indexing system of the repository runs in a high-availability active-active configuration, with multiple index agents and xPlore installations, each index agent/xPlore federation pair supports its own index. Creating, versioning, or deleting a SysObject or SysObject subtype creates a queue item for each pair, and each index is updated.

If the indexing system is in a high-availability active-active configuration, the name of each index is displayed at the top of this page, and only the queue items for one index at a time are displayed.

By default, the list page displays failed queue items. To filter the queue items by status, choose the appropriate status on the drop-down list:

- **Indexing Failed**, which is the default status displayed  
If indexing failed, information about the error is displayed in red under the name and other properties of queue item.
- **All**, which displays all current queue items in the repository
- **Indexing in Progress**, which indicates that the object is being processed by the index agent or xPlore federation
- **Awaiting Indexing**, which indicates that the index agent has not yet acquired the queue item and started the indexing process
- **Warning**, which indicates that the index agent encountered a problem when it attempted to start the indexing process for the object  
If indexing generated a warning, information about the problem is displayed in red under the name and other properties of queue item.

Queue items that have failed indexing can be resubmitted individually, or all failed queue items can be resubmitted with one command. *OpenText Documentum xPlore Administration Guide* contains the instructions on resubmitting objects for indexing.

#### **24.8.1 Resubmitting individual objects**

You can resubmit individual objects for indexing.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on resubmitting individual objects.

#### **24.8.2 Resubmitting all failed queue items**

You can resubmit for indexing all documents that failed indexing. This menu choice executes the mark\_for\_retry administration method. If the indexing system is installed in a high-availability configuration, all failed queue items for all indexes are resubmitted.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on resubmitting all failed queue items.

### 24.8.3 Removing queue items by status

You can remove index queue items by status.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on removing queue items by status.

### 24.8.4 Removing queue items

You can remove queue items from the indexing queue. Note that if a queue item has already been acquired by the index agent, it cannot be removed from the indexing queue.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on removing queue items.

### 24.8.5 Viewing queue items associated with an object

From the cabinets of a repository, you can view the index queue items associated with a particular object.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on viewing queue items associated with an object.

### 24.8.6 Creating new indexing queue item

You can create a queue item to submit a particular SysObject for indexing.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the instructions on creating new indexing queue item.



## Chapter 25

# OpenText Documentum Content Management (CM) Transformation Services management

A repository can be polled by multiple Transformation Services instances. All Transformation Services instances polling the repository are displayed in the **Content Transformation Services** node in Documentum Administrator.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the information on the following:

- Understanding Transformation Services overview
- Changing the Transformation Services user
- Configuring a Transformation Services instance
- Viewing a Transformation Services log file
- Viewing details of a Transformation Services instance
- Controlling your Transformation Services instance
- Reporting in Transformation Services



# Chapter 26

## Analytics management

Use Content Intelligence Services (CIS) to analyze the textual content of documents and know what the documents are about without having to read them.

By default, CIS analyzes the content of the documents, including the values of the file properties. You can change the default behavior and have CIS analyze the values of the OpenText Documentum CM object attributes in addition to, or instead of, the content of the documents.

CIS performs several types of analysis:

- *Categorization*: By detecting predefined keywords in the document content, the categorization identifies the category to which a document belongs. Categories for a subject area are organized in a structure called a taxonomy. Categorization enables you to organize content in a logical and consistent way.
- *Entity detection*: It relies on Natural Language Processing (NLP). Named entities are detected by performing a semantic analysis of their context. If there is too little context, or if the context is unclear, the detection can seem to be incomplete. You can use entity detection to find named entities such as people names or company names in documents.
- *Pattern detection*: Some pieces of information always have the same form. Use the pattern detection to retrieve this information when it is disseminated in text. For example, email addresses, because they comply with a standard, can be extracted using pattern detection. Pattern detection retrieves all pieces of information that match the pattern.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the information and instructions on the following:

- Understanding Content Intelligence Services in OpenText Documentum CM applications
- Configuring Content Intelligence Services in Documentum Administrator
- Building taxonomies for classic categorization
- Selecting and submitting the documents to analyze
- Managing analysis results



## Chapter 27

# Resource management

## 27.1 Understanding resource management

The Resource Management node provides an interface for viewing and managing OpenText Documentum CM resources exposed in the OpenText Documentum CM environment as Java Management Beans (MBeans). Documentum Administrator maintains the list of resource agents, which includes the information necessary to access a resource agent. The resource agent information is stored in the `ResourceAgentsRegistry` in the global registry.

Users access the MBean resources in the distributed network through a resource agent (JMX agent) to obtain a list of available MBean resources that they can manage. The Resource Management node displays a list of the resource agents; however, only a system administrator can create, delete, or update resource agents.

A resource agent may require authentication to access its resources (MBeans). Documentum Administrator first attempts to authenticate the user using the current session login information. If authentication fails, Documentum Administrator prompts for a user name and password.

## 27.2 Managing resource agents

Select the Resource Management node (**Administration > Resource Management**) to access the Resource Agents list page. The resource agent information is stored in the `ResourceAgentsRegistry` in the global registry. If no resource agents are configured in the global registry, the Resource Agents list page displays a message that no items were found.

System administrators can add, delete, and edit resource agents. A resource agent may require authentication to access its resources (MBeans). Documentum Administrator will first attempt to authenticate the user using the current session login information. If that fails, then Documentum Administrator prompts for a username and password.

From the **Resource Agents** list page, you can:

- Add resource agents.
- Access the Resource Agent Properties - Info page to view or modify resource agent properties.
- Delete resource agents.
- Access the Resources on Agent list page for a specific resource agent.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the information and instructions on the following:

- Adding resource agents
- Viewing or modifying resource agent properties
- Deleting resource agents

## 27.3 Managing resource properties

The Resources on Agent list page displays MBean resources for a selected resource agent. Select a resource to display the properties of the resource, such as attributes, operations, notifications, and a log file, if defined.

- The Resource Properties - Info page displays key information about the resource. The polling interval defines the frequency to poll the resource for activity. This is not used in the current release.
- The Resource Properties - Attributes page displays the resource attributes. Writeable attributes provide an input control to update the attribute value. Attribute changes will be updated on the resource by clicking the **Save Changes** or **OK** button.
- The Resource Properties - Operations page displays the operations that can be performed. Selecting an operation displays the operations dialog, which enables you to enter any required data, perform the operation, and view the results (if the operation has results).
- The Resource Properties - Notifications page displays the resource notifications you are subscribed to.
- The Resource Properties - Log page enables you to:
  - Specify the log level for tracing.
  - Specify the log level of messages.
  - Specify the number of viewable log file lines.
- The <MBean name> Monitor page displays information for resource types that have been configured for the server monitor interface.

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the information and instructions on the following:

- Managing general information for resources
- Managing resource attributes
- Managing resource operations
- Viewing resource notifications
- Viewing the notification page

- Viewing resource logs

### 27.3.1 Monitoring resources

The <MBean name> Monitor page displays information for resource types that have been configured for the server monitor interface. The monitor interface is available only for these MBean types:

- AcsServerMonitorMBean
- AcsServerConfigMBean
- JmxUserManagementMBean
- IndexAgent

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on monitoring resources.

### 27.3.2 Manual configuration steps for monitoring resources

This section details the manual configuration steps for monitoring resources.

#### To manually configure:

1. The following changes are required in \app\webcomponent\config\admin\resourcemanagement\resources\mbeanresourceslist\_component.xml.

Add the JMXBeans to the <mbeantypes> node list.

```
<mbeantypes>
<!--name denotes the exact name of MBean-->
    <mbeantype name='IndexAgent'>
        <!--onclickcomponent specifies the component to be invoked-->
            <onclickcomponent>mbeanresourcemonitordialogcontainer</onclickcomponent>
        </mbeantype>
    </mbeantypes>
```

2. The following changes are required in \app\webcomponent\config\admin\resourcemanagement\resources\mbeanresourcemonitor\_component.xml.

Add the JMXBeans to the <mbeantypes> node list.

```
<mbeantypes>
<!--name denotes the exact name of the MBean-->
    <mbeantype name='IndexAgent'>
        <!--attributes are the list of the attributes that need
        to be exposed in the monitor user interface-->
        <attributes>
            <attribute>Status</attribute>
            <attribute>Mode</attribute>
            <attribute>...</attribute>
        </attributes>
        <!--operations are the list of the operations that need to be exposed
        in the monitor user interface. launchcomponent=true will launch the
        operations user interface in a new window. Also if the operation
        requires user input, then the user interface automatically opens in a
        new window-->
        <operations>
            <operation launchcomponent='false'>Start</operation>
            <operation launchcomponent='true'>downloadLogFile</operation>
            <operation launchcomponent='true'>...</operation>
        </operations>
    </mbeantype>
</mbeantypes>
```

```
<!--notifications are the list of notifications, ideally the  
empty list will capture all notifications.-->  
    <notifications></notification></notifications>  
<!--refreshinterval denotes the interval in miliseconds for the  
monitor user interface to be refreshed. Ideal value should be 10sec.-->  
    <refreshinterval>10000</refreshinterval>  
</mbeantype></mbeantypes>
```

## Chapter 28

# Cabinets, files, and virtual documents

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the information and instructions on the following:

- Managing cabinets, folders, and files
- Understanding home cabinets
- Creating cabinets
- Creating folders
- Creating files
- Working with files
- Deleting cabinets, folders, or files
- Moving files
- Copying files
- Viewing the clipboard
- Linking cabinets, folders, or files
- Managing subscriptions
- Enabling change notifications
- Managing relationships
- Understanding renditions and transformations
- Configuring PDF Annotation Services
- Understanding virtual documents



## Chapter 29

# API and DQL

### 29.1 API and DQL

DQL queries and server APIs can be run from Documentum Administrator pages that contain a Tools menu. Use the DQL query pages to run DQL queries and to test whether DQL SELECT statements return the expected values. Use the API pages to enter methods and to send method calls directly to the server.

### 29.2 DQL editor

The Dql Enter Query page enables you to test whether a DQL SELECT statement returns the expected values. Use this page as a tool for testing DQL.

The number of rows returned by a DQL statement is limited based on the width of the rows requested. The query results may be truncated. When this happens, a warning message appears.

1. Select **Tools > Dql Editor**.
2. Type the query in the text box.
3. To display the SQL statement produced by the query, select **Show the SQL**.
4. Click **Execute**.

The query results are returned.

### 29.3 API tester

The API Tester page enables you to enter methods directly in the API text field by typing the method name and its arguments as a continuous string, with commas separating the parts.

For example, the following command creates a folder:

```
API> create,s0,dm_folder
```



**Note:** Methods entered in the API text field bypass the Foundation Java API and directly access the Documentum Client Libraries (DMCL). Therefore, the Foundation Java API cannot perform its usual validation of the methods.

#### To run server APIs:

1. Select **Tools > Api Tester**.
2. Select **Single-Line Command Entry or Script (multi-line) Entry**.

3. Enter the API.
  - If you are in Single-Line mode, enter the command and any necessary data in the **Command** and **Data** text boxes.
  - If you are in Script Entry mode, type the method and its arguments in the **Commands** text box.
4. To display the SQL statement produced by the query, select **Show the SQL**.
5. Click **Execute**.

# Chapter 30

## Search

### 30.1 Searches

Documentum Administrator offers different ways to search repositories and external sources. By default, Documentum Administrator provides a simple search and an advanced search. If Federated Search Services is installed on the Documentum CM Server host, administrators also have the option to create search templates and configure smart navigation.

*OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains more information on installing Federated Search Services.

### 30.2 Setting search preferences

Search preferences specify the default search locations and enable smart navigation.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on setting search preferences.

### 30.3 Search guidelines

In general, the following guidelines apply to searches:

- If a document cannot be indexed, it also cannot be searched. For example, documents that contain binary content cannot be indexed.
- Only certain characters can be searched, such as alphabetic, numeric, extender, and custom characters. Custom characters include Chinese, Japanese, Korean letters, and months.

Other characters, including punctuation, accent, and diacritical marks, and characters such as | and #, are not indexed or searched. These characters are removed from the indexed text and are treated as blank spaces. The xPlore federation treats characters such as !@#\$%^\_,&;:()+=< as white space.

- The plus and minus signs cannot be used as operators. You must use the AND operator, and the OR instead.
- The asterisk, and the question mark can be used as wildcards.

## 30.4 Running a simple search

When a user enters a search term (a word or phrase) in the simple search box, the term is matched to documents or other objects that have the search term within the document itself or within the properties of object. This kind of search is called a full-text search.

A full-text search searches the files in default search location that the user is specified in the search preferences. The search can include several repositories at the same time and external sources such as external databases, web sources or the desktop.

When displaying search results, Documentum Administrator displays files with the most matching words first. If a repository has been indexed for parts of speech, Documentum Administrator also displays files that include variations of the words. For example, if a user searches for *scanning*, Documentum Administrator also looks for files that contain the words *scan*, *scanned*, and *scanner*.

*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains the instructions on running a simple search.

### 30.4.1 Further define search terms

You can use the syntax in “[Further define search terms](#)” on page 590 to further define search terms within a simple search or within the **Contains** field in an advanced search.

**Table 30-1: Further define search terms**

Syntax	Description
Quotation marks around a word or phrase: “ ”	To search for an exact word or phrase, type quotation marks around the word or phrase.  For a simple search (including the Contains field in an advanced search), if you do not use quotation marks, Documentum Administrator displays files that contain both the exact words you typed as well as variations of the words, such as <i>scanning</i> for the word <i>scanner</i> .  This option is disabled when searching for more than one word or if your repository has not been indexed for variations.  Quotation marks cannot be used to match the exact case of a word.

Syntax	Description
The <b>AND</b> and <b>OR</b> operators	<p>To get results that contain two search terms, type <b>AND</b> between the terms. A term can be a word or quoted phrase.</p> <p>To get results that contain at least one term, type <b>OR</b> between the words or the quoted phrases.</p> <p>You can string together multiple terms with the <b>AND</b> and <b>OR</b> operators. The <b>AND</b> operator has precedence over the <b>OR</b> operator. For example, if you type:</p> <pre>knowledge or management and discovery</pre> <p>then your results must contain either knowledge or they must contain management, and discovery.</p>
The <b>NOT</b> operator	<p>To get results that do not contain a term, type <b>NOT</b> before this term. The term can be a word or a quoted phrase. Only the term that follows the operator is taken into account.</p> <p>The <b>NOT</b> operator can be used after the <b>AND</b> or <b>OR</b> operator, separated by a space.</p> <p>Valid syntaxes would be: <i>Documentum NOT adapter</i> or <i>Documentum AND NOT adapter</i>, both queries will return results that contain Documentum but do not contain adapter.</p> <p>If you type <i>Documentum OR NOT adapter</i>, you get results that either contain Documentum (and possibly contain adapter) or that do not contain adapter. Use this syntax cautiously. It can generate a very large number of results.</p> <p>The <b>NOT</b> operator can be used alone at the beginning of the query. For example, if you type <i>NOT adapter</i>, you get results that do not contain adapter. Use this syntax cautiously. It can generate a very large number of results.</p> <p>The <b>NOT</b> operator is not supported for queries on external sources when it is alone at the beginning of the query or if used with the <b>OR</b> operator.</p> <p>The <b>NOT</b> operator cannot be used with parentheses. This is invalid: <i>A NOT ( B OR C )</i>. However, the <b>NOT</b> operator can be used inside parentheses. This is valid: <i>(A NOT B) OR (A NOT C)</i>.</p> <p>ANDNOT (in one word) is not an operator, if you enter ANDNOT in a query, it will be considered as a search term.</p>

Syntax	Description
Parentheses around terms: ()	<p>To specify that certain terms must be processed together, use parentheses. When using parenthesis, you <i>must</i> type a space before, and after each parenthesis mark, as shown here: (<i>management or discovery</i>)</p> <p>As an example, if you type <i>knowledge and management or discovery</i>, then your results will contain both knowledge, and management or they will contain discovery. But if you type <i>knowledge and (management or discovery)</i>, then your results will contain knowledge, and either management or discovery.</p>
The multiple-character wildcard: *	<p>If the repository is indexed, you can use the multiple-character wildcard to indicate additional characters anywhere in a word. It matches zero or more characters. The multiple-character wildcard is only available or a simple search (including the <b>Contains</b> field in an advanced search).</p> <p>The multiple-character wildcard is not available for a searches on non-indexed repositories, for searches of property values, or for searches of external sources. For those, you should use truncation operators, such the <b>Begin with</b> operator.</p> <p> <b>Note:</b> If you use wildcards, then Documentum Administrator will not display results that include variations of the words you typed. For example, if you type d*ment then your results must contain: document, development, deployment, department, and so on but not documented or documentation.</p>
The single-character wildcard: ?	<p>If the repository is indexed, you can use the single-character wildcard to indicate a single, unknown character anywhere in a word.</p> <p>The single-character wildcard is only available or a simple search (including the <b>Contains</b> field in an advanced search).</p> <p>The single-character wildcard is not available for searches on non-indexed repositories, for searches of property values, or for searches of external sources.</p>



## Notes

- The operators AND, OR, and NOT are reserved words. To search a term that includes an operator, use quotation marks. For example, if you search for “hardware and software”, Documentum Administrator returns documents with that string of three words. If you type hardware, and software without quotation marks, Documentum Administrator returns all of the documents that contain both words.
- The operators AND, OR, and NOT are not case-sensitive. For example, for your convenience, you can type: AND, and, And.

## 30.5 Running an advanced search

To search for a document by one of its properties, use advanced search. An advanced search enables you to define more precisely your query on the properties of the document. For example, you can search the current version of the documents whose author is John Smith, and modified between November 1, 2006 and December 31, 2006.

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on running an advanced search.

## 30.6 Search results

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the information and instructions on the following:

- Viewing search results
- Using smart navigation feature
- Monitoring search results in real time
- Saving search results from external sources

## 30.7 Additional configuration options

The search functionality described in this guide refers to the default configuration. However, your system administrator can configure this functionality in many ways. This list details possible configurations that can affect your search experience:

- *Indexing*: Indexing capabilities can be used to define more precise queries. For example, wildcards can only be used if the repository is indexed, if not, they are skipped. If you want to run complex queries, consult the system administrator for details on the indexing configuration of the repository.
- *Relevancy ranking*: The system administrator can specify a bonus ranking for specific sources, add weight for a specific property value or improve the score for a specific format.
- *Presets*: The system administrator can define a preset to restrict the list of available types in the Advanced search page. Presets can be different from one repository to another. If you select only external sources, the preset of the current repository applies.
- *Customization of the Advanced search page*: The Advanced search page can be fully customized to guide you in running queries. For this reason, all the options described in this guide may not be available, and other may appear to narrow and/or condition your queries.
- *Maximum number of results*: The maximum number of results is defined at two levels. By default, the maximum number of results, taking all sources together, is 1000 and 350 results per source. However, your system administrator can modify

these parameters. When querying an external source, the maximum number of results also depends on the configuration set for this source. Results are selected according to their ranking. This way, you always get results with the best ranking; other results are skipped.

- *Case-sensitivity*: If the repository is indexed, queries are case-insensitive by default, even using quotation marks. If the repository is not indexed, then queries are case-sensitive. However, for non-indexed repositories, case-sensitivity can be turned on, and off by the system administrator.
- *Grammatical normalization (lemmatization)*: When you do not use quotation marks, Documentum Administrator displays files that include variations of the words you typed in addition to the exact words. These variations are based on the root of the word. This behavior depends on the configuration of the full-text engine, and is called grammatical normalization.
- *External sources*: When querying an external source, the results displayed in Documentum Administrator depend partly on the configuration of this source. For example, if the source does not return information on dates, then dates cannot be filtered.
- *Multiple repositories*: As for external sources, the results depend on the configuration of each repository. For example, the indexing may be set differently on various repositories.

## 30.8 Saved searches

Searches can be saved so that you can launch them regularly without redefining them, share them between users, or to quickly retrieve the corresponding results. *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the information and instructions saving a search, running a saved search, and editing a saved search.

## 30.9 Creating a search template

If Federated Search Services is installed on Documentum CM Server, Documentum Administrator provides the option to create search templates. A search template is a predefined search in which users can change certain search values each time they run the search. Search templates can be private or public. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains information on installing Federated Search Services. *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the instructions on creating a search template.

# Chapter 31

## Inbox

*OpenText Documentum Content Management - Administrator User Guide*  
(EDCAC250400-UGD) contains the information and instructions on the following:

- Understanding inboxes
- Opening a task or notifications
- Performing a task
- Completing a task
- Accepting a group task
- Rejecting a task
- Delegating a task
- Repeating a task
- Changing availability of tasks
- Understanding work queue tasks



## Chapter 32

# Workflows, work queues, and lifecycles

## 32.1 Workflows

A workflow is an automated process that passes files and instructions between individuals in sequence to accomplish specific tasks. When users are assigned a workflow task, the task appears in their Inbox.

Workflows can include automatic tasks that the system performs, such as the execution of scripts. Automatic tasks allow the integration of workflows and lifecycles.

### 32.1.1 Configuring the workflow agent

The workflow agent controls the execution of automatic activities in a workflow. The agent is comprised of a master repository session and one or more worker sessions. The master session is dormant until the workflow agent is notified by Documentum CM Server that an activity has been created or until the sleep interval expires. At that time, the master session queries the repository for information about the activity or activities and assigns the waiting activity to a free worker session.

#### 32.1.1.1 Changing the number of worker sessions

The number of worker sessions available to execute automatic activities is controlled by the workflow agent worker threads property value in the server configuration properties. By default, this value is set to 3. You can reset the value to any positive number to a maximum of 1000. [“Modifying general server configuration information” on page 32](#) contains more information on the server configuration properties.

You must stop and restart Documentum CM Server for your change to take effect. Reinitializing the server does not make the change effective.

#### 32.1.1.2 Changing the sleep interval

The sleep interval determines how long the master session sleeps after querying the repository for activity information in the absence of a notification from Documentum CM Server. If the sleep interval expires without a notification, the master session wakes up and queries the repository even though it has not received a notification from Documentum CM Server. The default sleep interval is 5 seconds. You cannot change this value in Documentum Administrator. Use IDQL to change the value.

The sleep interval is controlled by the wf\_sleep\_interval property in the server configuration object. The value is interpreted in seconds. You must stop and restart

Documentum CM Server for your change to take effect. Reinitializing the server does not make the change effective.

### 32.1.1.3 Changing the system shutdown timeout

The system shutdown timeout property in the server configuration object sets the time that the workflow agent attempts to shut down work items gracefully after receiving a shutdown command. This feature is only applicable for repositories that use multiple Documentum CM Servers.

If the shutdown timeout period is exceeded (or is set to zero), the workflow agent shuts down immediately. When the workflow agent does not shut down gracefully, automated tasks in certain states can be corrupted. If tasks are corrupted, restarting the Documentum CM Server does not result in resumption of the managed workflows. The server log file indicates when a graceful shutdown did not occur. Use the RECOVER\_AUTO\_TASKS administration method to recover the automated tasks.



**Note:** In some cases, restarting the Documentum CM Server after an ungraceful shutdown can result in automated tasks executing again.

If the timeout period is a negative value, Documentum CM Server waits for the workflow agent threads to complete the automatic tasks held by workflow agent workers before shutting down gracefully.

The default system shutdown timeout setting is 120 seconds. “[Modifying general server configuration information](#)” on page 32 contains more information on the server configuration properties.

### 32.1.1.4 Enabling immediate processing of automatic activities

The notify new task attribute (wf\_agent\_notify\_newtask) on the server configuration object enables you to force immediate processing of automatic activities. Configure the Documentum CM Server to notify the workflow agent to process automatic tasks immediately after the system creates them by setting the wf\_agent\_notify\_newtask attribute to TRUE. You cannot change this value in Documentum Administrator. Use IDQL to change the value.

When the wf\_agent\_newtask attribute is set to TRUE, the following occurs:

- If the system creates automatic tasks when the workflow agent is processing the previously collected tasks, then the workflow agent ignores the wf\_sleep\_interval and collects the next set of automatic activities.
- If the system has not created an automatic task when the workflow agent is processing the previously collected tasks, then the workflow agent sleeps for the time specified in wf\_sleep\_interval.
- If the system creates tasks when the workflow agent is sleeping, then the agent wakes up immediately and collects the next set of automatic activities.

When the wf\_agent\_notify\_newtask attribute is set to FALSE, the workflow agent honors the value of the wf\_sleep\_interval and sleeps for the time specified before the workflow agent collects the next set of automatic activities for processing.

By default, the value for the wf\_agent\_notify\_newtask attribute is TRUE.

#### 32.1.1.4.1 Skipping workflow task assignment

A parameter WF\_SKIP\_PARALLEL\_TASK\_EXECUTION can be set in the dm\_docbase\_config object for the following activities:

- To disallow workflow agent to query for workitems from workflows that already have other workitems assigned.
- To create a logic to skip task assignment if one of them is assigned from the same workflow.

To achieve, perform the following:

- Add r\_module\_name in dm\_docbase\_config to WF\_SKIP\_PARALLEL\_TASK\_EXECUTION
- Add r\_module\_mode in dm\_docbase\_config to 1
- Save dm\_docbase\_config
- Restart the repository

#### 32.1.1.5 Tracing the workflow agent

By default, tracing for the workflow agent is turned off. You can turn it on by executing a SET\_OPTIONS administration method with the -trace\_workflow\_agent option specified. For more information about the SET\_OPTIONS administration method, refer to “[SET\\_OPTIONS](#)” on page 347.

If you execute the SET\_OPTIONS administration method, tracing starts immediately. It is not necessary to restart the server. However, if you stop and restart the server, you must reissue the SET\_OPTIONS administration method to restart the tracing.

The trace messages are recorded in the server log file.

### 32.1.1.6 Disabling the workflow agent

Disabling the workflow agent stops the execution of automatic activities. To disable the workflow agent, set the workflow agent worker threads property in the server configuration properties to 0. [“Modifying general server configuration information” on page 32](#) contains more information on the server configuration properties.

Stop and restart Documentum CM Server for the change to take effect. Reinitializing the server does not make the change effective.

## 32.2 Work queue management

Work queues hold tasks that are to be performed by users who are assigned to the queue. Work queue users receive tasks in their Inboxes. Work queue users are assigned tasks either automatically by the server or manually by another user. To access work queues, users must belong to one of the roles described in [“User roles for work queues” on page 600](#). Work queue users are also referred to as *processors*.

Apart from work queue users there are

- Work queue managers

Managers monitor work queues to see which queues have overdue tasks that need to be addressed or which queues have too many tasks in the queue. Managers can add, edit, and assign skill profiles to individual work queue users.

- Work queue administrators

Administrators create work queues, assign users to work on queue tasks, define the skill profiles that enable the application to assign tasks to the appropriate processor, and add, edit, or assign skill profiles to the individual work queue users.

The administrator or manager can use the Work Queue Monitor to view the tasks in the queue, the name of the processor assigned to the task, the status of the task, when the task was received, and the current priority of the task.

**Table 32-1: User roles for work queues**

Role	Description
Queue_processor	Works on items that are assigned by the system from one or more work queue inboxes. Queue processors can request work, suspend, and unsuspend work, complete work, and reassign their work to others.
Queue_advance_processor	Works on items that are assigned by the system from one or more work queue inboxes. Additionally, selects tasks to work on from one or more work queue inboxes.

Role	Description
Queue_manager	<p>Monitors work queues, assigns roles to queues, and assigns users to work on queue items. Queue managers can reassign, and suspend tasks.</p> <p>Queue managers who have CREATE_GROUP privileges can create work queues.</p>
Queue_admin	<p>Creates work queues, and queue policies. Members of the queue_admin role <i>do not</i> by default have the administrator role.</p> <p>Queue administrators who have CREATE_GROUP privileges can create work queues.</p>
Process_report_admin	Runs historical workflow reports from the Workflow menu.

## 32.3 Lifecycles

A lifecycle defines a sequence of states a file can encounter. Typically, lifecycles are designed for documents to describe a review process. For example, a user creates a document, sends it off to other users for review and approval. The lifecycle defines the state of the file at each point in the process.

The lifecycle itself is created using OpenText™ Documentum™ Content Management Documentum Composer and is deployed in the repository as part of an application. Documentum Administrator manages the lifecycles that already exist in a repository. All lifecycle procedures are accessed through the Tools menu in Documentum Administrator.

## 32.4 References

*OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* contains the information and instructions on the following:

- Starting a workflow
- Sending a quickflow
- Viewing workflows
- Pausing a workflow
- Resuming a paused workflow
- Stopping a workflow
- Emailing the workflow supervisor or a workflow performer
- Processing a failed task in a workflow

- Changing the workflow supervisor
- Saving workflow information as a Microsoft Excel spreadsheet
- Viewing aggregated report for workflow performance
- Creating a workflow template
- Configuring the workflow agent
- Setting up a new work queue
- Setting up work assignment matching
- Understanding work queue policies
- Defining a queue category
- Defining a work queue
- Defining work queue override policies
- Managing work queue users
- Monitoring work queues
- Creating business calendars
- Assigning a lifecycle to a file
- Removing a lifecycle from a file
- Promoting a file to the next lifecycle state
- Demoting a file to its previous lifecycle state
- Suspending a file from its current lifecycle state
- Resuming a suspended file

## Chapter 33

# Performance and tuning

This chapter provides recommendations and best practices to help you improve the overall performance of OpenText Documentum CM.



**Note:** The best practices and/or test results are derived or obtained after testing the product in our testing environment. Every effort is made to simulate common customer usage scenarios during performance testing, but actual performance results will vary due to differences in hardware and software configurations, data, and other variables.

### 33.1 Common problems with Documentum CM Server performance

The most common problems in Documentum CM Server performance include the following:

- Application design and customization
  - Chatty or redundant application code is the most common cause of failure (40 percent in 1995 IEEE study)
  - Complex object models
  - Poor memory and cache management
- Network
  - High latency due to physical or logical limitations
  - Overburdened shared network
- Undersized Server resources (inadequate memory and CPU size)
- Unmanaged or under used RDBMS resources
  - RDBMS not regularly monitored and tuned
  - Performance and caching features not used
  - Insufficient tablespace available after performing the upgrade
- Unrealistic expectations (did not use realistic benchmarks)

Carefully design your highly available infrastructure to fit your business requirements. There is no single solution that fits all.

The following solutions are available to help with these problems:

## High availability Documentum CM Server clusters

Server clusters (also called *server sets*) can be active-active or active-passive. In an active-active cluster, there are two active load-balanced web application servers, two active sets consisting of a Documentum CM Server and connection broker, one active RDBMS with clustered standby server, one primary database with one synchronized standby, and one primary content store with one synchronized standby. In an active-passive cluster, everything is the same, except that there is only one active server plus connection broker set, with another set as standby.

These cluster configurations provide partial high availability coverage with increased scalability. The clusters can be managed with Documentum Administrator.

## Redundant connection brokers

Connection brokers (formerly known as docbrokers) can be configured to automatically reroute users to Documentum CM Servers that are online. Connection brokers can load balance user connections across multiple Documentum CM Servers using identical proximity values for connection brokers. *OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) contains more information.

## Replication

Replication can be configured either as read/write or read only.

## Disaster recovery

Disaster recovery is not the same as high availability. It assumes a total loss of the production data center. Disaster recovery servers are separate and independent from the main center. They share no resources, and each has an independent network infrastructure for WAN replication. Both systems have the capacity to carry out full normal and emergency workloads. They must be maintained to be compatible.

Failover for disaster recovery is manual, not automatic.

## Enhancing query performance

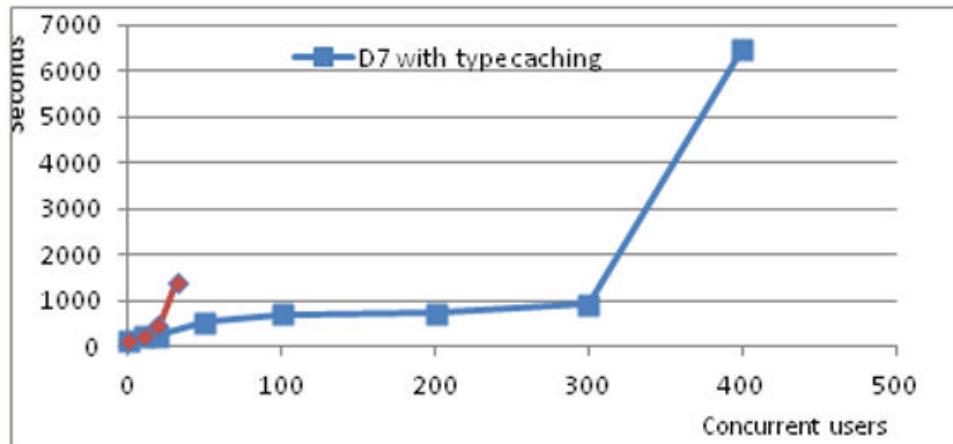
*OpenText Documentum Content Management - Administrator User Guide* (EDCAC250400-UGD) describes how to monitor query performance using the Update Statistics administration tool. It also describes how to limit poorly performing subqueries for users who belong to many groups.

## 33.2 Type caching

With the type caching enhancements in OpenText Documentum CM 7.0, every session shares types from a global cache thereby improving memory usage, which in turn can yield better concurrency and scalability. You can apply the following best practices for better performance when a large number of types are used:

### 33.2.1 Concurrency

- Unlike earlier versions of OpenText Documentum CM, the concurrency in OpenText Documentum CM 7.0 is not limited by the availability of memory on the Documentum CM Server when a large number of types were used. With the gains in concurrency seen in OpenText Documentum CM 7.0 for such use cases, additional physical memory can be added to get more concurrency. Here is an observation using a low level Foundation Java API-based test dealing with 1000 types of varying hierarchies.

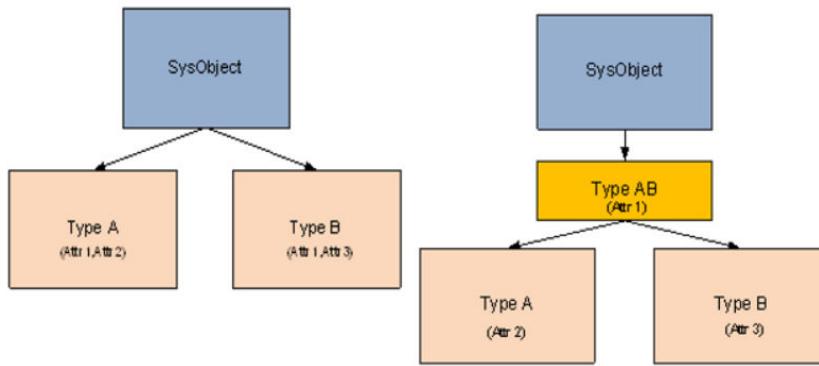


**Figure 33-1: Type caching results for a Foundation Java API-based test**

- The bottleneck is more likely the server session limitation for a single Documentum CM Server. The maximum number of sessions (that can run type related operations) on a single Documentum CM Server is still limited by the `max_concurrent_sessions` setting on the server.
- Read the database tuning guidelines as performance in type caching can be vastly improved by database tuning.

### 33.2.2 Deeper type hierarchy

A deeper type hierarchy (multiple levels of inheritance) can benefit from the memory usage improvements. For example, when there are two custom types, it is recommended to create a common parent type for the two types, with common attributes, as shown in the following figure:



**Figure 33-2: Deeper type hierarchy**

## 33.3 LDAP synchronization

LDAP integration for automated users and group management and authentication has become a common practice. In OpenText Documentum CM deployments using LDAP integration, user and group synchronization with Documentum CM Server repository has to perform well with minimal impacts to a live OpenText Documentum CM system. This section covers some tuning tips and best practices for the new LDAP Nested Group Synchronization (LDAP NG) feature in OpenText Documentum CM 7.0, to better utilize and schedule LDAP NG jobs.

### 33.3.1 Best throughput formula

- The `thread_pool_size` parameter is used to determine the working threads of LDAP NG job for concurrent processing. The default value of `thread_pool_size` is 5, and the maximum value is 25. To achieve the highest synchronization throughput (and speed), it is recommended to set a value that is best suited for the number of CPU cores in the host where Documentum CM Server is installed.
- The following table lists some observations on a host based on a Windows 2008 R2 based VM template with 8 GB of RAM:

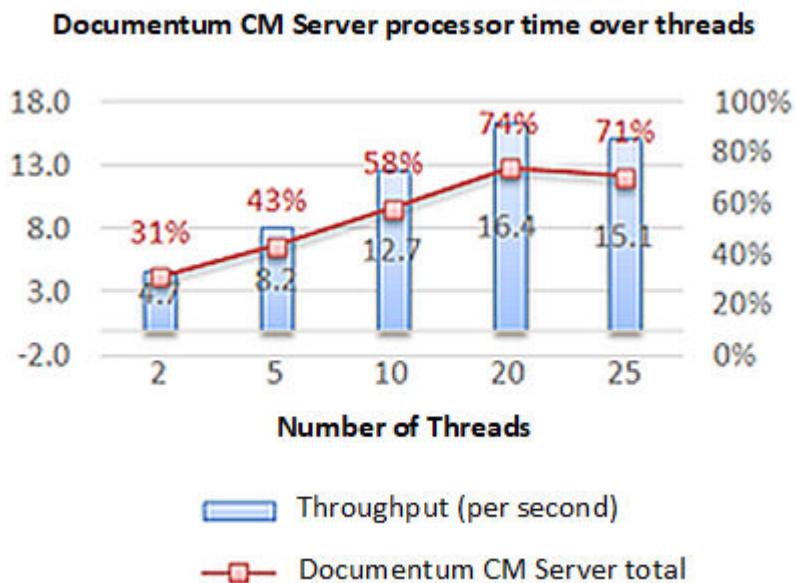
**Table 33-1: Synchronization throughput**

Throughput		Number of Threads			
Number of CPU cores		5	10	20	25
	2	7.4	10.5	10.2	
	4	7.7	12.8	16.8	14.4
	8			14.6	15.7

- For a system configuration with two and four cores, the optimal thread number is 5X cores.
- Adding more than 20 threads does not improve the throughput. It is recommended to use a maximum of 20 threads with more than four cores.

### 33.3.2 Throughput and CPU utilization balance

The CPU utilization of an LDAP NG job is notably higher than a traditional synchronization job. If the job cannot be scheduled at off-peak hours, one way to balance the CPU and throughput is to reduce the working threads, as shown in the following figure and table:

**Figure 33-3: Documentum CM Server processor time over threads**

**Table 33-2: Documentum CM Server processor time over threads**

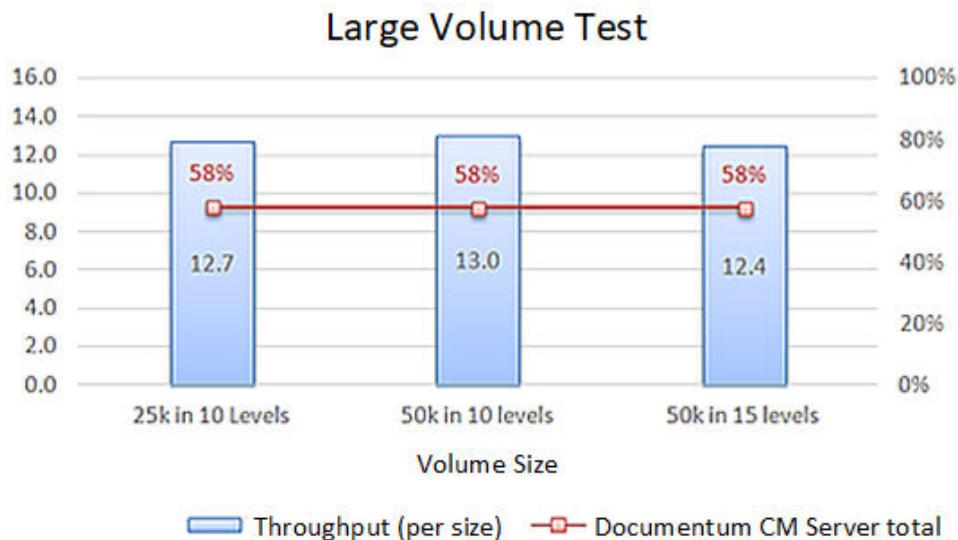
Documentum CM Server	Four Cores					
Parameters	Number of threads	2	5	10	20	25
	Heap size	1024	1024	1024	1024	1024
Performance metrics	Sync time (minutes)	90	56	33	25	30
	Throughput (per second)	4.8	7.7	12.8	16.8	14.4
Processor time						
OpenText Documentum CM	9%	17%	27%	35%	38%	
Java	19%	20%	22%	21%	21%	
contentserver_total	31%	42%	53%	59%	66%	
oracle_total	5%	8%	16%	19%	24%	

### 33.3.3 Large volume and hierarchy

- In an LDAP NG Synchronization test using large volume of groups and deeper group hierarchy as shown in the following table and figure, it was observed that the throughput, processor time, and memory cost were relatively close between different size of groups and hierarchy levels:

**Table 33-3: LDAP NG synchronization test results**

Test Case	Groups	Hierarchy Level	Users	Group Members
Baseline spread	25,716	10	100,000	192,914
Larger spread	51,432	10	100,000	360,024
Larger and deeper spread	49,152	15	100,000	344,064

**Figure 33-4: Large volume test**

- There is very little performance impact by extending the group entry size and hierarchy levels. CPU and memory are not affected by the larger size of LDAP. From the test results, it can be seen that the LDAP NG synchronization speed depends only on the number of Documentum CM Server cores and job working threads.

### 33.3.4 Java Method Server tuning

- There are two ways to execute an LDAP NG job:
  - Within Java Method Server as a method
  - As a standalone Java executable
- When executed within Java Method Server with default configuration settings (1024 heap size), the garbage collector runs at an acceptable range - the average garbage collection (GC) overhead was less than three percent, and there were no severe performance impact. However, you must consider other OpenText Documentum CM jobs running on Java Method Server at the same time, as there should be overall performance degradation if the GC overhead due to LDAP NG synchronization job is more than five percent.
  - It is recommended to use a larger heap, especially with more than 20 working threads, as shown in the following table:

**Table 33-4: Garbage collection at various Java Method Server heap sizes**

Documentum CM Server		Four Cores	
Parameters	Number of threads	20	20
	Heap size	1024	1680
Performance metrics	Sync time (minutes)	25	25
	<i>Throughput (per second)</i>	16.8	16.9
	<i>Processor time</i>		
	contentserver_total	59%	61%
	oracle_total	19%	20%
	<i>Garbage Collection</i>		
	Average GC overhead	2.40%	1.60%
	Number of all GC	142	86
	Number of full GC	22	6
	Total GC pause (in seconds)	41	34

- Another alternative is executing the LDAP NG job by a standalone Java process.
- The throughput improvement is limited while enlarging the Java Method Server heap size to 1680 MB, but the GC performance gets better.
- It was also observed during the tests that the maximum heap consumption (and therefore garbage collection) occurred when users are processed. The LDAP NG job will first synchronize all the users in the target nested group and then process new groups and members. Therefore, it is recommend that you set a larger Java heap if your registered users are more than 100,000.

### 33.3.5 Database tuning

- If the repository database is Oracle, then Oracle initialization parameter `Cursor sharing` should be set to `FORCE`. It could reduce SQL hard parses, improve library hit (from 0 to 99 percent), and reduce oracle CPU utilization (from 50 to 20 percent). By setting this parameter, the throughput of traditional synchronization jobs will also improve.
- High redo activity is also seen during the running of a job. You can increase the redo log size or number of redo logs to alleviate commits times.

## 33.4 Intelligent session management

The Intelligent Session Management (ISM) enhancements in OpenText Documentum CM 7.0 helps to improve the overall performance, scalability, and total cost of ownership (TCO). It achieves them through:

- Lower context switches on the Documentum CM Server.
- Lower memory usage on the Documentum CM Server (cache).
- Lower number of active sessions on the Documentum CM Server
- Lower number of sessions on the Oracle database

The session management enhancements have different levels of gains based on how sessions are created and used by the client transactions. The following list shows three classes of session usage:

- A: Reuse the existing connection (server session) and no authentication requirement (the same user).
- B: Reuse the existing connection (server session) and perform authentication.
- C: Create a new connection (server session).

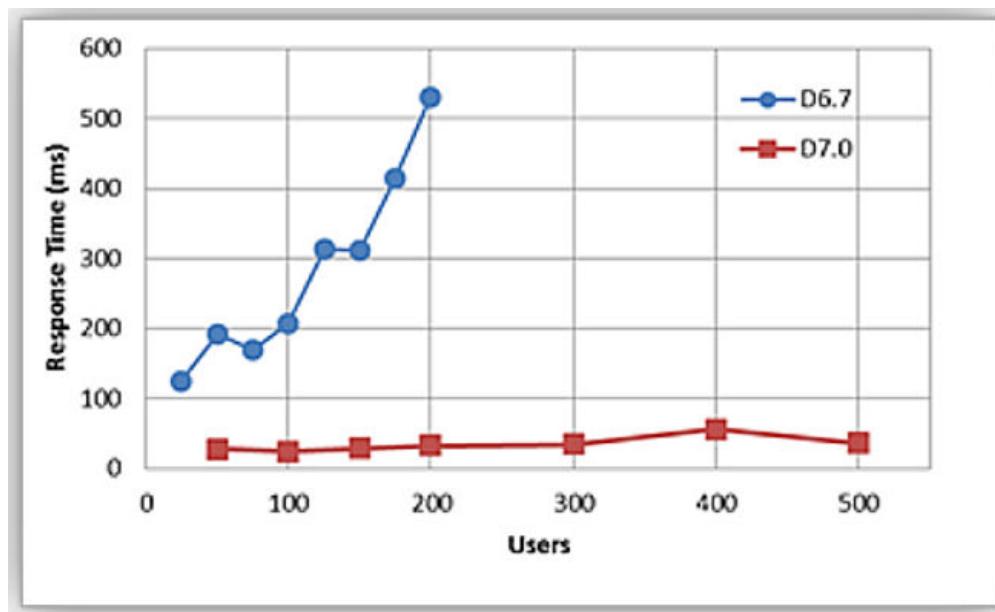
The performance implications in OpenText Documentum CM 7.0 for the three classes if session usages are the following:

- The number of connections is much smaller in OpenText Documentum CM 7.0 than OpenText Documentum CM 6.7 (connections will no longer be occupied in the Level-1 pool).
- A user is more likely to reuse the other user's session (class B) than to reuse his own session (class A).
- When you access the Documentum CM Server in a later transaction, your previous connection would have been used by others already. This will slightly affect the response time performance because additional authentication is required (the average response time of class A is generally smaller than that of class B).
- The average time of class B transactions is reduced from OpenText Documentum CM 6.7 to OpenText Documentum CM 7.0, due to more efficient context switching.
- For a large number of concurrent users, the number of class C transactions is smaller because of the following two reasons:
  1. The default value of the `dfc.session.reuse_limit` parameter is 100.
  2. The connections in the Level-1 pool will not be closed by force (thereby saving on creating/closing of connections), by using a more graceful queue algorithm.

In a Windows-based test involving short-living sessions, substantial gains were seen in response times when using the following settings:

**Table 33-5: Settings for the session usage test**

dfc.session.reuse_limit	100
dfc.connection.reuse_threshold	50
dfc.connection.cleanup_check_window	180
dfc.connection.queue_wait_time	500
dfc.session.max_count	1000
concurrent_sessions	100

**Figure 33-5: Response time test results**

In the same test, OpenText Documentum CM 7.0 consumed less system resource than 6.7.

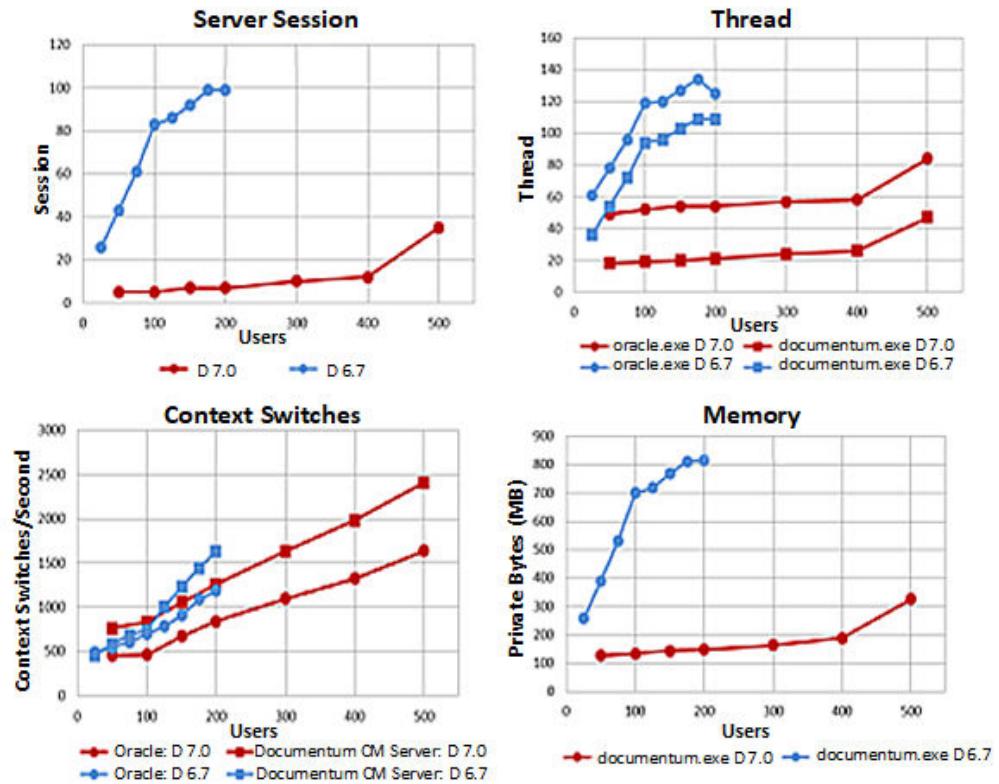


Figure 33-6: Resources usage

## 33.5 Multiple workflows in Linux

It is recommended that you follow these steps to avoid memory issues before you run multiple workflows in Linux.

1. The operating system has restriction of only 4096 file descriptors per user.

Edit `/etc/security/limits.conf` and set the following:

```
csuser soft nofile 8192
csuser hard nofile 16384
```

2. The kernel limits the number of user processes per user to 40.

Edit `/etc/security/limits.conf` and set the following:

```
csuser soft nproc 2047
```



# Chapter 34

## System events

This chapter lists and describes the system events recognized by Documentum CM Server. You can register most of these events for auditing. You can also use an `IDfSysobject.registerEvent` method to register to receive an Inbox notification for any of the Foundation Java API, workflow, or lifecycle events.

Those events which cannot be registered for auditing or notification are noted in their descriptions.

### 34.1 dm\_default\_set event

This dm\_default\_set events are audited by default. The following table describes the events for the `docbase_config` object type:

dm_archive	dm_checkin	dm_restore
dm_assemble	dm_checkout	dm_save
dm_bp_attach	dm_destroy	dm_setfile
dm_bp_demote	dm_freeze	dm_signoff
dm_bp_promote	dm_link	dm_unfreeze
dm_bp_resume	dm_lock	dm_unlink
dm_bp_suspend	dm_mark	dm_unlock
dm_branch	dm_prune	



**Note:** The dm\_default\_set event is registered against the docbase config object; however, it causes auditing of the listed events for dm\_document object type and its subtypes.

### 34.2 Foundation Java API events

The following table describes the events arising from Foundation Java API methods:

**Table 34-1: Foundation Java API events**

Event	Target object type	Event description	Trigger
dm_all (or all)	0 or omitted dm_sysobject	All	All auditable events in repository.  Any event on any Sysobject or the specified Sysobject.

Event	Target object type	Event description	Trigger
dm_add_dynamic_group	dm_group	Add To Dynamic Group	Execution of an IDfSession.addDynamicGroups call.
dm_adddigsignature	dm_sysobject	Add electronic signature	Execution of the addDigitalSignature method.  addDigitalSignature methods are always audited. It is not possible to unregister this event.
dm_addesignature	dm_sysobject	Add Electronic Signature	Execution of the addEsignature method.  addEsignature methods are always audited and the entries are always signed by Documentum CM Server. It is not possible to modify this behavior.
dm_addesignature_failed	dm_sysobject	Add Electronic Signature Failed	An attempt to execute the addEsignature method failed. These failures are always audited. It is not possible to modify this behavior.
dm_addnote	dm_sysobject dm_process	Add Note	Addition of a note to a SysObject.  When the target object is a process object, the SysObject is in a workflow package.
dm_addrrendition	dm_sysobject	Add Rendition	Addition of a rendition to an object.
dm_addretention	dm_sysobject	Add Retention	Object placed under control of a retention policy.

<b>Event</b>	<b>Target object type</b>	<b>Event description</b>	<b>Trigger</b>
dm_appendpart	dm_sysobject	Apend to Virtual Document	Addition of a component to a virtual document.
dm_archive	dm_sysobject	Archive Objects	Execution of an archive method.
dm_assemble	dm_sysobject	Assemble Virtual Document	Execution of assemble method.
dm_assume	dm_user	Assume User	Execution of Assume method.
dm_audit	all object types	Audit Event	Execution of method to register for auditing  Registrations for auditing are always audited. It is not possible to unregister this event.
dm_authenticate	dm_user	Authenticate User	Execution of an authenticate method.  Executing an authenticate method also generates a dm_connect method if the authentication requires a repository connection.
dm_branch	dm_sysobject dm_retainer	Branch Version	Execution of a branch method.
dm_checkin	dm_sysobject dm_retainer	Checkin Object	Checking in an object.
dm_checkout	dm_sysobject dm_retainer	Checkout Object	Checking out an object.

Event	Target object type	Event description	Trigger
dm_connect	dm_user	Logon	Establishing a repository connection.   <b>Note:</b> An authenticate method may also establish a repository connection, which will generate a dm_connect event in addition to the dm_authenticate event.
dm_destroy	dm_sysobject dm_acldm_user dm_group dm_retainer	Destroy Object	Execution of a destroy method.
dm_disassemble	dm_sysobject	Disassemble Virtual Document	Execution of a disassemble method.
dm_disconnect	dm_user	Logoff	Terminating a repository connection.
dm_fetch	dm_sysobject dm_retainer	Fetch Object	Fetching an object from the repository.
dm_freeze	dm_sysobject	Freeze Object	Execution of a freeze method.
dm_getfile	dm_sysobject	View/Export	Occurs when a document is viewed or exported or when the a getContent and getPath method is executed.
dm_getlogin	dm_user	Get Login	Execution of a getLoginTicket method.
dm_insertpart	dm_sysobject	Insert into Virtual Document	Execution of an insertPart method.
dm_install	dm_policy dm_process dm_activity	Install	Execution of an install method.
dm_invalidate	dm_process dm_activity	Invalidate	Execution of an invalidate method.

Event	Target object type	Event description	Trigger
dm_kill	not applicable	Kill Session	Execution of a Kill method.   <b>Note:</b> You cannot audit a Kill method that flushes the cache.
dm_link	dm_sysobject	Link To	Execution of a link method.
dm_lock	dm_sysobject	Lock Object	Execution of a lock method.
dm_logon_failure	dm_user	Logon Failure	User attempts to start a repository connection using invalid credentials.
dm_mark	dm_sysobject	Add Version Label	Execution of a mark method.
dm_move_content	dmr_content	Move Content	Execution of a MIGRATE_CONTENT administration method.
dm_prune	dm_sysobject dm_retainer	Prune Versions	Execution of a prune method.
dm_purgeaudit	dm_audittrail dm_audittrail_acl dm_audittrail_group	Purge Audit	Execution of a destroy method or PURGE_AUDIT administration method to remove audit trail entries.  Purging an audittrail entry is always audited. It is not possible to stop auditing this event.
dm_readonlysave	dm_sysobject	no event description provided	Generated when Documentum CM Server changes a property value of an immutable object.  This event is generated automatically for the full-text user.

Event	Target object type	Event description	Trigger
dm_remove_dynamic_group	dm_group	Remove From Dynamic Group	Execution of an IDfSession.removeDynamicGroups call
dm_removecontent	dm_sysobject	Remove Content	Execution of a removeContent method.
dm_removenote	dm_sysobject dm_process	Remove Note	Execution of a removeNote method.
dm_removepart	dm_sysobject	Remove from Virtual Document	Execution of a removePart method.
dm_removerendition	dm_sysobject	Remove Rendition	Execution of one of the removeRendition methods.
dm_removeretention	dm_sysobject	Remove Retention	Object removed from control of a retention policy.
dm_restore	dm_sysobject	Restore Object	Execution of a restore method.
dm_save	dm_sysobject dm_acl dm_group dm_user dm_retainer	Save Object	<p>Execution of a save method.</p> <p> <b>Note:</b> For new objects, Documentum CM Server stores the value Create in the audit trail attribute string_1. For existing objects, the value in the attribute is Save.</p> <p>For checked-out objects that are modified by users in the dm escalated_allow_save_on_lock group, Documentum CM Server stores the value SAVE_ON_LOCK in the string_2 attribute.</p>

Event	Target object type	Event description	Trigger
dm_saveasnew	dm_sysobject dm_acl dm_retainer	Copy Object	Execution of a saveAsNew method.
dm_setfile	dm_sysobject	Set Content	Execution of the following methods:  appendContent, appendFile, bindFile, iInsertFile, insertContent, setContent, setPath
dm_setoutput	dm_process	Setoutput	Execution of a Setoutput method.
dm_setretentionstatus	dm_retainer	Set Retention Status	Change to status of a retainer object.
dm_signoff	dm_sysobject	Signoff	Execution of a signoff method.  signoff methods are always audited. It is not possible to stop this auditing.
dm_unaudit	all object types	Unaudit Event	Removing an auditing registration.  Methods that remove (unregister) an audit registration are always audited. It is not possible to stop this auditing.
dm_unfreeze	dm_sysobject	Unfreeze Object	Execution of an unfreeze method.
dm_uninstall	dm_policy dm_process dm_activity	Uninstall	Execution of an uninstall method.
dm_unlink	dm_sysobject	Unlink From	Execution of an unLink method.
dm_unlock	dm_sysobject	Cancel Checkout	Execution of a cancelCheckOut method.
dm_unmark	dm_sysobject	Remove Version Label	Execution of an unMark method.
dm_updatepart	dm_sysobject	Update in Virtual Document	Execution of an updatePart method.

Event	Target object type	Event description	Trigger
dm_user_removepicture	dm_user	Remove user profile picture	Execution of a removeDisplayPicture method to remove the user profile picture.
dm_user_retrievepicture	dm_user	Retrieve user profile picture	Execution of a getDisplayPicture method to retrieve the user profile picture.
dm_user_updatepicture	dm_user	Update user profile picture	Execution of a setDisplayPicture method to add or modify the user profile picture.
dm_validate	dm_policy dm_process dm_activity	Validate	Execution of a validate method.

Events arising from methods that are specific to workflows are described in “Workflow events” on page 622.

### 34.3 Workflow events

The following table describes the events specific to workflows:

**Table 34-2: Workflow events**

Event	Target object type	Event description	Trigger
dm_all_workflow	dm_process (or not included)	All Workflow Events	<p>All events on workflows generated from the specified process object or all events in the repository.</p> <p> <b>Note:</b> This does not include dm_validate, dm_install, dm_invalidate, and dm_uninstall events, and dm_changestateprocess events.</p>

Event	Target object type	Event description	Trigger
dm_abortworkflow	dm_process	Abort Workflow	Aborting a workflow
dm_addattachment	dm_process	Add Attachment	An attachment is added to a running workflow or work item.
dm_addpackage	dm_process	Add Workflow Package	Execution of an addPackage method
dm_autotransactivity	dm_process	Automatic Workflow Activity Transition	An automatic activity transition occurs
dm_changedactivityinstancestate	dm_process	Change Workflow Activity to Failed State	An automatic activity changes state because the error handling flag is set to zero and the work item returns a non-zero value.
dm_changepriorityworkitem	dm_process	Change Workitem Priority	The priority value of a work item is changed at runtime.
dm_changestateactivity	dm_process	Change Workflow Activity State	An activity instance changes state to a state other than failed or changes state due to an automatic transition.
dm_changestateworkflow	dm_process	Change Workflow State	A workflow changes state by a method other than a save, execute, or abort.
dm_changeworkflowsupervisor	dm_process	Change Workflow Supervisor	Execution of a Setsupervisor method
dm_completedworkitem	dm_process	Complete Workitem	Execution of a Complete method
dm_createworkflow	dm_process	Create Workflow	A workflow is created.
dm_delegatedworkitem	dm_process	Delegate Workitem	A work item is delegated.
dm_finishworkflow	dm_process	Finish Workflow	A workflow is terminated.
dm_pauseworkitem	dm_process	Pause Workitem	A work item is paused.

Event	Target object type	Event description	Trigger
dm_portselect	dm_process	Select Workflow Port	Selection of output ports by a user or Documentum CM Server upon completion of an activity.   <b>Note:</b> This event is not triggered if the activity has a transition type of prescribed.
dm_pseudocomplete_dworkitem	dm_process	Pseudo_Complete Workitem	A work item is marked as pseudo-completed by Documentum CM Server
dm_removeattachment	dm_process	Remove Attachment	An attachment is removed from a workflow or work item
dm_removepackage	dm_process	Remove Workflow Package	A package is removed from a workflow
dm_repeatworkitem	dm_process	Repeat Workflow Work Item	A work item is repeated.
dm_resumeworkitem	dm_process	Resume Workitem	A work item is resumed.
dm_save_workqueue	Not applicable	Not applicable	Generated when a workqueue object is saved by the Workqueue SBO.  It is not possible to register for this event.
dm_save_workqueue_policy	Not applicable	Not applicable	Generated when a workqueue policy object is saved by the Workqueue SBO.  It is not possible to register for this event.
dm_selectedworkitem	dm_process	Select Workitem	A work item is acquired.
dm_startworkflow	dm_process	Start Workflow	A workflow is started.

Event	Target object type	Event description	Trigger
dm_startedworkitem	dm_process	Start Workitem	A work item is generated.
dm_suspendedworkqueueuetask	dm_process	Suspend Workqueue Tasks	A task on a workqueue is suspended.
dm_unsuspendedworkqueueuetask	dm_process	Unsuspend Workqueue Tasks	A task on a workqueue is resumed.
dm_wf_autodelegate_failure	dm_process	Auto Delegation Failed	Automatic delegation of an activity failed.
dm_wf_business_data	dm_process	All workflow events	An activity completes and at least one package is defined to generate a report on the activity.

Additional workflow events are:

- Pre Timer Expires: Alerts the workflow supervisor if an activity has not started within a specified time after the workflow starts.
- Post Timer Expires: Alerts the workflow supervisor if an activity does not complete within a specified time after it starts.

Several API events described in “[Foundation Java API events](#)” on page 615 are also applicable to workflows.

## 34.4 Lifecycle events

“[Lifecycle events](#)” on page 625 lists the events specific to lifecycles.

**Table 34-3: Lifecycle events**

Event	Target object type	Event description	Trigger
dm_bp_attach	dm_sysobject dm_retainer	Attach Lifecycle	Attaching a lifecycle to an object.
dm_bp_demote	dm_sysobject dm_retainer	Demote from Lifecycle State	Demoting an object from a lifecycle state.
dm_bp_promote	dm_sysobject dm_retainer	Promote to Lifecycle State	Promoting an object to a lifecycle state.
dm_bp_resume	dm_sysobject dm_retainer	Resume Lifecycle	Resuming a suspended lifecycle.
dm_bp_suspend	dm_sysobject dm_retainer	Suspend Lifecycle	Suspending a lifecycle.

## 34.5 Events sent to the fulltext user

The following events are generated automatically for the dm\_fulltext\_user user:

- dm\_checkin
- dm\_destroy
- dm\_move\_content
- dm\_readonlysave
- dm\_save

## 34.6 Events related to jobs

- Job\_Failure: Any issues specific to the execution of job reports the AE\_JOB\_QUEUE\_EVENT/Job\_Failure event.
- Agent\_Exec\_Failure: Any issues with the agent\_exec utility that manages the job scheduling, cleanup, and so on reports the AE\_QUEUE\_EVENT/Agent\_Exec\_Failure event.

## Chapter 35

# Populating and publishing the data dictionary

## 35.1 Populating the data dictionary

Data dictionary files for certain locales are installed with Documentum CM Server (see “[Default files provided by OpenText Documentum CM](#)” on page 640). When a repository is created, `dd_populate.ebs` is executed. If the locale of the host machine matches an installed, data dictionary file of locale, then `dd_populate.ebs` is executed with that data dictionary file of locale; otherwise, the English data dictionary file is used.

 **Note:** If the `server_codepage` property is set in the `server.ini` file, then you must set that property to UTF-8.

OpenText recommends that you add only the required locales to the data dictionary.

 **Note:** Additional data dictionary information may impact server performance depending on the configuration.

To add a new locale, use the population script provided by OpenText Documentum CM. To add to or change the locale information for installed data dictionary locales, you can use:

- The population script provided by OpenText Documentum CM
- The DQL CREATE TYPE or ALTER TYPE statement

Only some of the data dictionary information can be set using a population script. (“[Summary of settable data dictionary properties](#)” on page 631, describes the data dictionary properties that you can set in a population script.) The information that you cannot set using the population script must be set using the DQL statements. Additionally, you must use DQL if you want to set data dictionary information that applies only when an object is in a particular lifecycle state.

“[Using DQL statements](#)” on page 641, discusses using DQL to populate the data dictionary.

To change the data dictionary locale of repository, (in Documentum Administrator) change the **Data Dictionary Locales** property on the **Repository Configuration Properties - Info** page of repository.

### 35.1.1 Populating a repository's data dictionary with a locale-specific data dictionary file

The information in this section describes the populating a repository's data dictionary with a Japanese, Korean, Simplified Chinese, Russian, or Arabic locale-specific data dictionary file.

If the repository's machine is not running on the corresponding localized operating system (for example, the machine is running the English Windows 2008 operating system), you must run `dd_populate.ebs` on the repository's machine from another machine that is running the desired localized operating system.



**Note:** The corresponding localized machine term means a computer that is running the corresponding localized operating system.

You share and map the `%DM_HOME%\bin` (Windows) of repository machine or mount the `$DM_HOME\bin` (Linux) of repository machine (with the appropriate permissions) onto the corresponding localized machine; and then execute `dd_populate.ebs` from the corresponding localized machine. In addition, on Windows, you can specify the UNC path to `%DM_HOME%\bin`.



**Note:** For Russian and Arabic, if the repository machine is running the English operating system, then you can change the regional or language settings of the repository machine to one of the corresponding locales and then execute the `dd_populate.ebs` on the repository machine.

## 35.2 Data dictionary population script

The data dictionary population script, `dd_populate.ebs`, is a Docbasic script that reads an initialization file. The initialization file contains the names of one or more data files that define the data dictionary information you want to set. “[Executing the script](#)” on page 639 contains the instructions on executing the script.

### 35.2.1 Initialization file

You can name the initialization file to any desired name, but it must have a `.ini` extension. The structure of the initialization file is:

```
[DD_FILES]
<non-NLS_data_dictionary_data_file_1>
<non-NLS_data_dictionary_data_file_2>
.
.
.
<non-NLS_data_dictionary_data_file_n>

[NLS_FILES]
<NLS_data_dictionary_data_file_1>
<NLS_data_dictionary_data_file_2>
.
.
.
<NLS_data_dictionary_data_file_n>
```

The non-NLS data dictionary files contain the data dictionary information that is not specific to a locale.

The NLS data dictionary files contain the information that is specific to a locale.

You can include any number of data files in the initialization file. Typically, there is one file for the non-NLS data and an NLS data file for each locale. You can reference the data files by name or full path specification. If you reference a data file by name only, the data file must be stored in the same directory as the population script or it must be in %DM\_HOME%\bin (\$DM\_HOME/bin).

### 35.2.2 Data files

The data files are text files. You can create them with any text editor. There are two kinds of data files:

- Non-NLS
- NLS

In the non-NLS data files, the information you define is applied to all locales. In these files, you define the information that is independent of where the user is located. For example, you would set the `is_searchable` or `ignore_immutable` setting of the property in a non-NLS-sensitive file.

In an NLS data file, all the information is assumed to apply to one locale. In these files, you identify the locale at the beginning of the file and only the dd type info and dd attr info objects for that locale are created or changed. For example, if you set the label text for a new property in the German locale, the system sets `label_text` in the dd attr info object of new property in the German locale. It will not set `label_text` in the dd attr info objects of property for other locales.

If you do set NLS information in a non-NLS data file, the server sets the NLS information in the current locale of the session.

If you include multiple NLS files that identify the same locale, any duplicate information in them overwrites the information in the previous file. For example, if you include two NLS data files that identify Germany (de) as the locale and each sets `label_text` for properties, the label text in the second file overwrites the label text in the first file. Unduplicated information is not overwritten. For example, if one German file sets information for the document type and one sets information for a custom type called proposals, no information is overwritten.



**Note:** Future upgrades of Documentum CM Server may overwrite any changes you make to the data dictionary information about OpenText Documentum CM object types. To retain those changes, use a separate data file to create them. You can then re-run that data file after the upgrade to recreate the changes.

### 35.2.2.1 File structure

Each data file consists of sections headed by keywords that identify the object type and, if you are defining information for a property, the property. Additionally, an NLS file must identify the locale at the beginning of the file.

To specify the locale in an NLS file, place the following key phrases as the first line in the file:

- LOCALE=<locale\_name>CODEPAGE=<codepage\_name>

<locale\_name> is defined as a string of up to five characters. When the locale is defined in a file, the server resets the current session locale to the specified locale and the information in that data file is set for the given locale.

<codepage\_name> is the name of the code page appropriate for the specified locale.

**Table 35-1: Locale-based configuration settings for the data dictionary files installed with Documentum CM Server**

Locale	locale_name	default_client_codepage and codepage_name	server_os_codepage
Arabic	ar	ISO-8859-6	ISO-8859-6
English	en	ISO-8859-1	ISO-8859-1
Chinese (Simplified)	zh	MS936	MS936
Dutch	nl	ISO-8859-1	ISO-8859-1
French	fr	ISO-8859-1	ISO-8859-1
German	de	ISO-8859-1	ISO-8859-1
Italian	it	ISO-8859-1	ISO-8859-1
Japanese	ja	Shift_JIS	On Windows: Shift_JIS  On Linux: EUC-JP
Korean	ko	EUC-KR	EUC-KR
Portuguese (Brazilian)	pt	ISO-8859-1	ISO-8859-1
Russian	ru	Windows-1251	Windows-1251
Spanish	es	ISO-8859-1	ISO-8859-1
Swedish	sv	ISO-8859-1	ISO-8859-1
Hebrew	he	ISO-8859-8	ISO-8859-8

To define information for an object type, the format is:

```
TYPE=<type_name>
<data_dictionary_property_settings>
```

To define information for a property, the format is:

```
TYPE=<type_name>property=<property_name>
<data_dictionary_property_settings>
```

If you want to define information for multiple properties of one object type, specify the type only once and then list the properties and the settings:

```
TYPE=<type_name>property=<property_name>
<data_dictionary_property_settings>
{property=<property_name>
<data_dictionary_property_settings>
```

The setting for one data dictionary property settings must fit on one line.

[“Summary of settable data dictionary properties” on page 631](#) lists the data dictionary properties that you can set in data files. [“Examples of data file entries” on page 637](#) shows some examples of how these are used in a data file.

### 35.2.2.2 Summary of settable data dictionary properties

Data dictionary information is stored in the repository in internal object types. When you set data dictionary information, you are setting the properties of these types. Some of the information applies only to object types, some applies only to properties, and some can apply to either or both.

[“Settable data dictionary properties using population script” on page 631](#), lists and briefly describes the data dictionary properties that you can set using a population script.

**Table 35-2: Settable data dictionary properties using population script**

property name	Reference in script as:	Which level	NLS-specific (Yes or No)	Comments
ignore_immutab le	IGNORE_ IMMUTABLE	property	No	None
allowed_search_ ops default_search_o ps default_search_a rg	ALLOWED_ SEARCH_OPS DEFAULT_ SEARCH_OP DEFAULT_ SEARCH_ARG	property	No	If allowed_search_ops is set, you must set default_search_ops.  Default_search_arg, if set, must be set to one of the allowed_search_ops.

property name	Reference in script as:	Which level	NLS-specific (Yes or No)	Comments
read_only	READ_ONLY	property	No	None
is_hidden	IS_HIDDEN	property	No	None
is_required	IS_REQUIRED	property	No	None
not_null not_null_msg not_null_enf	NOT_NULL REPORT=<string> ENFORCE=<string>	property	Yes	<p>Setting not_null sets the not_null data dictionary property to TRUE.</p> <p>Including REPORT (not_null_msg) or ENFORCE (not_null_enf) is optional. If you include both, REPORT must appear first.</p> <p>Valid values for ENFORCE are application and disable.</p>
map_data_string map_display_string map_description	MAPPING_TABLE VALUE=<integer> DISPLAY=<string> COMMENT=<string>	property	Yes	<p>The key phrase MAPPING_TABLE must appear before the keywords that set the values for the mapping table.</p> <p>COMMENT is optional.</p> <p>VALUE and DISPLAY must be set. Set each once for each value that you want to map.</p> <p><i>"Examples of data file entries" on page 637</i> contains an example.</p>

property name	Reference in script as:	Which level	NLS-specific (Yes or No)	Comments
life_cycle	LIFE_CYCLE=<integer>	Object type	No	Valid values are: <Value> <Meaning> <ul style="list-style-type: none"><li>• Currently in use</li><li>• For future use</li><li>• Obsolete</li></ul>
label_text	LABEL_TEXT	Object type property	Yes	None
help_text	HELP_TEXT	Object type property	Yes	None
comment_text	COMMENT_TEXT	Object type property	Yes	None
is_searchable	IS_SEARCHABLE	Object type property	No	None
primary_key primary_key_ms g primary_key_enf	If defined at type level:  PRIMARY_KEY=<key> REPORT=<string> ENFORCE=<string>  If defined at property level:  PRIMARY_KEY REPORT=<string> ENFORCE=<string>	Object type property	Yes	If the primary key consists of one property, you can define the key at either the property or type level. At the type level, you must name the property in <key>. If you define the key at the property level, naming the property is not necessary.

property name	Reference in script as:	Which level	NLS-specific (Yes or No)	Comments
				<p>If the primary key consists of multiple properties, you must specify the key at the type level. Provide a comma-separated list of the properties in &lt;key&gt;.</p> <p>Including REPORT (primary_key_sg) or ENFORCE (primary_key_enf) is optional. If you include both, REPORT must appear first.</p> <p>Valid values for ENFORCE are application and disable.</p>

property name	Reference in script as:	Which level	NLS-specific (Yes or No)	Comments
unique_key unique_key_msg unique_key_enf	If defined at type level:  UNIQUE_KEY= <key> REPORT=<string> > ENFORCE=<string>  If defined at property level:  UNIQUE_KEY REPORT=<string> > ENFORCE=<string>	Object type property	Yes	<p>If the unique key consists of one property, you can define the key at either the property or type level. At the type level, you must name the property in &lt;key&gt;. If you define the key at the property level, naming the property is not necessary.</p> <p>If the unique key consists of multiple properties, you must specify the key at the type level. Provide a comma-separated list of the properties in &lt;key&gt;.</p> <p>Including REPORT (unique_key_msg) or ENFORCE (unique_key_enf) is optional. If you include both, REPORT must appear first.</p> <p>Valid values for ENFORCE are application and disable.</p>

property name	Reference in script as:	Which level	NLS-specific (Yes or No)	Comments
foreign_key foreign_key_ms g foreign_key_enf	At the type level: <code>FOREIGN_KEY=&lt;key&gt; REFERENCES=&lt;type&gt;(&lt;attr&gt;) REPORT=&lt;string&gt; &gt; ENFORCE=&lt;string&gt;</code>  At the property level: <code>FOREIGN_KEY=&lt;type&gt;(&lt;attr&gt;) REPORT=&lt;string&gt; &gt;ENFORCE=&lt;string&gt;</code>	Object type property	Yes	"Setting foreign keys" on page 636 contains the information to define this key.

### 35.2.2.3 Setting foreign keys

Similar to other keys, you can set a foreign key at either the type level or the property level.

If you set the key at the type level, you must identify which property of the type participates in the foreign key and which property in another type is referenced by the foreign key. The key phrase FOREIGN\_KEY defines the property in the object type that participates in the foreign key. The keyword REFERENCES defines the property which is referenced by the foreign key. For example, suppose a data file contains the following lines:

```
TYPE=personnel_action_doc
FOREIGN_KEY=user_name
REFERENCES=dm_user(user_name)
```

These lines define a foreign key for the personnel\_action\_doc subtype. The key says that a value in personnel\_action\_doc.user\_name must match a value in dm\_user.user\_name.

To define the same foreign key at the property level, the data file would include the following lines:

```
TYPE=personnel_action_doc
property=user_name
FOREIGN_KEY=dm_user(user_name)
```

REPORT and ENFORCE are optional. If you include both, REPORT must appear before ENFORCE. Valid values for ENFORCE are:

- application

- disable

### 35.2.2.4 Examples of data file entries

Here is an excerpt from a data file that sets non-NLS data dictionary information:

```
#set property level information for user_name property
TYPE=dm_user
property=user_name
IS_REQUIRED
DEFAULT_SEARCH_OP=contains

#set property level information for dm_document
TYPE=dm_document
property=acl_domain
IGNORE_IMMUTABLE
property=acl_name
IGNORE_IMMUTABLE
property=title
IS_REQUIRED
DEFAULT_SEARCH_OP=contains
property=subject
DEFAULT_SEARCH_OP=contains
property=authors
IS_REQUIRED
```

This excerpt is from a data file that defines data dictionary information for the English locale.

```
#This sets the locale to English.
LOCALE = en
CODEPAGE = ISO_8859-1

# Set property Information for dm_user
TYPE = dm_user
property = alias_set_id
LABEL_TEXT = User Alias Set ID

# Set property Information for dm_group
TYPE = dm_group
property = alias_set_id
LABEL_TEXT = Group Alias Set ID

# Set property Information for dm_process
TYPE = dm_process
property = perf_alias_set_id
LABEL_TEXT = Performer Alias Set ID

# Set property Information for dm_workflow
TYPE = dm_workflow
property = r_alias_set_id
LABEL_TEXT = Performer Alias Set ID

# Set property Information for dm_activity
TYPE = dm_activity
property = resolve_type
LABEL_TEXT = Alias Resolution Type
MAPPING_TABLE
VALUE = 0
DISPLAY = Default
COMMENT = Default Resolution
VALUE = 1
DISPLAY = Package-based
COMMENT = Resolution based on packages
VALUE = 2
DISPLAY = Previous Performer-based
COMMENT = Resolution based on last performer only
```

```
property = resolve_pkg_name
LABEL_TEXT = Alias Resolution Package

# Set property Information for dm_sysobject
TYPE = dm_sysobject
property = a_effective_label
LABEL_TEXT = Effective Label
property = a_effective_date
LABEL_TEXT = Effective Date
property = a_expiration_date
LABEL_TEXT = Expiration Date
property = a_effective_flag
LABEL_TEXT = Effective Flag
property = a_publish_formats
LABEL_TEXT = Publish Formats
property = a_category
LABEL_TEXT = Category
property = language_code
LABEL_TEXT = Language Code
property = authors
FOREIGN_KEY = dm_user(user_name)
REPORT = The author is not found in the repository.
ENFORCE = application

# Set property information for dmr_containment
TYPE = dmr_containment
property = a_contain_type
LABEL_TEXT = Containment Type
property = a_contain_desc
LABEL_TEXT = Containment Description

# Set property Information for dm_assembly
TYPE = dm_assembly
property = path_name
LABEL_TEXT = Path Name

# Set property Information for dm_relation
TYPE = dm_relation
property = r_object_id
LABEL_TEXT = Object ID
property = relation_name
LABEL_TEXT = Relation Name
property = parent_id
LABEL_TEXT = Parent ID
property = child_id
LABEL_TEXT = Child ID
property = child_label
LABEL_TEXT = Child Label
property = permanent_link
LABEL_TEXT = Permanent Link
property = order_no
LABEL_TEXT = Order Number
property = effective_date
LABEL_TEXT = Effective Date
property = expiration_date
LABEL_TEXT = Expiration Date
property = description
LABEL_TEXT = Description
```

This final example sets some constraints and search operators for the object types and their properties.

```
TYPE = TypeC
PRIMARY_KEY = Attr2, Attr3
REPORT = The primary key constraint was not met.
ENFORCE = application
UNIQUE_KEY = Attr2, Attr3
REPORT = The unique key constraint was not met.
ENFORCE = application
FOREIGN_KEY = Attr1
```

```

REFERENCES = TypeA(Attr1)
REPORT = TypeC:Attr1 has a key relationship with TypeA:Attr1
ENFORCE = disable
IS_SEARCHABLE = True
TYPE = TypeC
property = Attr1
ALLOWED_SEARCH_OPS = =,<,>,<=,>,>, NOT, CONTAINS, DOES NOT CONTAIN
DEFAULT_SEARCH_OP = CONTAINS
DEFAULT_SEARCH_ARG = 3
TYPE = TypeD
LIFE_CYCLE = 3
PRIMARY_KEY = Attr1
REPORT = Attr1 is a primary key.
ENFORCE = disable
LABEL_TEXT = label t TypeD
HELP_TEXT = help TypeD
COMMENT_TEXT = com TypeD
IS_SEARCHABLE = True
UNIQUE_KEY = Attr1
REPORT = Attr1 is a unique key.
ENFORCE = application
FOREIGN_KEY = Attr1
REFERENCES = TypeC(Attr1)
REPORT = Attr1 has a foreign key relationship.
TYPE = TypeE
property = Attr1
IGNORE_IMMUTABLE = True
NOT_NULL
ENFORCE = application
ALLOWED_SEARCH_OPS = CONTAINS, DOES NOT CONTAIN
DEFAULT_SEARCH_OP = CONTAINS
DEFAULT_SEARCH_ARG = 22
READ_ONLY = True
IS_REQUIRED = True
IS_HIDDEN = True
LABEL_TEXT = property 1
HELP_TEXT = This property identifies the age of the user.
COMMENT_TEXT = You must provide a value for this property.
IS_SEARCHABLE = False
UNIQUE_KEY
FOREIGN_KEY = TypeB(Attr1)
REPORT = This has a foreign key relationship with TypeB:Attr1
ENFORCE = application
FOREIGN_KEY = TypeC(Attr2)
REPORT = This has a foreign key relationship with TypeC:Attr2
ENFORCE = application

```

### 35.2.3 Executing the script

The population script is named dd\_populate.ebs and is found in %\DOCUMENTUM%\product\version\bin (\$DOCUMENTUM/product/<version>/bin).

A new locale is automatically added to the dd\_locales property of the dm\_docbase\_config object.

#### To execute the script:

1. Change to the %\DOCUMENTUM%\product\version\bin (\$DOCUMENTUM/product/<version>/bin) directory.
2. Enter the following command line at the operating system prompt:

```
dmbasic -f dd_populate.ebs -e Entry_Point -- <repository_name>
<username> <password> <ini_filename>
```

*<repository\_name>* is the name of the repository.

*<username>* is the name of the user executing the script. The user must have system administrator or superuser privileges.

*<password>* is the password of the user.

*<ini\_filename>* is the name of the initialization file that contains the data files. This can be a full path specification or only the file name. If you include just the file name, the file must be in the same directory as the population script.

### 35.2.4 Populating data dictionary on a repository from a non-English host

To populate data dictionary on a repository from a non-English host, connect to Documentum CM Server from a Windows computer in the desired locale and run the data dictionary population script from that computer. For example, to install the Japanese data dictionary information on a repository on a Korean host, connect to the repository from a Japanese Windows computer and run the script from the Japanese computer.

To install the data dictionary information on a 64-bit repository from a non-English host, you must copy the 64-bit Java installation, which defaults to the C:\Documentum\java64\<JDK\_version> folder (for example, “C:\Documentum\java64\1.6.0\_31”), to the host. Otherwise, an error occurs when you run the script.

### 35.2.5 Default files provided by OpenText Documentum CM

OpenText Documentum CM provides the following data dictionary files with Documentum CM Server:

- dd\_populate.ebs

dd\_populate.ebs is the script that reads the initialization file.

- data\_dictionary.ini

data\_dictionary.ini is the default initialization file.

- data files

The data files contain the default data dictionary information for OpenText Documentum CM object types and properties. They are located in %DM\_HOME%\bin (\$DM\_HOME/bin). There is a file for each supported locale. The files are named with the following format:

`data_dictionary_<localename>.txt`

where *<localename>* is the name of the locale. For example, the data file for the German locale is named data\_dictionary\_de.txt.

### 35.2.6 Using DQL statements

Use the DQL CREATE TYPE and ALTER TYPE statements to set data dictionary information if:

- You cannot add the information using a population file
- The information applies only when an object is in a particular lifecycle state
- You want to add or change information for a single object type or property

The DQL statements allow you to publish the new or changed information immediately, as part of the operations of statement. If you choose not to publish immediately, the change is published the next time the Data Dictionary Publisher job executes. You can also use the `publish_dd` method to publish the information. [“Publishing the data dictionary information” on page 641](#) contains more information on publishing.

*OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* contains the details on using these statements.

## 35.3 Publishing the data dictionary information

Information in the data dictionary is stored in internal object types and must be published before applications or users can access it. Publishing creates the `dd common info`, `dd type info`, and `dd attr info` objects that applications and users can query. After you add or change information in the data dictionary, the information must be published before the changes are accessible to users or applications.

Publishing can occur automatically, through the operations of the Data Dictionary Publisher job, or on request, using the `publishDataDictionary` method or the `PUBLISH` keyword.

### 35.3.1 Data dictionary publisher job

The Data Dictionary Publisher job publishes changes to the data dictionary. Each time the job runs, it publishes:

- Changes to previously published data dictionary information
- Previously unpublished data dictionary information, such as information added to a previously published locale or information for a new locale

The job uses the value of the `resync_needed` property of `dd common info` objects to determine which data dictionary objects need to be republished. If the property is set to TRUE, the job automatically publishes the data dictionary information for the object type or property represented by the `dd common info` object.

To determine what to publish for the first time, the job queries three views:

- `dm_resync_dd_attr_info`, which contains information for all properties that are not published

- dm\_resync\_dd\_type\_info, which contains information for all object types that are not published
- dm\_dd\_policies\_for\_type, which contains information for all object types that have lifecycle overrides defined

The Data Dictionary Publisher job is installed with the OpenText Documentum CM tool suite.

### **35.3.2 publishDataDictionary method**

The publishDataDictionary method publishes the data dictionary information. You can use the method to publish the entire data dictionary or just the information for a particular object type or a particular property. The Javadocs contains the information on using this method.

### **35.3.3 PUBLISH key phrase**

PUBLISH is a key phrase in the DQL CREATE TYPE and ALTER TYPE statements. If you include PUBLISH when you execute either statement, the server immediately publishes the new or changed information and any other pending changes for the particular object type or property.

For example, if you include PUBLISH when you create a new object type, the server immediately publishes the data dictionary for the new object type. If you include PUBLISH in an ALTER TYPE statement, the server immediately publishes the information for the altered object type or property and any other pending changes for that type or property.

If you do not include PUBLISH, the information is published the next time one of the following occurs:

- The Publish\_dd method is run to update the entire dictionary or just that object type or property
- The Data Dictionary Publisher job runs.
- An API method is executed to obtain data dictionary information about the changed object type or property.

# Chapter 36

## High-availability support scripts

OpenText Documentum CM provides a set of scripts that monitor processes to determine whether a given process is running or stopped. These scripts are installed when a Documentum CM Server installation is created. The scripts can be programmatically invoked from any commercial system management and monitoring package. This chapter describes the scripts and which processes they affect.

### 36.1 Monitoring scripts

Monitoring scripts are provided for Documentum CM Server, the connection broker, the Java method server, and for the Index Agent.

The scripts must be run as the Documentum CM Server installation owner. Each script returns success (the monitored process is running) as 0 or failure (the monitored process is stopped) as a non-zero value.

[“Monitoring scripts” on page 643](#), lists the processes that have monitoring scripts, the script names, and their locations and command-line syntax.

**Table 36-1: Monitoring scripts**

Process	Script	Syntax and location
Documentum CM Server	ContentServerStatus	A Java program in the server-impl.jar file.  The command line syntax is:  <code>java com.documentum.server.impl.u tils.ContentServerStatus - docbase_name xxxx -user_name</code>  On Linux, the return value is recorded in the variable \$?. On Windows, the return value is recorded in %ERRORLEVEL%.

Process	Script	Syntax and location
Connection broker	dmqdocbroker	<p>Located in %DM_HOME%\bin (\$DM_HOME/bin)</p> <p>The syntax is:</p> <pre>%DM_HOME%\bin\dmqdocbroker -t &lt;host_name&gt; -c ping</pre> <p>or</p> <pre>\$DM_HOME/bin/dmqdocbroker -t &lt;host_name&gt; -c ping</pre> <p>&lt;host_name&gt; is the name of the machine hosting the connection broker.</p> <p>On Linux, the return value is recorded in the variable \$. On Windows, the return value is recorded in %ERRORLEVEL%.</p>
Java method server	TestConnection	<p>A Java program in the server-impl.jar file.</p> <p>On Linux, the command line syntax is:</p> <pre>java com.documentum.server.impl.utils.TestConnection &lt;host&gt; &lt;port&gt; /DmMethods/servlet/DoMethod</pre> <p>On Windows, the command line syntax is:</p> <pre>java com.documentum.server.impl.utils.TestConnection &lt;host&gt; &lt;port&gt; /DmMethods/servlet/DoMethod</pre> <p>Where &lt;host&gt; is the Java Method Server (JVM) host machine, &lt;port&gt; is the port the JVM is using. You must include a space between the port and the servlet name.</p> <p>On Linux, the return value is recorded in the variable \$. On Windows, the return value is recorded in %ERRORLEVEL%.</p>

Process	Script	Syntax and location
Index Agent	IndexAgentCtrl	<p>A Java program in the server-impl.jar file.</p> <p>The command line syntax is:</p> <pre>java com.documentum.server.impl.u tils.IndexAgentCtrl - docbase_name &lt;repository_name&gt; - user_name &lt;user_name&gt; - action status</pre> <p>&lt;repository_name&gt; is the name of a repository served by the agent and &lt;user_name&gt; is the user account with which to connect to the repository.</p>
dm_agent_exec	dm_agent_exec	<p>The agent_exec_method method is used to configure the dm_agent_exec process for job scheduling. Enable the enable_ha_setup argument to achieve high-availability.</p> <ol style="list-style-type: none"> <li>1. Update the method_verb attribute to turn on high-availability feature:</li> </ol> <pre>retrieve,c,dm_method where object_name = 'agent_exec_method'</pre> <p>Methods of r_object_id is displayed.</p> <pre>get,c,l,method_verb ./dm_agent_exec (Linux) or .\dm_agent_exec.exe (Windows)</pre> <pre>set,c,l,method_verb ./dm_agent_exec - enable_ha_setup 1 (Linux) or .\dm_agent_exec.exe - enable_ha_setup 1 (Windows)</pre> <pre>save,c,l</pre> <ol style="list-style-type: none"> <li>2. Kill the existing dm_agent_exec process.</li> </ol> <p>On Linux, use the kill command and on Windows, use the <b>Task Manager</b> processes tab. dm_agent_exec restarts after a minute.</p>

## 36.2 Processes not requiring a script

The following processes do not require a separate script are dmbasic method server, Accelerated Content Services server, and Workflow agent. Documentum CM Server monitors these processes. If any of these processes stops, Documentum CM Server restarts it automatically.

# Chapter 37

## Consistency checks

### 37.1 General information

Consistency checks executed by the consistency checker job are sorted into tables that describe the checks on a particular area of the repository. Each table includes the following information:

- Consistency check number

Each consistency check has a unique number. When an inconsistency is reported, the report includes the consistency check number and some information about the particular inconsistency. For example:

```
WARNING CC-0001: User docu does not have a default group
```

- Description
- Severity level

The consistency checker script reports inconsistencies as a warning or an error.

- A warning is issued for a referential integrity inconsistency. For example, if the check finds a document referencing an author who no longer exists in the repository. A warning does not threaten repository operations, but should be fixed regardless.
- An error is issued for inconsistencies requiring immediate resolution. These inconsistencies include object corruption problems, such as missing \_r table entries or missing entries in a dmi\_object\_type table, and type corruption.

### 37.2 User and group checks

The consistency checks in the following table apply to users and groups:

**Table 37-1: Consistency checks for users and groups**

Consistency check number	Consistency check description	Severity
CC-0001	Check for users who belong to a group that does not exist.	Warning
CC-0002	Check for users who belong to groups that are not in dm_user.	Warning
CC-0003	Check for users who are not listed in dmi_object_type.	Error

Consistency check number	Consistency check description	Severity
CC-0004	Check for groups that are not listed in dmi_object_type.	Error
CC-0005	Check for groups that belong to groups that do not exist.	Warning
CC-0006	Check for groups belonging to supergroups that do not exist.	Warning
CC-0081	Check for groups with disconnected super groups.	Warning
CC-0082	Check for groups with disconnected subgroups.	Warning

### 37.3 ACL checks

The consistency checks in the following table apply to ACLs:

**Table 37-2: Consistency checks for ACLs**

Consistency check number	Consistency check description	Severity
CC-0007	Check for ACLs containing users who do not exist in the repository.	Warning
CC-0008	Check for ACLs which are missing dm_acl_r entries.	Error
CC-0009	Check for SysObjects whose acl_domain is set to a user who does not exist in the repository.	Warning
CC-0010	Check for SysObjects that belong to users who do not exist in the repository.	Warning
CC-0011	Check for SysObjects that are set to ACLs that do not exist.	Warning
CC-0012	Check for ACL objects with missing dm_acl_s entry.	Error
CC-0013	Check for ACL objects with r_accessor_permit values that are missing r_accessor_name values.	Error

Consistency check number	Consistency check description	Severity
CC-0014	Check for ACL objects with r_accessor_name values that are missing r_accessor_permit values.	Error
CC-0015	Check for ACL objects with r_is_group values that are missing r_accessor_permit values.	Error
CC-0016	Check for ACL objects with r_is_group values that are missing r_accessor_name values.	Error
CC-0017	Check for ACL objects with r_accessor_name values that are missing r_is_group values.	Error
CC-0018	Check for ACL objects with r_accessor_permit values that are missing r_is_group values.	Error

## 37.4 SysObject checks

The consistency checks in the following table apply to SysObjects:

**Table 37-3: Consistency checks for SysObjects**

Consistency check number	Consistency check description	Severity
CC-0019	Check for SysObjects that are not referenced in dmi_object_type.	Error
CC-0020	Check for SysObjects that point to non-existent content.	Warning
CC-0021	Check for SysObjects that are linked to non-existent folders.	Warning
CC-0022	Check for SysObjects that are linked to non-existent primary cabinets.	Warning
CC-0023	Check for SysObjects that reference non-existent i_chronicle_id.	Warning

Consistency check number	Consistency check description	Severity
CC-0024	Check for SysObjects that reference non-existent i_antecedent_id.	Warning
CC-0025	Check for SysObjects with dm_sysobject_s entry but missing dm_sysobject_r entries.	Error
CC-0026	Check for SysObjects with dm_sysobject_r entries but missing dm_sysobject_s entries.	Error

## 37.5 Folder and cabinet checks

The consistency checks in the following table apply to folders and cabinets:

**Table 37-4: Consistency checks for folders and cabinets**

Consistency check number	Consistency check description	Severity
CC-0027	Check for folders with missing dm_folder_r entries.	Error
CC-0028	Check for folders that are referenced in dm_folder_r but not in dm_folder_s.	Error
CC-0029	Check for dm_folder objects that are not referenced in dmi_object_type.	Error
CC-0030	Check for dm_folder objects that are missing dm_sysobject entries.	Error
CC-0031	Check for folders with non-existent ancestor_id.	Warning
CC-0032	Check for cabinet objects that are missing dm_folder_r table entries.	Error
CC-0033	Check that cabinet objects are not referenced in dmi_object_type.	Error
CC-0034	Check for folder objects that are missing dm_sysobject_r entries.	Error

Consistency check number	Consistency check description	Severity
CC-0035	Check for folder objects with null r_folder_path.	Error

## 37.6 Document checks

The consistency checks in the following table apply to documents:

**Table 37-5: Consistency checks for documents**

Consistency check number	Consistency check description	Severity
CC-0036	Check for documents with a dm_sysobject_s entry but no dm_document_s entry.	Error
CC-0037	Check for documents with missing dm_sysobject_s entries.	Error
CC-0038	Check for documents with missing dmi_object_type entry.	Error

## 37.7 Content object checks

The consistency checks in the following table apply to content objects:

**Table 37-6: Consistency checks for content objects**

Consistency check number	Consistency check description	Severity
CC-0039	Check for content objects referencing non-existent parents.	Warning
CC-0040	Check for content with invalid storage_id.	Warning
CC-0041	Check for content objects with non-existent format.	Warning

## 37.8 Workflow checks

The consistency checks in the following table apply to workflows:

**Table 37-7: Consistency checks for workflows**

Consistency check number	Consistency check description	Severity
CC-0042	Check for dmi_queue_item objects with non-existent queued objects.	Warning
CC-0043	Check for dmi_workitem objects that reference non-existent dm_workflow objects.	Warning
CC-0044	Check for workflow objects with missing dm_workflow_s entry.	Error
CC-0045	Check for dmi_package objects with missing dmi_package_s entries.	Error
CC-0046	Check for dmi_package objects that reference non-existent dm_workflow objects.	Warning
CC-0047	Check for workflow objects with non-existent r_component_id.	Warning
CC-0048	Check for dmi_workitem objects with missing dmi_workitem_s entry.	Error

## 37.9 Object type checks

The consistency checks in the following table apply to object types:

**Table 37-8: Consistency checks for object types**

Consistency check number	Consistency check description	Severity
CC-0049	Check whether any dm_type objects reference non-existent dmi_type_info objects.	Error

Consistency check number	Consistency check description	Severity
CC-0050	Check whether any dmi_type_info objects reference non-existent dm_type objects.	Error
CC-0051	Check whether any types have corrupted property positions.	Error
CC-0052	Check whether any types have invalid property counts.	Error

## 37.10 Data dictionary checks

The consistency checks in the following table apply to the data dictionary:

**Table 37-9: Consistency checks for the data dictionary**

Consistency check number	Consistency check description	Severity
CC-0053	Check whether any duplicate dmi_dd_attr_info objects exist.	Error
CC-0054	Check whether any duplicate dmi_dd_type_info objects exist.	Error
CC-0055	Check whether any dmi_dd_attr_info objects are missing an entry in dmi_dd_common_info_s.	Error
CC-0056	Check whether any dmi_dd_type_info objects are missing an entry in dmi_dd_common_info_s.	Error
CC-0057	Check whether any dmi_dd_attr_info objects are missing an entry in dmi_dd_attr_info_s.	Error
CC-0058	Check whether any dmi_dd_type_info objects are missing an entry in dmi_dd_type_info_s.	Error
CC-0078	Check whether any data dictionary objects reference non-existent default policy objects.	Error

## 37.11 Lifecycle checks

The consistency checks in the following table apply to document lifecycles:

**Table 37-10: Consistency checks for lifecycles**

Consistency check number	Consistency check description	Severity
CC-0059	Check for any dm_sysobject objects that reference non-existent dm_policy objects.	Warning
CC-0060	Check for any policy objects that reference non-existent types in included_type.	Warning
CC-0061	Check for any policy objects with missing dm_sysobject_s entries.	Error
CC-0062	Check for any policy objects with missing dm_sysobject_r entries.	Error
CC-0063	Check for any policy objects with missing dm_policy_r entries.	Error
CC-0064	Check for any policy objects with missing dm_policy_s entries.	Error

## 37.12 Object type index checks

The consistency checks in the following table apply to object type indexes:

**Table 37-11: Consistency checks for object type indexes**

Consistency check number	Consistency check description	Severity
CC-0073	Check for dmi_index objects that point to non-existent types.	Warning
CC-0074	Check for types with non-existent dmi_index object for _s table.	Warning
CC-0075	Check for types with non-existent dmi_index object for _r table.	Warning

Consistency check number	Consistency check description	Severity
CC-0076	Check for indexes with invalid property positions.	Warning

## 37.13 Method object consistency checks

These consistency checks in the following table apply to method objects:

**Table 37-12: Consistency checks for method objects**

Consistency check number	Consistency check description	Severity
CC-0077	Check for methods using jview rather than Java.	Warning



## Chapter 38

# Plug-in library functions for external stores

## 38.1 General recommendations

The following sections describe the C functions that you must implement to support Documentum CM Server operations through the plug-in:

- Call dm\_init\_content once when the plug-in is loaded. Call dm\_plugin\_version once after the plug-in is loaded.
- Use dm\_open\_content once for each getFile or getContent operation. Use dm\_read\_content multiple times to read the content in 16k blocks.
- Use dm\_close\_content once for each dm\_open\_content call.
- Use dm\_close\_all once in a session, and call dm\_deinit\_content once before the plug-in is unloaded.
- You can find sample code for a plug-in in the unsupported directory.

## 38.2 dm\_close\_all

The dm\_close\_all function is called by the plug-in when a session is terminated. The function is called to let the plug-in library cleanup any internal data structure(s) for the specified session.

The function definition is:

```
void dm_close_all (long <session>)
```

The following table describes arguments for the dm\_close\_all function:

**Table 38-1: dm\_close\_all arguments**

Argument	Description
session	Identifies the terminated session.

### 38.3 dm\_close\_content

The dm\_close\_content function is called by the plug-in to perform internal cleanup. This function is called after the read operation for the supplied handle is completed or if the read operation is interrupted. The function returns a boolean value.

The function definition is:

```
BOOL dm_close_content (long <handle>)
```

The following table describes the argument for the dm\_close\_content function:

**Table 38-2: dm\_close\_content arguments**

Argument	Description
handle	Identifies the read request.

### 38.4 dm\_deinit\_content

The dm\_deinit\_content function performs global internal cleanup operations. The function is called just before the server or client unloads the plug-in library, to let the plug-in perform any global internal cleanup operations.

The function definition is:

```
void dm_deinit_content(void)
```

### 38.5 dm\_init\_content

The dm\_init\_content function initializes internal data structures. This is the first function called by Documentum CM Server after the plug-in library is loaded.

The function definition is:

```
BOOL dm_init_content (long <maxsession>,
int <mode>)
```

The following table describes the arguments for the dm\_init\_content function:

**Table 38-3: dm\_init\_content arguments**

Argument	Description
maxsession	Contains the maximum number of concurrent sessions.
mode	Indicates who is invoking the plug-in. The only valid value is 0, indicating the server.

The function returns a positive value for successful initialization. A negative return value forces the server to unload the plug-in library. This function should return a positive value when called multiple times within the same address space.

## 38.6 dm\_open\_content

The dm\_open\_content function retrieves content.

The function definition is:

```
BOOL dm_open_content ( long <session>, char *<other_args>,
char *<token>, char *<store_object_id>, void *<callback>,
long *<handle>, long <errcode>)
```

The following table describes the arguments for the dm\_open\_content function:

**Table 38-4: dm\_open\_content arguments**

Argument	Description
session	Indicates the session that needs to retrieve the content.
other_args	Indicates the <other_args> supplied when executing a Mount method. NULL for the dm_extern_url, dm_extern_free storage types and when the token specified in a Setpath operation is an absolute path.
token	Is the path-translated token for which to retrieve the content.
store_object_id	Indicates the external storage object ID.
callback	Is a function pointer that can be called by the plug-in library to retrieve an attribute value for the supplied external storage object ID.
handle	Identifies the read request. Filled in on initialization and passed for subsequent read operations.
errcode	Contains error code in case of failure.

The plug-in DLL or shared library returns a positive value for successful initialization and fills in a value for the handle. For subsequent read operations for this token, the handle value is passed. In case of failure, the plug-in fills in an error code in errcode.

This function is called when the server or client needs to retrieve the content for the token.

The handle enables the plug-in to be a multi-threaded application with each thread servicing a particular read request, with a dispatching mechanism based on the handle value. For example, for dm\_extern\_file store objects, <other\_args> is the root path.

For client side plug-in configurations, if the Mount method has not been issued, the *<other\_args>* parameter is a pointer to the directory location represented by the def\_client\_root attribute.

For server side plug-in configurations, *<other\_args>* points to the directory represented by the a\_location value for the current sever configuration. If no a\_location is configured for the current server configuration, it points to the directory represented by the def\_server\_root attribute.

The call back function (which is part of server and client) is of the form:

```
char *dmPluginCallback (long <session>, char *<store_object_id>, char *attr_name, int <position>)
```

The call back function returns an attribute value in string form. The value for the position parameter should be zero when requesting an attribute value for an single-valued attribute and should be zero or greater for multi-valued attributes.

When this callback function is called for DM\_TIME datatype attribute values, the returned string format is *<mm/dd/yyyy hh:mi:ss>*.

Plug-in libraries can define the function pointer type as follows:

```
typedef char * (*DCTMPLUGINCALLBACK)(long, char *,char *,int)
```

Cast the callback parameter to DCTMPLUGINCALLBACK before calling by reference.

Advanced plug-ins may start performing the actual read asynchronously and start caching the content for performance reasons.

## 38.7 dm\_plugin\_version

The dm\_plugin\_version function enables backward compatibility for enhancement in future releases. This function is called once immediately after the plug-in is loaded into the process address space. The plug-in protocol version is 1.0. Therefore, the plug-in must set major to 1 and minor to 0.

The definition of this function is:

```
void dm_plugin_version(unsigned int *<major>, unsigned int *<minor>)
```

The following table describes the arguments for the dm\_plugin\_version function:

**Table 38-5: dm\_plugin\_version arguments**

Argument	Description
major	The major version number of the plug-in. The value of this argument must be 1.
minor	The minor version number of the plug-in. The value of this argument must be set to 0.

## 38.8 dm\_read\_content

The dm\_read\_content function requires the plug-in to return the content data into the location pointed to by buffer supplied.

The definition of this function is:

```
long dm_read_content ( long <handle>, char *<buffer>,
                      long <buffer_size>, long *<more_data>, long *<errcode>)
```

The following table describes the arguments for the dm\_read\_content function. The function returns the number of bytes read and filled into buffer. The plug-in must maintain its own internal bookkeeping to start reading from the next byte after the previous read.

**Table 38-6: dm\_read\_content arguments**

Argument	Description
handle	Identifies the read request.
buffer	Contains the location to return the content data; filled with zeros when there is no more content to be read or end-of-file is reached.
buffer_size	Contains the buffer size (16k).
more_data	When positive, indicates more reading is required.
errcode	Contains error code in case of failure.



## Chapter 39

# Usage tracking

The information in this chapter is intended to assist system administrators in interpreting the usage tracking information provided by Documentum CM Server.

## 39.1 Usage tracking

When a user logs into Documentum CM Server, the system makes an entry in a table managed by Documentum CM Server global registry. If this is the first time a user has logged in, a new line is added to the table that records the login name of the user, the name of the application used to log in, and the time of the login.

Consequent logins replace the latest use time and the login count in the table.

When a user logs into a OpenText Documentum CM application, that application, in turn, logs into Documentum CM Server with the credentials of the user. Therefore, one login to an application that supports usage tracking creates or modifies two lines in the table, one line for the application login and one line for the Documentum CM Server login. If you use an application that does not support usage tracking, only the Documentum CM Server line is created or modified.

For example, if a user logs in to Webtop, there are two lines modified in the global registry. One line shows the Webtop login and one line shows the Documentum CM Server login, since Webtop supports usage tracking. If a user logs in to Documentum CM Server using IDQL, there is only one line modified to show the Documentum CM Server login, because IDQL does not support usage tracking.

### 39.1.1 Tracking internal user accounts

Documentum CM Server creates several user accounts created for internal or system administration purposes. Usage tracking ignores these accounts, when these accounts are used to access Documentum CM Server. The Documentum CM Server installation owner account is also ignored when logging into Documentum CM Server.

However, if these accounts are used to log in to an application, the application login is recorded. For example, if the installation owner account is used to log into Webtop, there is a record of the Webtop login but no record of a Documentum CM Server login.

### 39.1.2 Tracking unique users

You can obtain a count of unique users from Documentum CM Server using the dm\_usageReport job. Depending on your environment, there are cases where you have to verify whether different user login names actually belong to different users or only one user.

When Documentum CM Server is set up in domain mode, the user name stored for usage tracking includes the user domain as well as the user login name. For example, user1 in the marketing domain is stored as marketing\user1. If there is a login name user1 in the engineering domain, a login for this user is stored as engineering\user1. When usage tracking counts unique users, it counts marketing\user1 and engineering\user1 as two distinct users. Depending on your environment, marketing\user1 and engineering\user1 could be the same or two different individuals.

It is also possible that some of the Documentum CM Servers using that global registry for usage tracking do not use domain mode, so the user name is stored without a domain. In this case, there can be entries for user1, engineering\user1, and marketing\user1.

You can export the usage tracking data from a global registry if you need to examine the individual entries and verify the unique user counts.

### 39.1.3 Tracking login times

Usage tracking record logins, but it does not provide user tracking in real-time. Usage tracking keeps a cache of previous logins that is retained by each application and Documentum CM Server for approximately one day. If a user logs in multiple times in a day, the usage tracking information is typically only updated once. The purpose of software usage tracking is to provide a long term view of usage without impacting Documentum CM Server and application performance.

Specific login times for a user can be obtained from the user object on the Documentum CM Server that the user logged into. That particular Documentum CM Server is not necessarily the global registry that is used for usage tracking.

### 39.1.4 Usage tracking and software compliance

Usage tracking tracks login information for certain software over time. Software compliance is using the software in conformance with the agreements governing the software license. While the information provided by usage tracking can assist with software compliance, you cannot rely upon it as your only source of compliance information.

Usage tracking reports are provided on an “AS IS” basis for informational purposes only. Inaccuracies can arise due to a number of factors such as inconsistencies in the setup of the global registry, access rights, customizations, availability of usage information within the software asset, and other similar issues. This can result in the collection and reporting of erroneous information. We shall not be liable for any

errors or omissions in the data, its collection and/or reporting by usage tracking. Regardless of the information provided by usage tracking, customers remain fully liable for utilizing the affected software in full compliance with the authorizing terms and quantities specified in the contract(s), quotes and purchase orders that governed the customer procurement of the software.

